Контроллер беспроводного доступа

WLC-30

Справочник команд CLI
Версия ПО 1.15.3

Содержание

1 Введение ... 3
2 История изменений ... 5
3 Правила пользования командной строкой ... 6
4 Структура системы команд ... 11
5 Команды пользовательского интерфейса ... 32
6 Управление программным обеспечением и конфигурацией ... 54
7 Настройка WLC ... 84
8 Настройка DNS ... 223
9 Настройка mDNS-reflector ... 226
10 Настройка общесистемных параметров ... 230
11 Управление системными часами ... 242
12 Настройка AAA ... 259
13 Конфигурирование и мониторинг интерфейсов ... 326
14 Конфигурирование и мониторинг туннелей ... 386
15 Управление L2-функциями ... 440
16 Работа с адресными таблицами ... 469
17 Настройка VRF ... 479
18 Настройка IP-адресации ... 483
19 Настройка IPv6-адресации ... 489
20 Управление профилями ... 502
21 Управление NAT ... 522
22 Настройки IPsec VPN ... 547
23 Управление VPN. Настройки удаленного доступа ... 594
24 Маршрутизация ... 627
25 Настройки MPLS ... 817
26 Резервирование ... 851
27 Безопасность ... 926
28 Управление QoS ... 1067
29 Мониторинг и управление ... 1103
30 Настройка DHCP ... 1203
31 Настройка SLA ... 1252
32 Настройка контроля абонентов (BRAS) ... 1283
33 Настройка Wi-Fi контроллера туннелей ... 1315

1 Введение

- Аннотация
- Целевая аудитория
- Примечания и предупреждения
- Используемые сокращения

Аннотация

В настоящем руководстве приведено описание команд CLI для администратора контроллера беспроводного доступа WLC-30 (в дальнейшем именуемого контроллером или устройством). Интерфейс командной строки (Command Line Interface, CLI) – интерфейс, предназначенный для управления, просмотра состояния и мониторинга устройства. Для работы потребуется любая установленная на ПК программа, поддерживающая работу по протоколам Telnet, SSH или прямое подключение через консольный порт (например, HyperTerminal).

Целевая аудитория

Справочник команд CLI предназначен для технического персонала, выполняющего настройку и мониторинг контроллера WLC-30 посредством интерфейса командной строки (CLI). Квалификация технического персонала предполагает знание основ работы стека протоколов TCP/IP, принципов построения Ethernet-сетей.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред программно-аппаратному комплексу, привести к некорректной работе системы или потере данных.

Используемые сокращения

- AAA – Authentication, Authorization, Accounting
- ARP – Address Resolution Protocol
- BGP – Border Gateway Protocol
- BRAS – Broadband Remote Access Server
- DHCP – Dynamic Host Configuration Protocol
- DNS – Domain Name System
- DDoS – Distributed Denial of Service
- DoS – Denial of Service
- FIFO – First In, First Out
- FTP – File Transfer Protocol
- FXO – Foreign eXchange Office
- FXS – Foreign eXchange Subscriber
- GRE – Generic Routing Encapsulation
- GRED – Gentle Random Early Detaction
- HTTP – HyperText Transfer Protocol
- HTTPS – HyperText Transfer Protocol Secure
- ICMP – Internet Control Message Protocol
- IKE – Internet Key Exchange
- IDS – Intrusion Detection System

- IP – Internet Protocol
- IP4IP4 – IP in IP
- IPS – Intrusion Prevention System
- IPsec – IP Security
- L2TP – Layer 2 Tunneling Protocol
- L2TPv3 – Layer 2 Tunneling Protocol version 3
- LACP – Link Aggregation Control Protocol
- LAG – Link Aggregation Group
- LDAP – Lightweight Directory Access Protocol
- LLDP – Link Layer Discovery Protocol
- MAC – Media Access Control
- MTU – Maximum Transmission Unit
- mDNS – Multicast Domain Name System
- NAT – Network Address Translation
- NAS – Network Access Server
- NTP – Network Time Protocol
- OSPF – Open Shortest Path First
- PPP – Point-to-Point Protocol
- PPTP – Point-to-Point Tunneling Protocol
- PPPOE – Point-to-point protocol over Ethernet
- PSK – Pre-Shared Key
- QoS – Quality of Service
- RADIUS – Remote Authentication Dial In User Service
- RED – Random early detection
- RIP – Routing Informational Protocol
- SFTP – Secure Shell File Transfer Protocol
- SIP – Session Initiation Protocol
- SLA — Service Level Agreement
- SNMP – Simple Network Management Protocol
- SCP – Secure Copy Protocol
- SP – Strict Priority
- SSH – Secure Shell
- STP – Spanning Tree Protocol
- TACACS – Terminal Access Controller Access Control System
- TFTP – Trivial File Transfer Protocol
- URL – Uniform Resource Locator
- VLAN – Virtual Local Area Network
- VPN –Virtual Private Network
- VRF – Virtual Routing/Forwarding
- VRRP – Virtual Router Redundancy Protocol
- VTI – Virtual Tunnel Interface
- WAN – Wide Area Network
- WINS – Windows Internet Name Service
- WRR – Weighted Round Robin
- XAUTH – eXtended Authentication

2 История изменений

Версия документа	Дата выпуска	Содержание изменений
Версия 1.1	10.01.2023	Вторая публикация
Версия 1.0	24.08.2022	Первая публикация
Версия программного обеспечения	**1.15.3**	

3 Правила пользования командной строкой

Для упрощения использования командной строки интерфейс поддерживает функцию автоматического дополнения команд. Эта функция активируется при неполно набранной команде и вводе символа табуляции <Tab>.

Другая функция, помогающая пользоваться командной строкой – контекстная подсказка. На любом этапе ввода команды можно получить подсказку о следующих элементах команды путем ввода вопросительного знака <?>.

Для упрощения команд всей системе команд придана иерархическая структура. Для перехода между уровнями иерархии предназначены специальные команды перехода. Это позволяет использовать менее объемные команды на каждом из уровней. Для обозначения текущего уровня, на котором находится пользователь, динамически изменяется строка приглашения системы.

Пример:

```
#Включение 15 уровня привилегий
wlc-30> enable
```

```
#Переход в режим конфигурирования устройства
wlc-30# configure
```

```
#Возврат на уровень выше
wlc-30(config)#
wlc-30(config)# exit
wlc-30#
```

Для удобства использования командной строки реализована поддержка горячих клавиш, перечисленных в таблице 1.

Таблица 1 – Описание горячих клавиш командной строки CLI

Сочетание клавиши	Описание
Ctrl+D	Во вложенном командном режиме – выход в предыдущий командный режим (команда exit), в корневом командном режиме – выход из CLI (команда logout)
Ctrl+Z	Выход в корневой командный режим (команда top)
Ctrl+A	Переход в начало строки
Ctrl+E	Переход в конец строки
Ctrl+U	Удаление символов слева от курсора
Ctrl+K	Удаление символов справа от курсора

Сочетание клавиши	Описание
Ctrl+C	Очистка строки, а также обрыв выполнения команды
Ctrl+W	Удаление слова слева от курсора
Ctrl+B	Переход курсора на одну позицию назад
Ctrl+F	Переход курсора на одну позицию вперед
Ctrl+L	Очистка экрана

Для удобства чтения добавлен постраничный вывод большой по объему информации.

Например:

```
wlc-30# show running-config
syslog max-files 3
syslog file-size 512
syslog file wlc-30 info
syslog console info
interface gigabitethernet 1/0/1
  ip address 10.100.14.1/24
exit
interface gigabitethernet 1/0/1.101
exit
interface gigabitethernet 1/0/2
  ip address 192.168.1.1/24
  ip address 10.100.100.2/24
exit
interface gigabitethernet 1/0/2.150
  ip address 10.150.150.2/24
exit
interface gigabitethernet 1/0/2.151
  ip address 10.151.151.15/24
exit
interface gigabitethernet 1/0/3
  ip address dhcp enable
exit
interface gigabitethernet 1/0/5.55
More? Enter - next line; Space - next page; Q - quit; R - show the rest.
```

Для отключения постраничного вывода в текущей сессии необходимо ввести команду:

```
wlc-30# terminal datadump
```

Интерфейс командной строки обеспечивает авторизацию пользователей и ограничивает доступ к командам на основании уровня привилегий, заданного администратором.

В системе может быть создано необходимое количество пользователей. Необходимый уровень привилегий задаётся индивидуально для каждого из них.

В заводской конфигурации в системе создан один пользователь с именем **admin** и паролем **password**.

Для обеспечения безопасности командного интерфейса команды распределены между 1, 10 и 15 уровнем привилегий:

- 1 уровень – доступен только мониторинг устройства;
- 10 уровень – доступно конфигурирование устройства, кроме создания пользователей, перезагрузки устройства, загрузки ПО;
- 15 уровень – нет ограничений.

Получение 15 уровня привилегий:

```
(wlc-30)> enable
(wlc-30)#
```

Возвращение на первоначальный уровень привилегий:

```
(wlc-30)# disable
(wlc-30)>
```

Система позволяет нескольким пользователям одновременно подключаться к устройству.

Для уменьшения объема отображаемых данных в ответ на запросы пользователя и облегчения поиска необходимой информации можно воспользоваться фильтрацией. Для фильтрации информации требуется добавить в конец командной строки символ «|» и использовать одну из опций фильтрации:

- begin – выводить все после строки, содержащей заданный шаблон;
- count – выводить только количество строк, отображаемых в выводе команды (без вывода информации, отображаемой самой командой);
- counter – добавляет к выводимой информации номера строк;
- include – выводить все строки, содержащие заданный шаблон;
- exclude – выводить все строки, не содержащие заданный шаблон;
- until – выводить все до строки, содержащей заданный шаблон.

Шаблон поиска может быть задан регулярным выражением и содержать:

– Перечень символов. Можно определить перечень, заключив символы в квадратные скобки «[]». Соответствие будет проверяться по символам, перечисленным в перечне. Если первый символ перечня «^», то соответствие будет проверяться по любому символу, не входящему в перечень. Примеры:

- [-az] – 'a', 'z' и '-';
- [a-z] – все латинские буквы от 'a' до 'z'.

– Специальные символы:

- ^ – начало строки;
- $ – конец строки;
- . – любой символ в строке;
- * – ноль или более раз.

Вывод команды «show running-config syslog» без параметров:

```
wlc-30# show running-config syslog
syslog max-files 3
syslog file-size 512
syslog file default info
```

Вывод команды «show running-config syslog» с параметром «begin»:

```
wlc-30# show running-config syslog | begin file-size
syslog file-size 512
syslog file default info
```

Вывод команды «show running-config syslog» с параметром «include»:

```
wlc-30# show running-config syslog | include file-size
syslog file-size 512
```

Вывод команды «show running-config syslog» с параметром «exclude»:

```
wlc-30# show running-config syslog | exclude file-size
syslog max-files 3
syslog file default info
```

Примеры использования регулярных выражений:

```
wlc-30# show interfaces status | include "^te.*"
te1/0/1         Up      Down    1500     a8:f9:4b:aa:05:d9
te1/0/2         Up      Down    1500     a8:f9:4b:aa:05:da
wlc-30# show interfaces status | include "^gi1/0/1[2568]"
gi1/0/12        Up      Down    1500     a8:f9:4b:aa:05:cc
gi1/0/15        Up      Down    1500     a8:f9:4b:aa:05:cf
gi1/0/16        Up      Down    1500     a8:f9:4b:aa:05:d0
gi1/0/18        Up      Down    1500     a8:f9:4b:aa:05:d2
wlc-30# show interfaces status | include "^[^tgI -]"
bridge 1        Up      Up      1500     a8:f9:4b:aa:05:c0
bridge 2        Up      Up      1500     a8:f9:4b:aa:05:c0
```

Для вывода информации, запрошенной командой show, в файл требуется добавить в конец командной строки соответствующий символ, путь и имя для создания или дополнения текстового файла.

Символы для вывода информации в файл:

- > – записать вывод команды в файл;
- >> – дописать вывод команды в конец файла;

Возможные пути для сохранения текстовых файлов вывода команд:

- flash:data/<FILE> – файл будет создан или дополнен в энергонезависимой памяти устройства в разделе flash:data;
- usb://<USB-NAME>:/<FILE> – файл будет создан или дополнен на USB-носителе с именем <USB-NAME>;
- mmc://<MMC-NAME>:/<FILE> – файл будет создан или дополнен на USB-носителе с именем <MMC-NAME>.

4 Структура системы команд

- Глобальный режим
- Конфигурирование контроллера
- Типы и порядок именования интерфейсов контроллера
- Типы и порядок именования туннелей контроллера

Система команд интерфейса командной строки контроллера WLC-30 разделена на иерархические уровни (разделы).

Глобальный режим

Верхний уровень иерархии команд приведен в таблице 2.

Таблица 2 − Иерархия командных режимов (верхний уровень)

Уровень	Команда входа	Вид строки подсказки	Команда выхода
Корневой режим (**ROOT**)		wlc-30> wlc-30#	exit end
Режим конфигурирования (**CONFIG**)	configure	wlc-30(config)#	exit
Режим отладки работы устройства (**DEBUG**)	debug	wlc-30(debug)#	exit

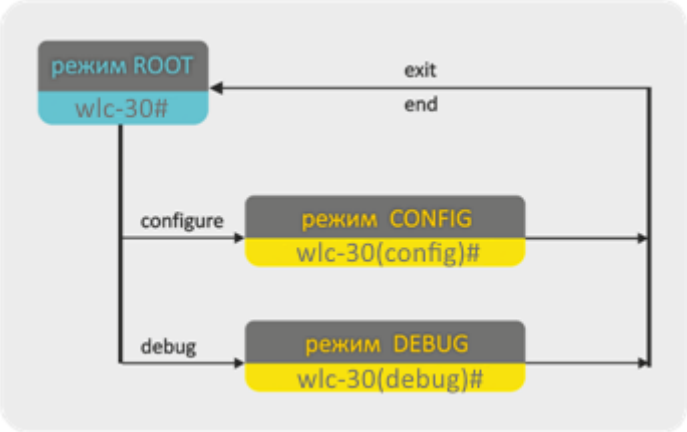

Рисунок 1 − Верхний уровень иерархии режимов команд

В корневом командном режиме (ROOT) осуществляется:

− работа с файлами конфигурации:

- применение;
- подтверждение;
- сброс;
- сохранение;
- отмена не примененных изменений;
- возврат к подтвержденной конфигурации.

− перезагрузка контроллера;

− мониторинг работы и просмотр текущей конфигурации устройства.

Из корневого режима (ROOT) осуществляется переход к следующим разделам:

– режим конфигурирования устройства (CONFIG);

– режим отладки работы устройства (DEBUG).

Конфигурирование контроллера

Конфигурирование контроллера выполняется в режиме **CONFIG**. Данный режим доступен из корневого режима (ROOT). Переход в режим конфигурирования осуществляется только в привилегированном режиме.

Для перехода из корневого режима (ROOT) необходимо выполнить следующие команды:

```
wlc-30> enable
wlc-30# configure
wlc-30(config)#
```

В режиме конфигурирования контроллера выполняется:

– управление системными часами;

– управление системным журналом;

– управление удаленным доступом;

– настройка QoS;

– настройка Spanning Tree;

– настройка VLAN;

– настройка статических маршрутов;

– настройка приоритетности протоколов маршрутизации;

– переход к режимам конфигурирования функций, описание режимов приведено в таблице 3.

Таблица 3 – Командные режимы для управления контроллером

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка глобальных параметров **(CONFIG)**	**configure**	wlc-30(config)#	ROOT
Настройка WLC **(CONFIG-WLC)**	**wlc**	wlc-30(config-wlc)#	CONFIG
Настройка локального RADIUS-сервера **(CONFIG-RADIUS)**	**radius-server local**	wlc-30(config-radius)#	CONFIG
Настройка NAS **(CONFIG-RADIUS-NAS)**	**config-radius-nas**	wlc-30(config-radius-nas)#	CONFIG-RADIUS
Настройка виртуального RADIUS-сервера **(CONFIG-RADIUS-VSERVER)**	**config-radius-vserver**	wlc-30(config-radius-vserver)#	CONFIG-RADIUS
Настройка виртуального RADIUS-сервера как используемого сервера **(CONFIG-RADIUS-SERVER)**	**config-radius-server**	wlc-30(config-radius-server)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка профиля AAA **(CONFIG-AAA-RADIUS-PROFILE)**	**config-aaa-radius-profile**	wlc-30(config-aaa-radius-profile)#	CONFIG
Настройка GigabitEthernet интерфейсов **(CONFIG-IF-GI)**	**interface gigabitethernet <PORT>**	wlc-30(config-if-gi)#	CONFIG
Настройка TengigabitEthernet интерфейсов **(CONFIG-IF-TE)**	**interface tengigabitethernet <PORT>**	wlc-30(config-if-te)#	CONFIG
Настройка группы агрегации каналов **(CONFIG-PORT-CHANNEL)**	**intrerface port-channel <CH>**	wlc-30(config-port-channel)#	CONFIG
Настройка сабинтерфейсов **(CONFIG-SUBIF)**	**interface gigabitethernet <PORT>.<VLAN> или** **interface tengigabitethernet <PORT>.<VLAN> или** **interface port-channel <CH>.<VLAN>**	wlc-30(config-subif)#	CONFIG
Настройка сабинтерфейсов **(CONFIG-QINQ-IF)**	**interface gigabitethernet <PORT>.<VLAN>.<VLAN> или** **interface tengigabitethernet <PORT>.<VLAN>.<VLAN> или** **interface port-channel <CH>.<VLAN>.<VLAN>**	wlc-30(config-qinq-if)#	CONFIG
Настройка виртуальных интерфейсов **(CONFIG-LOOPBACK)**	**interface loopback <PORT>**	wlc-30(config-loopback)#	CONFIG
Настройка E1-интерфейсов **(CONFIG-E1)**	**interface e1 <PORT>**	wlc-30(config-e1)#	CONFIG
Настройка группы агрегации E1-каналов **(CONFIG-MULTILINK)**	**interface multilink <PORT>**	wlc-30(config-multilink)#	CONFIG
Настройка виртуальных туннельных интерфейсов VTI **(CONFIG-VTI)**	**tunnel vti <VTI>**	wlc-30(config-vti)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка L2TPv3-туннелей **(CONFIG-L2TPV3)**	**tunnel l2tpv3 <L2TPV3>**	wlc-30(config-l2tpv3)#	CONFIG
Настройка GRE-туннелей **(CONFIG-GRE)**	**tunnel gre <GRE>**	wlc-30(config-gre)#	CONFIG
Настройка SoftGRE-туннелей **(CONFIG-SOFTGRE)**	**tunnel softgre <SOFTGRE>**	wlc-30(config-softgre)#	CONFIG
Настройка логических туннелей **(CONFIG-LT)**	**tunnel lt <LT>**	wlc-30(config-lt)#	CONFIG
Настройка сабинтерфейса на L2-туннеле **(CONFIG-SUBTUNNEL)**	**tunnel softgre <GRE>.<VLAN>**	wlc-30(config-subtunnel)#	CONFIG
Настройка IPv4-over-IPv4 туннелей **(CONFIG-IP4IP4)**	**tunnel ip4ip4 <IP4IP4>**	wlc-30(config-ip4ip4)#	CONFIG
Настройка сетевых мостов **(CONFIG-BRIDGE)**	**bridge <BRIDGE>**	wlc-30(config-bridge)#	CONFIG
Настройка VLAN **(CONFIG-VLAN)**	**vlan <VLAN>**	wlc-30(config-vlan)#	CONFIG
Настройка сетевой политики для определения VLAN по LLDPDU-сообщениям клиента **(CONFIG-NET-POLICY)**	**network-policy <NAME>**	wlc-30(config-net-policy)	CONFIG
Настройка пула адресов DHCP-сервера **(CONFIG-DHCP-SERVER)**	**ip dhcp-server pool <NAME>**	wlc-30(config-dhcp-server)#	CONFIG
Настройка DHCP опции 43 **(CONFIG-IP-DHCP-SERVER-VENDOR-SPECIFIC)**	**vendor-specific**	wlc-30(config-dhcp-server-vendor-specific)#	CONFIG-DHCP-SERVER

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка DHCP опции 60 **(CONFIG-DHCP-VENDOR-ID)**	**ip dhcp-server vendor-class-id <NAME>**	wlc-30(config-dhcp-vendor-id)#	CONFIG
Настройка пула адресов DHCP-сервера **(CONFIG-IPV6-DHCP-SERVER)**	**ipv6 dhcp-server pool <NAME>**	wlc-30(config-ipv6-dhcp-server)#	CONFIG
Настройка DHCP опции 60 **(CONFIG-IPV6-DHCP-VENDOR-ID)**	**ipv6 dhcp-server vendor-class-id <NAME>**	wlc-30(config-dhcp-vendor-id)#	CONFIG
Настройка резервирования DHCP-сервера **(CONFIG-DHCP-SERVER-FAILOVER)**	**ip dhcp-server failover [vrf <VRF>]**	wlc-30(config-dhcp-server-failover)#	CONFIG
Настройка профиля приложений **(CONFIG-OBJECT-GROUP-APPLICATION)**	**object-group application <NAME>**	wlc-30(config-object-group-application)#	CONFIG
Настройка профиля IP-адресов **(CONFIG-OBJECT-GROUP-NETWORK)**	**object-group network <NAME>**	wlc-30(config-object-group-network)#	CONFIG
Настройка профиля связок IP-адресов и TCP/UDP-портов **(CONFIG-OBJECT-GROUP-ADDRESS-PORT)**	**object-group address-port <NAME>**	wlc-30(config-object-group-address-port)#	CONFIG
Настройка профиля TCP/UDP-портов **(CONFIG-OBJECT-GROUP-SERVICE)**	**object-group service <NAME>**	wlc-30(config-object-group-service)#	CONFIG
Настройка профиля URL **(CONFIG-OBJECT-GROUP-URL)**	**object-group url <NAME>**	wlc-30(config-object-group-url)#	CONFIG
Настройка поставщика категорий контентной фильтрации **(CONFIG-OBJECT-GROUP-CONTENT-FILTER)**	**object-group content-filter <NAME>**	wlc-30(config-object-group-content-filter)#	CONFIG
Настройка профиля категорий контентной фильтрации от вендора Kaspersky Laboratory **(CONFIG-OBJECT-GROUP-CF-KASPERSKY)**	**vendor <VENDOR>**	wlc-30(config-object-group-cf-kaspersky)#	CONFIG-OBJECT-GROUP-CONTENT-FILTER

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка профиля почтовых доменов и адресов почтовых ящиков **(CONFIG-OBJECT-GROUP-MAIL)**	**object-group email <NAME>**	wlc-30(config-object-group-email)#	CONFIG
Настройка профиля XAUTH **(CONFIG-ACCESS-PROFILE)**	**access profile <NAME>**	wlc-30(config-access-profile)#	CONFIG
Настройка пула IP-адресов **(CONFIG-POOL)**	**address-assignment pool <NAME>**	wlc-30(config-pool)#	CONFIG
Настройка шлюза протокола IKE **(CONFIG-IKE-GATEWAY)**	**security ike gateway <NAME>**	wlc-30(config-ike-gw)#	CONFIG
Настройка политики протокола IKE **(CONFIG-IKE-POLICY)**	**security ike policy <NAME>**	wlc-30(config-ike-policy)#	CONFIG
Настройка профиля протокола IKE **(CONFIG-IKE-PROPOSAL)**	**security ike proposal <NAME>**	wlc-30(config-ike-proposal)#	CONFIG
Настройка политики набора протоколов IPsec **(CONFIG-IPSEC-POLICY)**	**security ipsec policy <NAME>**	wlc-30(config-ipsec-policy)#	CONFIG
Настройка профиля набора протоколов IPsec **(CONFIG-IPSEC-PROPOSAL)**	**security ipsec proposal <NAME>**	wlc-30(config-ipsec-proposal)#	CONFIG
Настройка VPN на основе набора протоколов IPsec **(CONFIG-IPSEC-VPN)**	**security ipsec vpn <NAME>**	wlc-30(config-ipsec-vpn)#	CONFIG
Настройка списка контроля доступа **(CONFIG-ACL)**	**ip access-list extended <NAME>**	wlc-30(config-acl)#	CONFIG
Настройка правила для списка контроля доступа **(CONFIG-ACL-RULE)**	**rule <ORDER>**	wlc-30(config-acl-rule)#	CONFIG-ACL

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка зоны безопасности **(CONFIG-ZONE)**	**security zone <NAME>**	wlc-30(config-zone)#	CONFIG
Настройка группы правил для пар зон безопасности **(CONFIG-ZONE-PAIR)**	**security zone-pair <FROM> <TO>**	wlc-30(config-zone-pair)#	CONFIG
Настройка правила для пары зон безопасности **(CONFIG-ZONE-PAIR-RULE)**	**rule <ORDER>**	wlc-30(config-zone-rule)#	CONFIG-ZONE-PAIR
Настройка сервиса трансляции адресов получателя **(CONFIG-DNAT)**	**nat destination**	wlc-30(config-dnat)#	CONFIG
Настройка пула IP-адресов и TCP/UDP-портов для DNAT **(CONFIG-DNAT-POOL)**	**pool <NAME>**	wlc-30(config-dnat-pool)#	CONFIG-DNAT
Настройка группы правил для DNAT **(CONFIG-DNAT-RULESET)**	**ruleset <NAME>**	wlc-30(config-dnat-ruleset)#	CONFIG-DNAT
Настройка правила для DNAT **(CONFIG-DNAT-RULE)**	**rule <ORDER>**	wlc-30(config-dnat-rule)#	CONFIG-DNAT-RULESET
Настройка сервиса трансляции адресов отправителя **(CONFIG-SNAT)**	**nat source**	wlc-30(config-snat)#	CONFIG
Настройка пула IP-адресов и TCP/UDP-портов для SNAT **(CONFIG-SNAT-POOL)**	**pool <NAME>**	wlc-30(config-snat-pool)#	CONFIG-SNAT
Настройка группы правил для SNAT **(CONFIG-SNAT-RULESET)**	**ruleset <NAME>**	wlc-30(config-snat-ruleset)#	CONFIG-SNAT
Настройка правила для SNAT **(CONFIG-SNAT-RULE)**	**rule <ORDER>**	wlc-30(config-snat-rule)#	CONFIG-SNAT-RULESET

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка пользователей системы **(CONFIG-USER)**	**username <NAME>**	wlc-30(config-user)#	CONFIG
Настройка локальной консоли **(CONFIG-LINE-CONSOLE)**	**line console**	wlc-30(config-line-console)#	CONFIG
Настройка удаленной консоли **(CONFIG-LINE-TELNET)**	**line telnet**	wlc-30(config-line-telnet)#	CONFIG
Настройка защищенной удаленной консоли **(CONFIG-LINE-SSH)**	**line ssh**	wlc-30(config-line-ssh)#	CONFIG
Настройка TACACS-сервера **(CONFIG-TACACS-SERVER)**	**tacacs-server host <ADDR>**	wlc-30(config-tacacs-server)#	CONFIG
Настройка RADIUS-сервера **(CONFIG-RADIUS-SERVER)**	**radius-server host <ADDR>**	wlc-30(config-radius-server)#	CONFIG
Настройка профиля RADIUS-серверов **(CONFIG-RADIUS-SERVER-PROFILE)**	**aaa radius-profile <NAME>**	wlc-30(config-aaa-radius-profile)#	CONFIG
Настройка DAS-сервера **(CONFIG-DAS-SERVER)**	**das-server <NAME>**	wlc-30(config-das-server)#	CONFIG
Настройка профиля DAS-серверов **(CONFIG-DAS-SERVER-PROFILE)**	**aaa das-profile <NAME>**	wlc-30(config-aaa-das-profile)#	CONFIG
Настройка LDAP-сервера **(CONFIG-LDAP-SERVER)**	**ldap-server host <ADDR>**	wlc-30(config-ldap-server)#	CONFIG
Настройка сервера для удаленного доступа по протоколу PPTP **(CONFIG-PPTP-SERVER)**	**remote-access pptp <NAME>**	wlc-30(config-pptp-server)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка пользователей для удаленного доступа по протоколу PPTP **(CONFIG-PPTP-USER)**	**username <NAME>**	wlc-30(config-pptp-user)#	CONFIG-PPTP
Настройка сервера для удаленного доступа по протоколу L2TP **(CONFIG-L2TP-SERVER)**	**remote-access l2tp <NAME>**	wlc-30(config-l2tp-server)#	CONFIG
Настройка пользователей для удаленного доступа по протоколу L2TP **(CONFIG-L2TP-USER)**	**username <NAME>**	wlc-30(config-l2tp-user)#	CONFIG-L2TP-SERVER
Настройка сервера для удаленного доступа по протоколу OpenVPN **(CONFIG-OPENVPN-SERVER)**	**remote-access openvpn <NAME>**	wlc-30(config-openvpn-server)#	CONFIG
Настройка пользователей для удаленного доступа по протоколу L2TP **(CONFIG-OPENVPN-USER)**	**username <NAME>**	wlc-30(config-openvpn-user)#	CONFIG-OPENVPN-SERVER
Настройка клиента удаленного доступа по протоколу PPTP **(CONFIG-PPTP)**	**tunnel pptp <PPTP-ID>**	wlc-30(config-pptp)#	CONFIG
Настройка клиента удаленного доступа по протоколу PPPOE **(CONFIG-PPPOE)**	**tunnel pppoe <PPPOE-ID>**	wlc-30(config-pppoe)#	CONFIG
Настройка клиента удаленного подключения по протоколу L2TP **(CONFIG-L2TP)**	**tunnel l2tp <L2TP-ID>**	wlc-30(config-l2tp)#	CONFIG
Настройка клиента удаленного подключения по протоколу OpenVPN **(CONFIG-OPENVPN)**	**tunnel openvpn <OPENVPN-ID>**	wlc-30(config-openvpn)#	CONFIG
Настройка SNMP-пользователя **(CONFIG-SNMP-USER)**	**snmp-server <NAME>**	wlc-30(config-snmp-user)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка NTP-сервера или пира **(CONFIG-NTP)**	**ntp server <ADDR>** **ntp peer <ADDR>**	wlc-30(config-ntp)#	CONFIG
Настройка BGP-процесса **(CONFIG-BGP)**	**router bgp <AS>**	wlc-30(config-bgp)#	CONFIG
Настройка BGP-процесса в vrf **(CONFIG-BGP-VRF)**	**vrf <VRF>**	wlc-30(config-bgp-vrf)#	CONFIG-BGP
Настройка IPv4/IPv6 адресации BGP-процесса **(CONFIG-BGP-FAMILY)**	**address-family { ipv4 | ipv6 } unicast**	wlc-30(config-bgp-af)#	CONFIG-BGP
Настройка IPv4/IPv6 адресации BGP-процесса в vrf **(CONFIG-BGP-VRF-FAMILY)**	**address-family { ipv4 | ipv6 } unicast**	wlc-30(config-bgp-vrf-af)#	CONFIG-BGP-VRF
Настройка группирования BGP-соседей **(CONFIG-BGP-GROUP)**	**peer-group <NAME>**	wlc-30(config-bgp-group)#	CONFIG-BGP
Настройка группирования BGP-соседей в vrf **(CONFIG-BGP-VRF-GROUP)**	**peer-group <NAME>**	wlc-30(config-bgp-vrf-group)#	CONFIG-BGP-VRF
Настройка соседа BGP-процесса **(CONFIG-BGP-NEIGHBOR)**	**neighbor { <ADDR> | <IPV6-ADDR> }**	wlc-30(config-bgp-neighbor)#	CONFIG-BGP
Настройка соседа BGP-процесса в vrf **(CONFIG-BGP-VRF-NEIGHBOR)**	**neighbor { <ADDR> | <IPV6-ADDR> }**	wlc-30(config-bgp-vrf-neighbor)#	CONFIG-BGP-VRF
Настройка IPv4/IPv6 адресации BGP-соседа **(CONFIG-BGP-NEIGHBOR-FAMILY)**	**address-family { ipv4 | ipv6 | vpnv4 } unicast**	wlc-30(config-bgp-neighbor-af)#	CONFIG-BGP-NEIGHBOR
Настройка IPv4/IPv6 адресации BGP-соседа в vrf **(CONFIG-BGP-NEIGHBOR-FAMILY)**	**address-family { ipv4 | ipv6 | vpnv4 } unicast**	wlc-30(config-bgp-neighbor-af-vrf)#	CONFIG-BGP-VRF-NEIGHBOR

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка списка подсетей **(CONFIG-PL)**	**ip prefix-list <NAME>**	wlc-30(config-pl)#	CONFIG
Настройка списка подсетей **(CONFIG-IPV6-PL)**	**ipv6 prefix-list <NAME>**	wlc-30(config-ipv6-pl)#	CONFIG
Настройка маршрутной карты **(CONFIG-ROUTE-MAP)**	**route-map <NAME>**	wlc-30(config-route-map)#	CONFIG
Настройка правила маршрутной карты **(CONFIG-ROUTE-MAP-RULE)**	**rule <ORDER>**	wlc-30(config-route-map-rule)#	CONFIG-ROUTE-MAP
Настройка RIP-протокола **(CONFIG-RIP)**	**router rip**	wlc-30(config-rip)#	CONFIG
Настройка RIPNG-протокола **(CONFIG-RIPNG)**	**ipv6 router rip**	wlc-30(config-ripng)#	CONFIG
Настройка IS-IS-процесса **(CONFIG-ISIS)**	**router isis <ID>**	wlc-30(config-isis)#	CONFIG
Настройка OSPF-процесса **(CONFIG-OSPF)**	**router ospf <ID>**	wlc-30(config-ospf)#	CONFIG
Настройка OSPF-области **(CONFIG-OSPF-AREA)**	**area <ID>**	wlc-30(config-ospf-area)#	CONFIG-OSPF
Настройка виртуального соединения OSPF **(CONFIG-OSPF-VLINK)**	**virtual-link <ID>**	wlc-30(config-ospf-vlink)#	CONFIG-OSPF-AREA
Настройка OSPFv3-процесса **(CONFIG-OSPFV3)**	**ipv6 router ospf <ID>**	wlc-30(config-ipv6-ospf)#	CONFIG
Настройка OSPFv3-области **(CONFIG-OSPFV3- AREA)**	**area <ID>**	wlc-30(config-ipv6-ospf-area)#	CONFIG-OSPFV3

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка виртуального соединения OSPFv3 **(CONFIG-OSPFV3-VLINK)**	**virtual-link <ID>**	wlc-30(config-ipv6-ospf-vlink)#	CONFIG-OSPFV3-AREA
Настройка ISIS-процесса **(CONFIG-ISIS)**	**router isis <ID>**	wlc-30(config-isis)#	CONFIG
Настройка списка ключей **(CONFIG-KEYCHAIN)**	**key-chain <KEYCHAIN>**	wlc-30(config-keychain)#	CONFIG
Настройка ключа **(CONFIG-KEYCHAIN-KEY)**	**key <ID>**	wlc-30(config-keychain-key)#	CONFIG-KEYCHAIN
Настройка параметров MSTP **(CONFIG-MST)**	**spanning-tree mst configuration**	wlc-30(config-mst)#	CONFIG
Настройка правил WAN **(CONFIG-WAN-RULE)**	**wan load-balance rule <ID>**	wlc-30(config-wan-rule)#	CONFIG
Настройка правил WAN (IPv6) **(CONFIG-IPV6-WAN-RULE)**	**Ipv6 wan load-balance rule <ID>**	wlc-30(config-ipv6-wan-rule)#	CONFIG
Настройка target-листов **(CONFIG-TARGET-LIST)**	**wan load-balance target-list <NAME>**	wlc-30(config-target-list)#	CONFIG
Настройка target-листов (IPv6) **(CONFIG-IPV6-TARGET-LIST)**	**Ipv6 wan load-balance target-list <NAME>**	wlc-30(config-ipv6-target-list)#	CONFIG
Настройка target **(CONFIG-WAN-TARGET)**	**target <ID>**	wlc-30(config-wan-target)#	CONFIG-TARGET-LIST
Настройка target (IPv6) **(CONFIG-IPV6-WAN-TARGET)**	**target <ID>**	wlc-30(config-ipv6-wan-target)#	CONFIG-IPV6-TARGET-LIST
Настройка объектов отслеживания событий **(CONFIG-TRACK)**	**track <ID>**	wlc-30(config-track)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка Wi-Fi Controller **(CONFIG-WIRELESS)**	**wireless-controller**	wlc-30(config-wireless)#	CONFIG
Настройка VRF **(CONFIG-VRF)**	**ip vrf <NAME>**	wlc-30(config-vrf)#	CONFIG
Настройка политики QoS **(CONFIG-POLICY-MAP)**	**policy-map <NAME>**	wlc-30(config-policy-map)#	CONFIG
Настройка класса QoS **(CONFIG-CLASS-MAP)**	**class-map <NAME>**	wlc-30(config-class-map)#	CONFIG
Настройка класса внутри политики QoS **(CONFIG-POLICY-MAP-CLASS)**	**class <NAME>**	wlc-30(config-class-policy-map)#	CONFIG
Настройка PPP-пользователя для аутентификации удаленной стороны **(CONFIG-PPP-USER)**	**ppp chap username <NAME>**	wlc-30(config-ppp-user)#	CONFIG-E1
	ppp chap username <NAME>		CONFIG-MULTILINK
	user <NAME>		CONFIG-CELLULAR-PROFILE
	user <NAME>		CONFIG-ACCESS-PROFILE
	username <NAME>		CONFIG-L2TP-SERVER
	username <NAME>		CONFIG-PPTP-SERVER
Настройка параметров резервирования конфигурации **(CONFIG-ARCHIVE)**	**archive**	wlc-30(config-archive)#	CONFIG
Настройка сервера сбора статистики Netflow **(CONFIG-NETFLOW-HOST)**	**netflow collector <ADDR>**	wlc-30(config-netflow-host)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка сервера сбора статистики sFlow **(CONFIG-SFLOW-HOST)**	**sflow collector <ADDR>**	wlc-30(config-sflow-host)#	CONFIG
Настройка сервера получения уведомлений SNMP **(CONFIG-SNMP-HOST)**	**snmp-server host <ADDR>**	wlc-30(config-snmp-host)#	CONFIG
Изменение пароля после истечения срока действия **(CHANGE-EXPIRED-PASSWORD)**	**-**	wlc-30(change-expired-password)#	-
Настройка профиля фильтрации http-запросов **(CONFIG-PROFILE)**	**ip http profile <NAME>**	wlc-30(config-profile)	CONFIG
Настройка общих параметров MPLS **(CONFIG-MPLS)**	**mpls**	wlc-30(config-mpls)#	CONFIG
Настройка общих параметров LDP **(CONFIG-LDP)**	**ldp**	wlc-30(config-ldp)#	CONFIG
Настройка IPv4-адресации протокола LDP **(CONFIG-LDP-AF-IPV4)**	**address-family ipv4**	wlc-30(config-ldp-af-ipv4)#	CONFIG-LDP
Настройка LDP-unicast-соседства **(CONFIG-LDP-NEIGH)**	**neighbor <ADDR>**	wlc-30(config-ldp-neig)#	CONFIG-LDP
Настройка IPv4-адресации протокола LDP для отдельного ip-интерфейса **(CONFIG-LDP-AF-IPV4-IF)**	**interface <IF>**	wlc-30(config-ldp-af-ipv4-if)#	CONFIG-LDP-AF-IPV4
Создание L2-MPLS-туннелей **(CONFIG-L2VPN)**	**l2vpn**	wlc-30(config-l2vpn)#	CONFIG-MPLS

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка L2-MPLS-туннеля **(CONFIG-L2VPN-EOMPLS)**	**vpls <NAME>** **p2p <NAME>**	wlc-30(config-l2vpn-vpls)# wlc-30(config-l2vpn-p2p)#	CONFIG-L2VPN
Настройка PW-class (шаблона pseudo-wire) **(CONFIG-L2VPN-PW-CLASS)**	**pw-class <WORD>**	wlc-30(config-l2vpn-pw-class)#	CONFIG-L2VPN
Настройка параметров pseudo-wire L2-MPLS-туннеля **(CONFIG-L2VPN-PW)**	**pw <PW_ID> <LSR_ID> [<NEIGH_ADDR>]**	wlc-30(config-l2vpn-pw)#	CONFIG-L2VPN-EOMPLS
Настройка BGP auto-discovery and singnaling **(CONFIG-AUTODISCOVERY-BGP)**	**autodiscovery bgp**	wlc-30(config-bgp)#	CONFIG-L2VPN-EOMPLS
Настройка политики IPS/IDS **(CONFIG-IPS-POLICY)**	**security ips policy <NAME>**	wlc-30(config-ips-policy)#	CONFIG
Настройка поставщика правил IPS/IDS **(CONFIG-IPS-VENDOR)**	**vendor <VENDOR>**	wlc-30(config-ips-vendor)#	CONFIG-IPS-POLICY
Настройка категорий правил IPS/IDS **(CONFIG-IPS-VENDOR-CATEGORY)**	**category <CATEGORY>**	wlc-30(config-ips-vendor-category)#	CONFIG-IPS-VENDOR
Настройка сервиса IPS/IDS **(CONFIG-IPS)**	**security ips**	wlc-30(config-ips)#	CONFIG
Настройка источника обновления правил IPS/IDS, распространяемых по коммерческой лицензии **(CONFIG-CONTENT-PROVIDER)**	**content-provider**	wlc-30(config-content-provider)#	CONFIG
Настройка автообновления правил IPS/IDS из внешних источников **(CONFIG-IPS-AUTO-UPGRADE)**	**auto-upgrade**	wlc-30(config-ips-auto-upgrade)#	CONFIG-IPS

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка пользовательского сервера обновлений правил IPS/IDS **(CONFIG-IPS-UPGRADE-USER-SERVER)**	**user-server <WORD>**	wlc-30(config-ips-upgrade-user-server)#	CONFIG-IPS-AUTO-UPGRADE
Настройка категорий пользовательских правил IPS/IDS **(CONFIG-IPS-CATEGORY)**	**security ips-category user-defined <CATEGORY_NAME>**	wlc-30(config-ips-category)#	CONFIG
Настройка пользовательских правил IPS/IDS **(CONFIG-IPS-CATEGORY-RULE)**	**rule <ORDER>**	wlc-30(config-ips-category-rule)#	CONFIG-IPS-CATEGORY
Настройка расширенных пользовательских правил IPS/IDS **(CONFIG-IPS-CATEGORY-RULE-ADVANCED)**	**rule-advanced <ORDER>**	wlc-30(config-ips-category-rule-advanced)#	CONFIG-IPS-CATEGORY
Настройка параметров работы zabbix-agent **(CONFIG-ZABBIX-AGENT)**	**zabbix-agent**	wlc-30(config-zabbix-agent)#	CONFIG
Настройка параметров работы zabbix-proxy **(CONFIG-ZABBIX-PROXY)**	**zabbix-proxy**	wlc-30(config-zabbix-proxy)#	CONFIG
Настройка профиля сервиса «Антиспам» **CONFIG-ANTISPAM-PROFILE**	**security antispam profile <NAME>**	wlc-30(config-antispam-profile)#	CONFIG
Настройка правила для профиля сервиса «Антиспам» **CONFIG-ANTISPAM-PROFILE-RULE**	**rule <ORDER>**	wlc-30(config-antispam-profile-rule)#	CONFIG
Настройка почтового домена **CONFIG-MAILSERVER-DOMAIN**	**mailserver domain <NAME>**	wlc-30(config-mailserver-domain)#	CONFIG
Настройка почтового сервера **CONFIG-MAILSERVER**	**mailserver**	wlc-30(config-mailserver)#	CONFIG

Уровень	Команда входа [1]	Вид строки подсказки	Предыдущий уровень
Настройка локального syslog-файла **CONFIG-SYSLOG-FILE**	**syslog file { flash:syslog/<NAME> | tmpsys:syslog/<NAME> }**	(config-syslog-file)	CONFIG
Настройка удаленного syslog-сервера **CONFIG-SYSLOG-HOST**	**syslog host <HOSTNAME>**	(config-syslog-host)	CONFIG

[1] Подробное описание команд приведено ниже.

Типы и порядок именования интерфейсов контроллера

При работе контроллера используются сетевые интерфейсы различного типа и назначения. Система именования позволяет однозначно адресовать интерфейсы по их функциональному назначению и местоположению в системе. Далее в таблице приведен перечень типов интерфейсов.

Таблица 4 – Типы и порядок именования интерфейсов контроллера

Тип интерфейса	Обозначение
Физические интерфейсы	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор физических интерфейсов имеет вид **<UNIT>/<SLOT>/<PORT>**, где • **<UNIT>** – номер устройства в группе устройств, • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта.
Порты 1 Гбит/с	**gigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **gigabitethernet 1/0/12** Допускается использовать сокращенное наименование, например gi1/0/12.
Порты 10 Гбит/с	**tengigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **tengigabitethernet 1/0/2** Допускается использовать сокращенное наименование, например te1/0/2.

Тип интерфейса	Обозначение
Группы агрегации каналов	Обозначение группы агрегации каналов включает в себя его тип и порядковый номер интерфейса: **port-channel <CHANNEL_ID>** Пример обозначения: **port-channel 6** ⚠ Допускается использовать сокращенное наименование, например, po1.
Сабинтерфейсы	Обозначение сабинтерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) сабинтерфейса, разделенных точкой. Примеры обозначений: **gigabitethernet 1/0/12.100** **tengigabitethernet 1/0/2.123** **port-channel 1.6** ⚠ Идентификатор сабинтерфейса может принимать значения [1..4094].
Q-in-Q интерфейсы	Обозначение Q-in-Q интерфейса образуется из обозначения базового интерфейса, идентификатора сервисного VLAN и идентификатора пользовательского VLAN, разделенных точкой. Примеры обозначений: **gigabitethernet 1/0/12.100.10** **tengigabitethernet 1/0/2.45.12** **port-channel 1.6.34** ⚠ Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].
E1-интерфейсы	Обозначение E1-интерфейса включает в себя его тип и идентификатор. Идентификатор E1-интерфейсов имеет вид **< UNIT>/< SLOT>/< STREAM>**, где • **<UNIT>** – номер устройства в группе устройств [1..1], • **<SLOT>** – номер E1-модуля в составе устройства [0..12], • **<STREAM>** – порядковый номер E1-потока [1..1]. Пример обозначения: **e1 1/0/1**
Группы агрегации E1-каналов	Обозначение группы агрегации E1-каналов включает в себя его тип и порядковый номер интерфейса: **multilink <CHANNEL_ID>** Пример обозначения: **multilink 3**

Тип интерфейса	Обозначение
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: **loopback 4** **bridge 60** **service-port 1**
USB-модемы	Обозначение USB-модема включает в себя его тип и порядковый номер: **modem <MODEM-NUM>** Пример обозначения: **modem 1**

1. **Текущая версия ПО не поддерживает стекирование устройств. Номер устройства в группе устройств unit может принимать только значение 1.**
2. **Некоторые команды поддерживают одновременную работу с группой интерфейсов. Для указания группы интерфейсов может быть использовано перечисление через запятую или указание диапазона идентификаторов через дефис «-».**

Примеры указания групп интерфейсов:

```
interface gigabitethernet 1/0/1, gigabitethernet 1/0/5
interface tengigabitethernet 1/0/1-2
interface gi1/0/1-3,gi1/0/7,te1/0/1
```

Типы и порядок именования туннелей контроллера

При работе контроллера используются сетевые туннели различного типа и назначения. Система именования позволяет однозначно адресовать туннели по их функциональному назначению. Далее в таблице приведен перечень типов туннелей.

Таблица 5 – Типы и порядок именования туннелей контроллера

Тип туннеля	Обозначение
L2TP-туннель	Обозначение L2TP-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tp <L2TP_ID>** Пример обозначения: **l2tp 1**
L2TPv3-туннель	Обозначение L2TPv3-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tpv3 <L2TPV3_ID>** Пример обозначения: **l2tpv3 1**
GRE-туннель	Обозначение GRE-туннеля состоит из обозначения типа и порядкового номера туннеля: **gre <GRE_ID>** Пример обозначения: **gre 1**
GRE-сабтуннель	Обозначение GRE-сабтуннеля состоит из обозначения типа, порядкового номера туннеля и идентификатора VLAN для сабтуннеля: **gre <GRE_ID>.<VLAN_ID>** Пример обозначения: **gre 1.200**
SoftGRE-туннель	Обозначение SoftGRE-туннеля состоит из обозначения типа, порядкового номера туннеля и, опционально, VLAN ID виртуального интерфейса: **softgre <GRE_ID>[.<VLAN>]** Примеры обозначения: **softgre 1, softgre 1.10**
IPv4-over-IPv4-туннель	Обозначение IPv4-over-IPv4-туннеля состоит из обозначения типа и порядкового номера туннеля: **ip4ip4 <IPIP_ID>** Пример обозначения: **ip4ip4 1**
IPsec-туннель	Обозначение виртуального IPsec-туннеля состоит из обозначения типа и порядкового номера туннеля: **vti <VTI_ID>** Пример обозначения: **vti 1**

Тип туннеля	Обозначение
Логический туннель (туннель между VRF)	Обозначение логического туннеля состоит из обозначения типа и порядкового номера туннеля: **lt <LT_ID>** Пример обозначения: **lt 1**
PPPoE-туннель	Обозначение PPPoE-туннеля состоит из обозначения типа и порядкового номера туннеля: **pppoe <PPPoE_ID>** Пример обозначения: **pppoe 1**
PPTP-туннель	Обозначение PPPTP-туннеля состоит из обозначения типа и порядкового номера туннеля: **pptp <PPTP_ID>** Пример обозначения: **pptp 1**

5 Команды пользовательского интерфейса

- alarm
- clear alarms
- clear ssh host
- clear storage-device
- configure
- do
- end
- exit
- help
- history size
- logout
- monitor
- ping
- reload system
- show alarms brief
- show alarms brief active
- show alarm settings
- show history
- ssh
- telnet
- terminal datadump
- terminal resize
- traceroute
- uptime
- verify
- verify filesystem
- verify storage-device

alarm

Данной командой устанавливаются значения порогов аварий.

Синтаксис

```
alarm { facility <FACILITY-ALARMS> | memory <MEMORY-ALARMS> | process <PROCESS-ALARMS> } <VALUE>
```

```
no alarm { facility <FACILITY-ALARMS> | memory <MEMORY-ALARMS> | process <PROCESS-ALARMS> } <VALUE>
```

Параметры

<FACILITY-ALARMS> – пороги аварий, связанных с окружением (скорость FAN, температура процессора и датчиков). Принимает следующие значения:

- fan-speed high – порог скорости вращения вентилятора, выраженный в процентах от максимальной скорости вращения (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvFanSpeedHigh (авария). Значение этого порога должно быть больше, чем alarm facility fan-speed low;
- fan-speed low – порог скорости вращения вентилятора, выраженный в процентах от максимальной скорости вращения (0..100), при переходе через который от больших значений к меньшим, генерируется SNMP trap eltexEnvFanSpeedHighOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm facility fan-speed high;
- temperature cpu critical high – порог температуры процессора, выраженный в градусах по шкале Цельсия (0..255), при переходе через который от меньших значений к большим, генерируется

SNMP trap eltexEnvTempCritical (авария). Значение этого порога должно быть самым большим из всех значений температурных порогов процессора;

- temperature cpu critical low – порог температуры процессора, выраженный в градусах по шкале Цельсия (0..255), при переходе через который от больших значений к меньшим, генерируется SNMP trap eltexEnvTempCriticalOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm facility temperature cpu critical high, но больше, чем alarm facility temperature cpu overheat high;
- temperature <sensor> overheat high – порог температуры сенсора, выраженный в градусах по шкале Цельсия (0..255), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvTempOverheat (авария). Значение этого порога должно быть меньше, чем alarm facility temperature <sensor> critical low, но больше, чем alarm facility temperature <sensor> overheat low;
- temperature <sensor> overheat low – порог температуры сенсора, выраженный в градусах по шкале Цельсия (0..255), при переходе через который от больших значений к меньшим, генерируется SNMP trap eltexEnvTempOverheatOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm facility temperature <sensor> overheat high;
- temperature <sensor> supercooling high – порог температуры сенсора, выраженный в градусах по шкале Цельсия (0..255), при переходе через противоположенное значение которого от меньших значений к большим, генерируется SNMP trap eltexEnvTempSupercoolingOk (нормализация аварии). Этот порог предназначен для задания отрицательных температур, и его значение должно быть меньше, чем alarm facility temperature <sensor> supercooling low;
- temperature <sensor> supercooling low – порог температуры сенсора, выраженный в градусах по шкале Цельсия (0..255), при переходе через противоположенное значение которого от больших значений к меньшим, генерируется SNMP trap eltexEnvTempSupercooling (авария). Этот порог предназначен для задания отрицательных температур, и его значение должно быть больше, чем alarm facility temperature <sensor> supercooling high;
  Поле сенсор может принимать значение: cpu.

<MEMORY-ALARMS> – пороги аварий, связанных с свободным пространством NAND и RAM. Принимает следующие значения:

- free low-watermark flash high – порог количества свободной flash-памяти, выраженной в процентах от максимального (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvMemoryLowOk (нормализация аварии). Значение этого порога должно быть самым большим из всех значений порогов количества свободной flash-памяти;
- free low-watermark flash low – порог количества свободной flash-памяти, выраженной в процентах от максимального (0..100), при переходе через который от больших значений к меньшим, генерируется SNMP trap eltexEnvMemoryLow (авария). Значение этого порога должно быть меньше, чем alarm memory free low-watermark flash high;
- free low-watermark ram high – порог количества свободной RAM-памяти, выраженной в процентах от максимального (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvMemoryLowOk (нормализация аварии). Значение этого порога должно быть самым большим из всех значений порогов количества свободной RAM-памяти;
- free low-watermark ram low – порог количества свободной RAM-памяти, выраженной в процентах от максимального (0..100), при переходе через который от больших значений количества к меньшим, генерируется SNMP trap eltexEnvMemoryLow (авария). Значение этого порога должно быть меньше, чем alarm memory free low-watermark ram high;
- reserve critical flash high – порог количества свободной flash-памяти, выраженной в процентах от максимального (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvMemoryCriticalLowOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm memory free low-watermark flash low, но больше, чем alarm memory reserve critical flash low;
- reserve critical flash low – порог количества свободной flash-памяти, выраженной в процентах от максимального (0..100), при переходе через который от больших значений количества к меньшим, генерируется SNMP trap eltexEnvMemoryCriticalLow (авария). Значение этого порога должно быть меньше, чем alarm memory reserve critical flash high;

- reserve critical ram high – порог количества свободной RAM-памяти, выраженной в процентах от максимального (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvMemoryCriticalLowOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm memory free low-watermark ram low, но больше, чем alarm memory reserve critical ram low;
- reserve critical ram low – порог количества свободной RAM-памяти, выраженной в процентах от максимального (0..100), при переходе через который от больших значений количества к меньшим, генерируется SNMP trap eltexEnvMemoryCriticalLow (авария). Значение этого порога должно быть меньше, чем alarm memory reserve critical ram high.

<PROCESS-ALARMS> – пороги аварий, связанных с загрузкой процессора. Принимает следующие значения:

- cpu threshold falling – порог утилизации CPU, выраженной в процентах от максимальной (0..100), при переходе через который от больших значений к меньшим, генерируется SNMP trap eltexEnvCpuLoadHighOk (нормализация аварии). Значение этого порога должно быть меньше, чем alarm process cpu threshold rising;
- cpu threshold rising – порог утилизации CPU, выраженной в процентах от максимальной (0..100), при переходе через который от меньших значений к большим, генерируется SNMP trap eltexEnvCpuLoadHigh (авария). Значение этого порога должно быть больше, чем alarm process cpu threshold falling.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# alarm facility fan-speed high 80
```

clear alarms

Данной командой осуществляется очистка записей об авариях.

Синтаксис

```
clear alarms { inactive | all }
```

Параметры

inactive – удаляются записи только о архивных авариях;

all – удаляются записи о архивных и активных авариях.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# clear alarms inactive
```

clear ssh host

Данной командой осуществляется сброс сохраненного SSH-ключа удаленного хоста.

Синтаксис

```
clear ssh host { <ADDR> | <IPV6-ADDR> }
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# clear ssh host 192.168.1.1
```

clear storage-device

Данной командой запускается форматирование подключенного носителя.

Синтаксис

```
clear storage-device { usb-dev://<ID> | usb://<USB-NAME> | mmc } <NAME>
```

Параметры

<ID> – номер подключенного USB-носителя по порядку;

<USB-NAME> – имя подключенного USB-носителя. Имя можно узнать в выводе команды show storage-devices;

mmc – ключ для проверки установленного mmc-носителя;

<NAME> – новое имя раздела, которое будет назначено после форматирования.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30-# clear storage-device usb://BC1E-2E16:/ SOFT
Formatting will erase all data on this device
Do you really want to continue? (y/N): y
Device clear success.
```

configure

Данная команда позволяет перейти в режим глобального конфигурирования.

Синтаксис

```
configure
configure terminal
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# configure
wlc-30(config)#
```

do

Команда do позволяет выполнять команды корневого режима (ROOT) из любого другого режима командного интерфейса.

Синтаксис

```
do <command>
```

Параметры

<command> – команда корневого режима.

Необходимый уровень привилегий

1

Командный режим

Все режимы, кроме корневого.

Пример:

```
wlc-30(config)# do show version
Boot version:
  1.0.7.16 (date 18/11/2015 time 13:40:59)
SW version:
  1.0.7 build 17[d9bdbda] (date 21/11/2015 time 18:06:41)
HW version:
  1v7
```

end

Команда служит для возврата в корневой командный режим (ROOT).

Синтаксис

`end`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

Все режимы, кроме корневого.

exit

Данная команда служит для возврата на уровень выше в иерархической системе командных режимов.

При выполнении данной команды в режиме ROOT завершается сеанс работы пользователя с интерфейсом командной строки CLI контроллера.

Синтаксис

`exit`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

Все режимы.

help

Данной командой на дисплей выводится информация о работе с командной строкой.

Синтаксис

```
help
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

Все режимы.

history size

Данной командой можно изменить максимальное число последних введенных команд пользователя, которые сохранятся в истории команд текущей сессии. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
history size <SIZE>
no history size
```

Параметры

<SIZE> – число последних введенных команд, принимает значения [10..1000].

Значение по умолчанию

50

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# history size 20
```

logout

Данной командой завершается сеанс работы пользователя с интерфейсом командной строки CLI.

Синтаксис

`logout`

Параметры

Команда не содержит параметров

Необходимый уровень привилегий

1

Командный режим

ROOT

CHANGE-EXPIRED-PASSWORD

Пример:

```
wlc-30# logout
```

monitor

Данной командой включается мониторинг трафика на сетевом интерфейсе в режиме реального времени попакетно.

Синтаксис

```
monitor { <IF> | <TUN> } [ protocol <TYPE> [ source-port <SRC-PORT> ] [ destination-port
<DST-PORT> ] [ port <PORT> ] ] [ source-address {<SRC-ADDR> | <SRC-IPV6-ADDR> } ]
[ destination-address { <DST-ADDR> | <DST-IPV6-ADDR> } ]
[address { <ADDR> | <IPV6-ADDR> } ] [ packets <VALUE> ] [ detailed ]
```

Параметры

<IF> – интерфейс или группа интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<SRC-ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<DST-ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-IPV6-ADDR> – IPv6-адрес отправителя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<DST-IPV6-ADDR> – IPv6-адрес получателя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<ADDR> – IP-адрес отправителя или получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес отправителя или получателя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<SRC-MAC> – mac-адрес отправителя ethernet-кадра, задается в виде HH:HH:HH:HH:HH:HH, где каждая HH-часть принимает значения в шестнадцатеричном формате [0..FF];

<DST-MAC> – mac-адрес получателя ethernet-кадра, задается в виде HH:HH:HH:HH:HH:HH, где каждая HH-часть принимает значения в шестнадцатеричном формате [0..FF];

<SRC-MAC> – mac-адрес отправителя или получателя ethernet-кадра, задается в виде HH:HH:HH:HH:HH:HH, где каждая HH-часть принимает значения в шестнадцатеричном формате [0..FF];

<TYPE> – тип протокола, принимает значения: tcp, udp, icmp, icmp6, igrp, igmp, arp, gre, ipip, esp, ah, eigrp, ospf, pim, vrrp, l2tp, RDP или номер протокола [0..255]**;**

<SRC-PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535];

<DST-PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535];

<PORT> – номер TCP/UDP-порта отправителя или получателя, принимает значения [1..65535];

<VALUE> – количество пакетов, после получения которых анализ будет остановлен, указывается в диапазоне [1…4294967295];

detailed – информация выдается в детализированном формате.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# monitor gigabitethernet 1/0/5 detailed
23:37:44.324049 d8:50:e6:d2:f0:46 > a8:f9:4b:aa:03:a5, ethertype IPv4 (0x0800), length 98: (tos
0x0, ttl
 64, id 50760, offset 0, flags [DF], proto ICMP (1), length 84)
    10.255.100.1 > 10.255.100.5: ICMP echo request, id 11730, seq 19, length 64
```

ping

Данная команда используется для проверки доступности указанного сетевого устройства.

Синтаксис

```
ping [ vrf <VRF>] { <ADDR> | <IPV6-ADDR> | <HOSTNAME> [ { ip | ipv6 } ] [ ttl <TTL> ]
[ packets <COUNT> |unlimited ] [ size <SIZE> ] [ timeout <TIMEOUT> ] [interval
```

```
<INTERVAL>] [ source { ip { <SRC-ADDR> | <SRC-IPV6-ADDR> }
| interface <IF> | tunnel <TUN> } ] [ data <HEX> ] [ dscp <DSCP> ] [ flood ] [detailed]
[ strategy <STRATEGY> ] [ nodeinfo <INFO> ] [ broadcast ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа;

<ADDR> – IP-адрес устройства, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес устройства, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<HOSTNAME> – DNS-имя устройства, задаётся строкой до 255 символов;

- ip – проверять доступность при помощи ipv4-пакетов;
- ipv6 – проверять доступность при помощи ipv6-пакетов.

<TTL> – время жизни IP-пакета, принимает значение [1..255], по умолчанию 64;

<COUNT> – количество передаваемых пакетов [1..4294967295], по умолчанию 5;

<SIZE> – размер icmp-пакета в байтах, принимает значение [1..65468], по умолчанию 56 байт, что соответствует 64 байтам после добавления заголовка ICMP и 84 байтам после добавления ip-заголовка;

<TIMEOUT> – время ожидания ответа, в секундах. Опция влияет на таймаут, если отсутствуют какие-либо ответы, в противном случае утилита ждет два RTTs. Принимает значение [1..60], по умолчанию 1 секунда;

<INTERVAL> – интервал между отправками icmp-пакетов в миллисекундах, принимает значение [200..60000], по умолчанию 1000;

<SRC-ADDR> – IP-адрес отправителя, в качестве данного адреса может использоваться любой IP-адрес контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-IPV6-ADDR> – IPv6-адрес отправителя, в качестве данного адреса может использоваться любой IPv6-адрес контроллера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<IF> – имя интерфейса контроллера, через который будут отправлены пакеты, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля маршрутизатора, через который будут отправлены пакеты, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<HEX> – шаблон данных, которым будет заполняться пакет, задаётся числом в шестнадцатеричной системе до 16 байт;

<DSCP> – DSCP-приоритет в соответствии с RFC 2474, принимает значение [0..63], значение по умолчанию 0;

flood – при указании данной команды пакеты будут отправляться с максимальной скоростью, ответы от устройства не отображаются до окончания выполнения команды;

broadcast – при указании данной команды будет разрешено отправлять пакеты на широковещательный адрес;

detailed – при указании данного ключа будет выводиться полная информация о icmp-ответах и общая статистика работы команды. Без указания – только статистика;

<STRATEGY> – стратегия фрагментации пакетов, принимает одно из следующих значений:

- allow-fragmentation – разрешить фрагментацию, не устанавливать флаг DF (don’t fragment);
- discovery-pmtu – выполнять изучение PMTU (Path MTU), фрагментировать локально, если размер пакета слишком большой;
- disallow-fragmentation – запретить фрагментацию, в том числе локальную.

<INFO> – только для IPv6. Отправка ICMPv6 Node Information Queries (RFC4620), вместо Echo Request принимает одно из следующих значений:

- name – запрос DNS имен(и) узла;
- ipv6 – запрос IPv6-адресов узла;
- ipv6-global – запрос глобальных IPv6-адресов узла;
- ipv6-sitelocal – запрос site-local IPv6-адресов узла;
- ipv6-linklocal – запрос link-local IPv6-адресов узла;
- ipv6-all – запрос unicast IPv6-адресов узла;
- ipv4 – запрос IP-адресов узла;
- ipv4-all – запрос IP-адресов со всех сетевых интерфейсов узла.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# ping 192.168.100.39 packets 5 size 1400 detailed
PING 192.168.100.39 (192.168.100.39) 1400(1428) bytes of data.
1408 bytes from 192.168.100.39: icmp_req=1 ttl=64 time=0.084 ms
1408 bytes from 192.168.100.39: icmp_req=2 ttl=64 time=0.053 ms
1408 bytes from 192.168.100.39: icmp_req=3 ttl=64 time=0.082 ms
1408 bytes from 192.168.100.39: icmp_req=4 ttl=64 time=0.051 ms
1408 bytes from 192.168.100.39: icmp_req=5 ttl=64 time=0.075 ms
--- 192.168.100.39 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.051/0.069/0.084/0.014 ms
wlc-30# ping ipv6 fc00::1
PING fc00::1(fc00::1) 56 data bytes
64 bytes from fc00::1: icmp_seq=1 ttl=64 time=0.379 ms
64 bytes from fc00::1: icmp_seq=2 ttl=64 time=0.161 ms
--- fc00::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.161/0.270/0.379/0.109 ms
```

reload system

Данной командой осуществляется перезагрузка устройства.

Синтаксис

```
reload system
```

Параметры

Команда не содержит параметров

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# reload system
```

show alarms brief

Данной командой выводится краткая история аварий на устройстве (активных и завершенных).

Синтаксис

`show alarms brief`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show alarms brief

   History Alarms
   ~~~~~~~~~~~~~~
Severity   Group         Set time            Clear time          Description
--------   ------        -----------         ------------        ------------------
major      environment   03/31/00 17:27:38   03/31/00 17:31:53   Reserve Power Supply Fault
```

show alarms brief active

Данной командой выводится краткая информация о текущих (активных) авариях на устройстве.

Синтаксис

`show alarms brief active`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show alarms brief active
   History Alarms
   ~~~~~~~~~~~~~~
Severity   Group          Set time             Clear time        Description
--------   -----------    -------------        -------------
-------------------------------------
notify     environment    03/31/00 16:47:05    -                 Reserve Power Supply removed
```

show alarm settings

Данной командой выводится информация о настройках порогов срабатывания аварий.

Синтаксис

```
show alarm settings <TYPE>
```

Параметры

<TYPE> – тип аварий:

- facility – пороги аварий, связанных с окружением (скорость FAN, температура процессора и датчиков);
- memory – пороги аварий, связанных с свободным пространством NAND и RAM;
- process – пороги аварий, связанных с загрузкой процессора.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show alarm facility
    fan-speed:
        high:                   80
        low:                    75
    temperature CPU:
        critical high:          95
        critical low:           92
        overheat high:          80
        overheat low:           78
        supercooling high:      -12
        supercooling low:       -15
    temperature sensor1:
        overheat high:          60
        overheat low:           57
        supercooling high:      -12
        supercooling low:       -15
    temperature sensor2:
        overheat high:          60
        overheat low:           57
        supercooling high:      -12
        supercooling low:       -15
    temperature sensor3:
        overheat high:          60
        overheat low:           57
        supercooling high:      -12
        supercooling low:       -15
```

show history

Данной командой на дисплей выводится информация о командах, которые использовались в текущей сессии или о количестве сохраняемых команд.

Синтаксис

```
show history [size | <NUM> ]
```

Параметры

size – максимальное число последних введенных команд пользователя, которые сохранятся в истории команд текущей сессии;

<NUM> – количество последних введенных команд пользователя, которые необходимо отобразить [0..100].

Значение по умолчанию

0. Соответствует выводу всей истории введенных команд.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show history
    1  enable
    2  show history
    3  configure
    4  service nat
    5  service nat source
    6  exit
    7  show history
```

ssh

Данная команда используется для подключения к удаленному узлу по протоколу SSH.

Синтаксис

```
ssh [ vrf <VRF>] <USERNAME> { <ADDR> | <IPV6-ADDR> | <HOSTNAME> } [ port <PORT> ]
[ version <VERSION> ] [ source { <SRC-ADDR> | <SRC-IPV6-ADDR> } ] [ dscp <DSCP> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа;

<USERNAME> – имя пользователя, задаётся строкой до 31 символа;

<ADDR> – IP-адрес устройства, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес устройства, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<HOSTNAME> – DNS-имя устройства, задаётся строкой до 253 символов;

<PORT> – номер TCP-порта, прослушиваемого SSH-сервером, принимает значения [1..65535]. По умолчанию установлено 22;

<VERSION> – версия SSH-протокола, принимает значения [1..2]. По умолчанию используется версия 1;

<SRC-ADDR> – IP-адрес отправителя, в качестве данного адреса может использоваться любой IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-IPV6-ADDR> – IPv6-адрес отправителя, в качестве данного адреса может использоваться любой IPv6-адрес маршрутизатора, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<DSCP> – DSCP-приоритет в соответствии с RFC 2474, принимает значение [0..63], значение по умолчанию 0.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# ssh tester 10.100.100.1
The authenticity of host '10.100.100.1 (10.100.100.1)' can't be established.
ECDSA key fingerprint is db:e4:0a:93:59:87:7d:9f:90:5c:19:a3:e7:97:ec:d5.
Are you sure you want to continue connecting (yes/no)? yes
%AAA-I-SSH: Warning: Permanently added '10.100.100.1' (ECDSA) to the list of known hosts.
tester@10.100.100.1's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-51-generic x86_64)
 * Documentation:  https://help.ubuntu.com/
  System information as of Mon May 25 09:25:10 NOVT 2015
Last login: Tue May 12 19:39:11 2015
(tester@kubuntu  ~) $
```

telnet

Данная команда используется для подключения к удаленному узлу по протоколу Telnet.

Синтаксис

```
telnet [ vrf <VRF>] { <ADDR> | <IPV6-ADDR> | <HOSTNAME> } [ port <PORT> ] [ source
{ <SRC-ADDR> | <SRC-IPV6-ADDR> } ] [ dscp <DSCP> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа;

<ADDR> – IP-адрес устройства, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес устройства, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<HOSTNAME> – DNS-имя устройства, задаётся строкой до 253 символов;

<PORT> – номер TCP-порта, прослушиваемого SSH-сервером, принимает значения [1..65535], по умолчанию 23;

<SRC-ADDR> – IP-адрес отправителя, в качестве данного адреса может использоваться любой IP-адрес контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-IPV6-ADDR> – IPv6-адрес отправителя, в качестве данного адреса может использоваться любой IPv6-адрес контроллера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<DSCP> – DSCP-приоритет в соответствии с RFC 2474, принимает значение [0..63], значение по умолчанию 0.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# telnet 10.100.100.1
Entering character mode
Escape character is '^]'.
Ubuntu 14.04.2 LTS
kubuntu login: tester
Password:
Last login: Mon May 25 15:23:06 NOVT 2015 from sw31-1.eltex.loc on pts/16
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-51-generic x86_64)
 * Documentation:  https://help.ubuntu.com/
  System information as of Mon May 25 15:23:01 NOVT 2015
(tester@kubuntu  ~) $
```

terminal datadump

Команда используется для выключения постраничного режима вывода трассировок для текущей сессии.

Использование отрицательной команды включает постраничный режим вывода трассировок.

Синтаксис

```
[no] terminal datadump
```

Параметры

Команда не содержит параметров

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# terminal datadump
```

terminal resize

Команда используется для масштабирования размера терминала под размер окна при использовании консольного подключения.

Синтаксис

```
terminal resize
```

Параметры

Команда не содержит параметров

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# terminal resize
```

traceroute

Данная команда используется для трассировки маршрута до указанного сетевого устройства.

Синтаксис

```
traceroute [ vrf <VRF> ] { <ADDR> | | <IPV6-ADDR> | <HOSTNAME> [ { ip | ipv6 } ] }
[ first-ttl <FIRST-TTL> ] [ max-ttl <MAX-TTL> ] [ timeout <TIMEOUT> ]
[ source { ip { <SRC-ADDR> | <SRC-IPV6-ADDR> } | interface <IF> | tunnel <TUN> } ] [ dscp
<DSCP> ] [ protocol { icmp | udp [ <PORT> ] | tcp [ <PORT> ] } ]
[ gateway { <GW-ADDR> | <GW-IPV6-ADDR> } ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа;

<ADDR> – IP-адрес устройства, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес устройства, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<HOSTNAME> – DNS-имя устройства, задаётся строкой до 255 символов:

- ip – проводить трассировку при помощи ipv4-пакетов;
- ipv6 – проводить трассировку при помощи ipv6-пакетов.

<FIRST-TTL> – время жизни IP-пакета, значение с которого начинается трассировка маршрута, принимает значение [1..255], по умолчанию 1;

<MAX-TTL> – время жизни IP-пакета, значение на котором заканчивается трассировка маршрута, принимает значение [1..255], по умолчанию 30;

<TIMEOUT> – время ожидания ответа, в секундах. Опция влияет на таймаут, если отсутствуют какие-либо ответы, в противном случае утилита ждет два RTTs. Принимает значение [1..60], по умолчанию 5 секунд;

<SRC-ADDR> – IP-адрес отправителя, в качестве данного адреса может использоваться любой IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-IPV6-ADDR> – IPv6-адрес отправителя, в качестве данного адреса может использоваться любой IPv6-адрес контроллера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<IF> – имя интерфейса контроллера, через который будут отправлены пакеты, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля маршрутизатора, через который будут отправлены пакеты, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<DSCP> – DSCP-приоритет в соответствии с RFC 2474, принимает значение [0..63], значение по умолчанию 0;

<PORT> – номер TCP/UDP-порта, принимает значение [1..65535], значение по умолчанию 53 для UDP и 80 для TCP;

<GW-ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. При указании данного параметра в исходящий пакет добавляется IP source routing опция, которая сообщает контроллеру, через какой шлюз должен маршрутизироваться пакет в сети. На большинство контроллеров отключена маршрутизация по данной опции из соображений безопасности;

<GWIPV6-ADDR> – IPv6-адрес шлюза, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. При указании данного параметра в исходящий пакет добавляется IP source routing опция, которая сообщает контроллеру, через какой шлюз должен маршрутизироваться пакет в сети. На большинство контроллеров отключена маршрутизация по данной опции из соображений безопасности.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# traceroute 192.168.27.128
traceroute to 192.168.27.128 (192.168.27.128), 30 hops max, 60 byte packets
1 192.168.16.1 (192.168.16.1)  1.240 ms  1.546 ms  1.883 ms
2 192.168.27.128 (192.168.27.128)  0.451 ms  0.437 ms  0.411 ms
```

uptime

Данной командой осуществляется просмотр продолжительности времени работы устройства.

Синтаксис

```
uptime
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# uptime
System uptime:          26 minutes and 35 seconds
```

verify

Данной командой выполняется расчет хэш-суммы для отдельного файла с использованием указанного алгоритма хэширования.

Синтаксис

```
verify <ALGORITHM> <FILE>
```

Параметры

<ALGORITHM> – алгоритм хэширования, принимает значения [md5, sha2-256, sha2-512].

<FILE> – путь и имя файла для проверки, может принимать следующие значения:

- usb://usb_name:/PATH
- mmc://mmc_name:/PATH
- system:candidate-config
- system:running-config
- system:factory-config
- system:default-config
- system:firmware-image-1
- system:firmware-image-2
- system:boot-1
- system:boot-2
- flash:critlog/FILE
- flash:syslog/FILE
- flash:data/FILE
- tmpsys:syslog/FILE

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# verify md5 system:firmware-image-1
system:firmware-image-1 16ef38a292e96ce972e910da6db2d1f4
```

verify filesystem

Данной командой запускается процесс расчета хэш-сумм для всех системных файлов контроллера и сравнения с эталонными значениями. В результате выводится информация о соответствии рассчитанных хэш-сумм эталонным.

Синтаксис

```
verify filesystem [detailed]
```

Параметры

detailed – ключ отвечающий за подробный вывод информации о проверке каждого файла.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# verify filesystem
Total:          2949
Success:        2949
Changed:        0
Deleted:        0


Filesystem verification success.
```

verify storage-device

Данной командой запускается процесс проверки внешнего носителя на наличие ошибок.

Синтаксис

```
verify storage-device { usb-dev://<ID> | usb://<USB-NAME> | mmc }
```

Параметры

<ID> – номер подключенного USB-носителя по порядку;

<USB-NAME> – имя подключенного USB-носителя. Имя можно узнать в выводе команды show storage-devices;

mmc – ключ для проверки установленного mmc-носителя.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# verify storage-device usb://BC1E-2E16
Device verify
Do you really want to continue? (y/N): y
CP437: Invalid argument
fsck.fat 4.0 (2016-05-06)
/dev/sda2: 14 files, 63908/255496 clusters
Device verification success.
```

6 Управление программным обеспечением и конфигурацией

- archive
- auto
- banner exec
- banner login
- boot host auto-config
- boot host auto-update
- boot system
- by-commit
- commit
- confirm
- copy
- count-backup
- delete
- dir
- merge
- path
- restore
- rollback
- save
- show bootvar
- show boot-licence
- show candidate-config
- show configuration changes
- show crypto certificates
- show licence
- show running-config
- show storage-devices
- show usb
- show version
- time-period
- type

archive

Данной командой осуществляется переход в режим настройки параметров резервирования конфигурации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию для параметров резервирования конфигурации.

Синтаксис

```
[no] archive
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# archive
wlc-30(config-archive)#
```

auto

Данной командой включается режим создания файла резервной конфигурации на удаленном сервере и/или локально через указанный промежуток времени (раздел time-period).

Использование отрицательной формы команды (no) выключает режим отправки через указанный промежуток времени.

Синтаксис

```
[no] auto
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# auto
```

banner exec

Данной командой задаётся текстовое сообщение, выводимое после успешной аутентификации пользователя на контроллере.

Использование отрицательной формы команды (no) удаляется текстовое сообщение, выводимое после успешной аутентификации пользователя на контроллере.

Синтаксис

```
banner exec <BUNNER>
no banner exec
```

Параметры

<BUNNER> – текстовое сообщение, задаётся в кавычках строкой до 2047 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# banner exec "                          ----- Hello! This is an Eltex
router.-----                                \n----- Unauthorized configuration changes are
prosecuted by the law of the Russian Federation. -----"
```

banner login

Данной командой задаётся текстовое сообщение, выводимое до аутентификации пользователя на контроллере.

Синтаксис

```
banner login <BUNNER>
no banner login
```

Параметры

<BUNNER> – текстовое сообщение, задаётся в кавычках строкой до 2047 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# banner login "                      ----- Hello! This is an Eltex router.-----
\n----- Unauthorized connection is prosecuted by the law of the Russian Federation. -----"
```

boot host auto-config

Данная команда включает загрузку конфигурации контроллера при помощи протокола DHCP Option 54 (IP-адрес TFTP-сервера) и 67 (имя файла конфигурации).

Использование отрицательной формы команды (no) отключает загрузку конфигурации контроллера при помощи протокола DHCP Option 66 и 67.

Синтаксис

```
[no] boot host auto-config
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Значение по умолчанию

Отключено.

Командный режим

CONFIG

Пример:

```
wlc-30(config)# boot host auto-config
```

boot host auto-update

Данная команда включает загрузку ПО контроллера при помощи протокола DHCP Option 54 (IP-адрес TFTP-сервера) и имя файла ПО в поле FILE в DHCP OFFER. При использовании совместно с boot host auto-config, обновление ПО имеет более высокий приоритет.

Использование отрицательной формы команды (no) отключает загрузку ПО контроллера при помощи протокола DHCP Option 150 и 67.

Синтаксис

```
[no] boot host auto-update
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Значение по умолчанию

Отключено.

Командный режим

CONFIG

Пример:

```
wlc-30(config)# boot host auto-update
```

boot system

Данная команда служит для выбора активного образа программного обеспечения, загруженного на устройство.

Синтаксис

```
boot system <IMAGE>
```

Параметры

<IMAGE> – название образа программного обеспечения, который будет загружаться на устройство:

- image-1 – следующая загрузка устройства будет выполнена из первого образа ПО;
- image-2 – следующая загрузка устройства будет выполнена из второго образа ПО.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# boot system image-2
```

by-commit

Данной командой включается режим отправки файла конфигурации на сервер резервирования после удачного применения конфигурации.

Использование отрицательной формы команды (no) выключает режим отправки после удачного применения конфигурации.

Синтаксис

```
[no] by-commit
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# by-commit
```

commit

Данная команда позволяет применить (сделать действующими) изменения конфигурации. RUNNING-конфигурация замещается конфигурацией CANDIDATE. Для того чтобы примененные изменения стали постоянно действующими, эту операцию необходимо подтвердить командой «confirm» в течение времени, не превышающего время действия таймера подтверждения (по умолчанию 600 секунд, изменяется при помощи команды system config-confirm timeout).

Синтаксис

```
commit
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

CHANGE-EXPIRED-PASSWORD

Пример:

```
wlc-30# commit
```

Изменения конфигурации применены.

confirm

Команда предназначена для подтверждения применения конфигурации. Если в течение заданного времени (по умолчанию 600 секунд, изменяется при помощи команды system config-confirm timeout) после применения конфигурации командой «commit» не было введено подтверждение, произойдет автоматический откат на действующую ранее конфигурацию. Автоматическая система откатов предотвращает ситуации потери связи с устройством.

Синтаксис

```
confirm
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

CHANGE-EXPIRED-PASSWORD

Пример:

```
wlc-30# confirm
```

Подтверждение изменений в конфигурации.

copy

Данная команда служит для копирования файлов между различными источниками и получателями.

Синтаксис

`copy <SOURCE> <DESTINATION>`

Параметры

<SOURCE> – источник, задаётся в виде:

- tftp://<ip>[<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ip> – IP-адрес TFTP-сервера;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на TFTP-сервере.
- tftp://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ipv6> – IPv6-адрес TFTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
  - <path> – путь к файлу на TFTP-сервере.
- ftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
  - <ip> – IP-адрес FTP-сервера;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
  - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на FTP-сервере.
- ftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
  - <ipv6> – IPv6-адрес FTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;

    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес FTP-сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес FTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- scp://[<user>:<password>@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password*, описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на сервере.
- scp://[<user>:<password>@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password,* описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на сервере.
- http:// <ip>[<port>]:/<path> – адрес файла на HTTP-сервере, где:
    - <ip> – IP-адрес HTTP-сервера;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на HTTP-сервере.
- http://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на HTTP-сервере, где:
    - <ipv6> – IPv6-адрес HTTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на TFTP-сервере.
- https://[ca/<CA-FILE>][:server-crt/<SC-FILE>][:server-key/<SK-FILE>]@<ip>[<port>]:/<path> – адрес файла на HTTPS-сервере, где:

    - <CA-FILE> – имя файла сертификата удостоверяющего сервера в соответствующем разделе памяти контроллера;
    - <SC-FILE> – имя файла публичного сертификата сервера в соответствующем разделе памяти контроллера;
    - <SK-FILE> – имя файла приватного ключа сервера в соответствующем разделе памяти контроллера;
    - <ip> – IP-адрес HTTP-сервера;
    - <port> – порт, на котором запущен HTTPS-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на HTTP-сервере.
- https://[ca/<CA-FILE>][:server-crt/<SC-FILE>][:server-key/<SK-FILE>]@<ipv6>[%<interface>][<port>]:/<path> – адрес файла на HTTPS-сервере, где:
    - <CA-FILE> – имя файла сертификата удостоверяющего сервера в соответствующем разделе памяти контроллера;
    - <SC-FILE> – имя файла публичного сертификата сервера в соответствующем разделе памяти контроллера;
    - <SK-FILE> – имя файла приватного ключа сервера в соответствующем разделе памяти контроллера;
    - <ipv6> – IPv6-адрес HTTPS-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на TFTP-сервере.
- usb://usb_name:/PATH
    - usb_name – имя, назначенное USB-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
    - <path> – путь к файлу на USB-носителе.
- mmc://mmc_name:/PATH
    - mmc_name – имя назначенное MMC-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
    - <path> – путь к файлу на MMC-носителе.
- system:factory-config – заводская конфигурация;
- system:default-config – конфигурация по умолчанию (пустая);
- system:running-config – текущая конфигурация;
- system:candidate-config – конфигурация, которая будет применена после выполнения команды «commit»;
- system:firmware – программное обеспечение устройства. Копирование производится с неактивного образа программного обеспечения устройства;
- system:boot-1 – первичный загрузчик устройства (SBI, bl1, x-loader).
- system:boot-2 – вторичный загрузчик устройства (u-boot, boot).
- flash:critlog/FILE – папка для сохранения сообщений ядра за все время работы устройства;
- flash:syslog/FILE – папка для сохранения логов текущей сессии, сохраняется после перезагрузки;
- tmpsys:syslog/FILE – папка для сохранения логов текущей сессии, не сохраняется после перезагрузки;
- flash:backup/FILE – папка для сохранения резервных копий текущих конфигураций контроллера;
- flash:data/FILE – папка для скачивания файлов с контроллера.

<DESTINATION> – назначение, задаётся в виде:

- tftp://<ip>[<port>]:/<path> – адрес файла на TFTP-сервере, где:
    - <ip> – IP-адрес TFTP-сервера;
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на TFTP-сервере.
- tftp://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на TFTP-сервере, где:
    - <ipv6> – IPv6-адрес TFTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;

    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на TFTP-сервере.
- ftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес FTP-сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на FTP-сервере.
- ftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес FTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес FTP-сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес FTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- scp://[<user>:<password>@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password,* описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на сервере.
- scp://[<user>:<password>@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password,* описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);

    - <path> – путь к файлу на сервере.
- usb://usb_name:/PATH
    - usb_name – имя назначенное USB-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
    - <path> – путь к файлу на USB-носителе.
- mmc://mmc_name:/PATH
    - mmc_name – имя назначенное MMC-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
    - <path> – путь к файлу на MMC-носителе.
- system:candidate-config – конфигурация, которая будет применена после выполнения команды «commit»;
- system:licence – лицензия устройства;
- system:boot-licence – лицензия устройства, применяющаяся при запуске вторичного загрузчика;
- system:firmware – программное обеспечение устройства. Копирование всегда происходит в неактивный образ программного обеспечения устройства;
- system:boot2 – вторичный загрузчик устройства (u-boot, x-loader);
- certificate/ca/ – папка для хранения сертификата удостоверяющего центра;
- certificate/dh/ – папка для хранения ключа Диффи-Хеллмана;
- certificate/server_key/ – папка для хранения приватного ключа OPENVPN-сервера;
- certificate/server_crt/ – папка для хранения приватного ключа OPENVPN-сервера;
- certificate:client-key/FILE – папка для хранения приватного ключа OPENVPN-клиента;
- certificate:client-crt/FILE – папка для хранения сертификата OPENVPN-клиента;
- certificate/ta/ – папка для хранения HMAC-ключа;
- certificate/crl/ – папка для хранения списка отозванных сертификатов;
- flash:data/FILE – папка для скачивания файлов с контроллера.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример 1

```
wlc-30# copy tftp://10.100.100.1/wlc-30.cfg system:candidate-config
```

Пример 2

```
wlc-30# copy tftp://10.100.100.1/crl.pem system:certificate/crl/crl.pem
```

count-backup

Данной командой устанавливается максимальное количество локально сохраняемых резервных копий конфигураций.

При использовании отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
count-backup <NUM>
no count-backup
```

Параметры

<NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# count-backup 20
```

delete

Данная команда служит для удаления лицензий, сертификатов, ключей.

Синтаксис

```
delete <FILE>
```

Параметры

<FILE> – тип файла, может принимать следующие значения (при удаление из папки необходимо указать название файла):

- flash:backup/FILE – папка для сохранения резервных копий текущих конфигураций контроллера;
- flash:critlog/FILE – папка для сохранения сообщений ядра за все время работы устройства;
- flash:data/FILE – папка для скачивания файлов с контроллера;
- flash:syslog/FILE – папка для сохранения логов текущей сессии, сохраняется после перезагрузки;
- tmpsys:syslog/FILE – папка для сохранения логов текущей сессии, не сохраняется после перезагрузки;
- certificate/ca/FILE – папка для хранения сертификата удостоверяющего центра;
- certificate/dh/FILE – папка для хранения ключа Диффи-Хеллмана;
- certificate/server_key/FILE – папка для хранения приватного ключа IPsec/OpenVPN-сервера;
- certificate/server_crt/FILE – папка для хранения публичного сертификата IPsec/OpenVPN-сервера;
- certificate:client-key/FILE – папка для хранения приватного ключа OPENVPN-клиента;
- certificate:client-crt/FILE – папка для хранения сертификата OPENVPN-клиента;
- certificate/ta/FILE – папка для хранения HMAC-ключа;
- certificate/crl/FILE – папка для хранения списка отозванных сертификатов;
- system:licence – лицензия для активации функционала, требующего лицензию;
- system:boot- licence – лицензия устройства, применяющаяся при запуске вторичного загрузчика;
- usb://usb_name:/FILE
    - usb_name – имя, назначенное USB-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
    - <FILE> – путь к файлу и его имя на USB-носителе.

- mmc://mmc_name:/<FILE>
  - mmc_name – имя назначенное MMC-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
  - <FILE> – путь к файлу и его имя на MMC-носителе.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# delete system:certificate/dh/dh.key
```

dir

Данная команда позволяет отобразить содержимое внешних носителей информации (USB/MMC карт памяти) и локальных разделов контроллера.

Синтаксис

```
dir <PATH>
{ usb://<USB-device-name>/<PATH> | mmc://<MMC-device-name>/<PATH> | flash:backup/FILE |
flash:data/FILE }
```

Параметры

<PATH> – имя локального раздела или путь до папки на внешнем носителе. Принимает значения:

- flash:critlog/ – папка для сохранения сообщений ядра за все время работы устройства;
- flash:syslog/ – папка для сохранения логов текущей сессии, сохраняется после перезагрузки;
- flash:backup/ – папка для сохранения резервных копий текущих конфигураций контроллера;
- flash:data/ – папка для скачивания файлов с контроллера;
- tmpsys:syslog/ – папка для сохранения логов текущей сессии, не сохраняется после перезагрузки;
- certificate/ca/ – папка для хранения сертификата удостоверяющего центра;
- certificate/dh/ – папка для хранения ключа Диффи-Хеллмана;
- certificate/ta/ – папка для хранения HMAC ключа;
- certificate/crl/ – папка для хранения списка отозванных сертификатов;
- certificate/server_key/ – папка для хранения приватного ключа IPsec/OpenVPN-сервера;
- certificate/server_crt/ – папка для хранения публичного сертификата IPsec/OpenVPN-сервера;
- certificate:client-key/ – папка для хранения приватного ключа OPENVPN-клиента;
- certificate:client-crt/ – папка для хранения сертификата OPENVPN-клиента;
- usb://usb_name:/PATH
  - usb_name – имя, назначенное USB-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
  - <PATH> – путь к файлу на USB-носителе.
- mmc://mmc_name:/PATH
  - mmc_name – имя, назначенное MMC-носителю. Возможно посмотреть командой "show storage-devices" (см. раздел show storage-devices);
  - <PATH> – путь к файлу на MMC-носителе.

<USB-device-name> – назначенное системой имя USB-носителя. Отображается в выводе команды show storage-devices usb, раздел show storage-devices.

<MMC-device-name> – назначенное системой имя MMC-носителя. Отображается в выводе команды show storage-devices mmc, раздел show storage-devices.

- flash:backup/FILE – файл для сохранения резервных копий текущих конфигураций контроллера;
- flash:data/FILE – папка для скачивания файлов с контроллера;

<PATH> – путь до необходимой папки на USB/MMC-носителе.

flash:backup/FILE – файл для сохранения резервных копий текущих конфигураций контроллера;

flash:data/FILE – папка для скачивания файлов с контроллера;

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# dir mmc://EF28-D074
Name                                      Type          Size
----------------------------------------   ----------   --------   --
wlc-30-1.4.0-build21.uboot                File          0.00       B
.Trash-1000                               Directory     0.00       B
```

merge

Данная команда служи для объединения локального или загружаемого файла конфигурации с candidate-config.

Синтаксис

```
merge <SOURCE> system:candidate-config
```

Параметры

<SOURCE> – источник, задаётся в виде:

- tftp://<ip>[<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ip> – IP-адрес TFTP-сервера;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на TFTP-сервере.
- tftp://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ipv6> – IPv6-адрес TFTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
  - <path> – путь к файлу на TFTP-сервере.
- ftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
  - <ip> – IP-адрес FTP-сервера;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);

    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на FTP-сервере.
- ftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес FTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client username);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес FTP-сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес FTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на FTP-сервере.
- scp://[<user>:<password>@]<ip>[<port>]:/<path>
    - <ip> – IP-адрес сервера;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password*, описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на сервере.
- scp://[<user>:<password>@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password,* описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на сервере.
- http://<ip>[<port>]:/<path> – адрес файла на HTTP-сервере, где:
    - <ip> – IP-адрес HTTP-сервера;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на HTTP-сервере.
- http://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на HTTP-сервере, где:

    - <ipv6> – IPv6-адрес HTTP-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на TFTP-сервере.
- https://[ca/<CA-FILE>][:server-crt/<SC-FILE>][:server-key/<SK-FILE>]@<ip>[<port>]:/<path> – адрес файла на HTTPS-сервере, где:
    - <CA-FILE> – имя файла сертификата удостоверяющего сервера в соответствующем разделе памяти контроллера;
    - <SC-FILE> – имя файла публичного сертификата сервера в соответствующем разделе памяти контроллера;
    - <SK-FILE> – имя файла приватного ключа сервера в соответствующем разделе памяти контроллера;
    - <ip> – IP-адрес HTTP-сервера;
    - <port> – порт, на котором запущен HTTPS-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на HTTP-сервере.
- https://[ca/<CA-FILE>][:server-crt/<SC-FILE>][:server-key/<SK-FILE>]@<ipv6>[%<interface>][<port>]:/<path> – адрес файла на HTTPS-сервере, где:
    - <CA-FILE> – имя файла сертификата удостоверяющего сервера в соответствующем разделе памяти контроллера;
    - <SC-FILE> – имя файла публичного сертификата сервера в соответствующем разделе памяти контроллера;
    - <SK-FILE> – имя файла приватного ключа сервера в соответствующем разделе памяти контроллера;
    - <ipv6> – IPv6-адрес HTTPS-сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <port> – порт, на котором запущен HTTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на TFTP-сервере.
- flash:data/FILE – папка для скачивания файлов с контроллера.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# merge tftp://10.100.100.1/wlc-30.cfg system:candidate-config
```

path

Данной командой определяется протокол, адрес сервера, а также расположение и префикс имени файла на сервере. При выполнении резервирования к префиксу имени файла добавляется текущее время и дата в формате ГГГГММДД_ЧЧММСС.

Использование отрицательной формы команды (no) удаляет установленное значение.

Синтаксис

```
path <PATH>
```

```
no path
```

Параметры

<PATH> – формат пути до папки на удаленном сервере по протоколам tftp/ftp/sftp/scp в одном из следующих форматов:

- tftp://<ip>[<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ip> – IP-адрес TFTP-сервера;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на TFTP-сервере.
- tftp://<ipv6>[%<interface>][<port>]:/<path> – адрес файла на TFTP-сервере, где:
  - <ipv6> – IPv6-адрес TFTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;
  - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
  - <path> – путь к файлу на TFTP-сервере.
- ftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
  - <ip> – IP-адрес FTP-сервера;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
  - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client password);
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на FTP-сервере.
- ftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
  - <ipv6> – IPv6-адрес FTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ftp client username*, описанной в ip ftp client username);
  - <password> – пароль (настроить пароль по умолчанию можно командой *ip ftp client password*, описанной в ip ftp client username);
  - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
  - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ip>[<port>]:/<path>
  - <ip> – IP-адрес FTP-сервера;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
  - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
  - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
  - <path> – путь к файлу на FTP-сервере.
- sftp://[<user>[:<password>]@]<ipv6>[%<interface>][<port>]:/<path>
  - <ipv6> – IPv6-адрес FTP-сервера;
  - <interface> – исходящий сетевой интерфейс для link-local адресов;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip sftp client username*, описанной в ip sftp client username);
  - <password> – пароль (настроить пароль по умолчанию можно командой *ip sftp client password*, описанной в ip sftp client password);
  - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
  - <path> – путь к файлу на FTP-сервере.
- scp://[<user>:<password>@]<ip>[<port>]:/<path>
  - <ip> – IP-адрес сервера;
  - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);

    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password*, описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IP-адреса символом «#» или «:»;
    - <path> – путь к файлу на сервере.
- scp://[<user>:<password>@]<ipv6>[%<interface>][<port>]:/<path>
    - <ipv6> – IPv6-адрес сервера;
    - <interface> – исходящий сетевой интерфейс для link-local адресов;
    - <user> – имя пользователя (настроить имя пользователя по умолчанию можно командой *ip ssh client username*, описанной в ip ssh client username);
    - <password> – пароль (настроить пароль по умолчанию можно командой *ip ssh client password,* описанной в ip ssh client password);
    - <port> – порт, который слушает TFTP-сервер, отделяется от IPv6-адреса символом '#' или ':' (в данном случае IPv6-адрес должен быть заключен в квадратные скобки «[]»);
    - <path> – путь к файлу на сервере.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# path tftp://10.10.10.1:/wlc-30/config
```

restore

Данная команда позволяет отменить примененную, но неподтвержденную конфигурацию и вернуться к последней подтвержденной. Команда применяется ко всей конфигурации устройства. Отмена изменений может быть выполнена только до ввода команды «confirm». При выполнении команды «restore» происходит потеря неподтвержденной конфигурации.

Синтаксис

`restore`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# restore
```

Осуществлен возврат к последней подтвержденной конфигурации.

rollback

Данная команда позволяет отменить непримененные изменения конфигурации. В результате выполнения команды будет удалена CANDIDATE-конфигурация. Команда может быть использована только до ввода команды «commit».

Команда применяется ко всей конфигурации устройства.

Синтаксис

`rollback`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# rollback
```

Произведена отмена всех непримененных изменений в конфигурации.

save

Команда служит для сохранения CANDIDATE-конфигурации в постоянную память устройства.

Синтаксис

`save`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# save
```

Сохранение текущей конфигурации на Flash-память устройства.

show bootvar

Данная команда служит для просмотра информации об образах программного обеспечения, загруженных на устройство.

Синтаксис

`show bootvar`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show bootvar
Image   Version                      Date                   Status         After reboot
-----   --------------------------   --------------------   ------------   ------------
1       1.0.7 build 119[5cd22b8]       date 22/12/2015 time   Not Active
                                       18:00:47
2       1.0.7 build 119[5cd22b8]       date 22/12/2015 time   Active            *
                                       18:00:47
```

show boot-licence

Данная команда служит для просмотра информации об активной лицензии устройства применяемых на этапе загрузки вторичного загрузчика.

Синтаксис

```
show boot-licence
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

5

Командный режим

ROOT

Пример:

```
wlc-30# show boot-licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    WLC-30
S/N:     NP01000530
MAC:     A8:F9:4B:AA:44:BB
Features:
 KSS - Kaspersky Security System
```

show candidate-config

Данной командой осуществляется просмотр конфигурации устройства, которая будет установлена после применения настроек (команда «commit»).

Синтаксис

```
show candidate-config [ full ] [ <SECTION> ]
```

Параметры

full – ключ для отображения в конфигурации значений всех параметров, в том числе и ненастроенных.

<SECTION> – раздел конфигурации:

- aaa – настройка параметров аутентификации, авторизации и учета;
- access-list – конфигурация списков доступа;
- bridges – конфигурация сетевых мостов;
    - [<NUM>] – номер сетевого моста.
- channel-group – конфигурация группы агрегации каналов;
- clock – конфигурация системных часов контроллера и NTP-протокола;
- dhcp – конфигурация DHCP-сервера, клиента и Relay-агента;
- content-provider – конфигурация источника обновлений правил распространяемых по коммерческой лицензии;
- extended – расширенный вывод конфигурации;
- hostname – сетевое имя контроллера;

- interfaces [<IF>] – конфигурация интерфейсов:
  - <IF> – наименование интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.
- ip-address – конфигурация IP-интерфейсов;
- ipv6 [<SUBSECTION>] – конфигурация IPv6:
  - address – конфигурация IPv6-интерфейсов;
  - dhcp [<SUBSECTION>] – конфигурация IPv6 DHCP-сервисов;
  - client – конфигурация IPv6 DHCP-сервера:
    - relay – конфигурация IPv6 DHCP Relay-агента;
    - server – конфигурация IPv6 DHCP-клиента.
  - routing [<SUBSECTION>] – конфигурация IPv6-маршрутизации:
    - bfd – конфигурация протокола IPv6 BFD;
    - bgp – конфигурация протокола IPv6 BGP;
    - ospf – конфигурация протокола OSPFv3;
    - prefix-lists – конфигурация IPv6 префикс-листов;
    - rip – конфигурация протокола RIP;
    - static – конфигурация статических маршрутов.
  - vrrp – конфигурация IPv6 VRRP-протокола.
- dialplan – конфигурация плана нумерации;
- lldp – конфигурация протокола LLDP;
- mailservers – конфигурация почтовых серверов и доменов;
- mdns – функционала mDNS;
- mpls – конфигурация протоколов технологии MPLS;
- mdns – конфигурация функционала mDNS;
- multiwan – конфигурация сервиса резервирования и балансировки WAN-интерфейсов;
- nat [<SUBSECTION>] – конфигурация сервиса NAT:
  - source – конфигурация сервиса Source NAT;
  - destination – конфигурация сервиса Destination NAT;
  - alg – конфигурация алгоритма NAT.
- netflow – конфигурация Netflow протокола;
- object-groups [<TYPE> [<NAME>]] – конфигурация профилей;
  - <TYPE> – тип профиля, принимает значения:
    - content-filter;
    - email;
    - network;
    - address-port;
    - application;
    - mac;
    - service;
    - url.
  - <NAME> – имя профиля заданного типа.
- qos – конфигурация QoS;
- remote-access [<SUBSECTION>] – конфигурация профилей L2TP over IPsec и PPTP-серверов;
  - l2tp – конфигурация профилей L2TP over IPsec-серверов;
  - pptp – конфигурация профилей PPTP-серверов;
  - openvpn – конфигурация профилей OpenVPN-серверов.
- remote-client – конфигурация удаленного доступа (SSH, Telnet, etc.);
- rmon – конфигурация RMON;
- routing [<SUBSECTION>] – конфигурация маршрутизации:
  - bfd – конфигурация протокола BFD;
  - bgp – конфигурация протокола BGP;
  - isis – конфигурация протокола IS-IS;
  - key-chains – конфигурация ключей аутентификации;
  - ospf – конфигурация протокола OSPF;
  - prefix-list – конфигурация префикс-листов;
  - rip – конфигурация протокола RIP;

        - route-maps – конфигурация маршрутных карт:
            - [<RM-NAME>] – имя маршрутной карты.
        - static – конфигурация статических маршрутов.
- security [<SUBSECTION>] – конфигурация сервисов IPsec VPN и Firewall;
        - antispam - конфигурация профилей сервиса «Антиспам»;
        - ike – конфигурация IKE;
        - ipsec – конфигурация IPsec;
        - zone – конфигурация зон Firewall;
        - zone-pair – конфигурация переходов между зонами Firewall;
- sip – конфигурация протокола SIP;
        - profile – конфигурация SIP-профилей;
        - service – конфигурация SIP-профилей;
- sflow – конфигурация sFlow протокола;
- snmp – конфигурация SNMP-сервера;
- spanning-tree – конфигурация протоколов семейства Spanning Tree;
- sla – конфигурация сервиса IP SLA;
- system – конфигурация общесистемных параметров;
- syslog – конфигурация сервиса Syslog;
- tracks – конфигурация Tracking-объектов.
- tunnels [<TYPE> [<NUM>]] – конфигурация туннелей:
        - <TYPE> – тип туннеля, принимает значения:
            - gre – конфигурация GRE-туннелей;
            - ip4ip4 – конфигурация IPv4 over IPv4-туннелей;
            - l2tp – конфигурация L2TP-туннелей;
            - l2tpv3 – конфигурация L2TPv3-туннелей;
            - lt – конфигурация логических туннелей;
            - vti – конфигурация VTI-туннелей;
            - pptp – конфигурация PPTP-клиентов;
            - pppoe – конфигурация PPPoE-клиентов;
            - l2tp – конфигурация L2TP- клиентов;
            - openvpn – конфигурация OPENVPN-клиентов;
        - <NUM> – номер туннеля данного типа в конфигурации контроллера.
- vlans – конфигурация VLAN;
- vrf – конфигурация VRF;
- vrrp – конфигурация VRRP-протокола;
- wisla – конфигурация системы мониторинга качества услуг wiSLA;
- wireless-controller – конфигурация параметров Wi-Fi контроллера;
- zabbix – конфигурация Zabbix-агента.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show candidate-config
ntp enable
ntp broadcast-client enable
syslog max-files 3
syslog file-size 512
syslog file default info
vlan 2
exit
security zone trusted
exit
security zone untrusted
exit
object-group service telnet
  port-range 23
exit
object-group service ssh
  port-range 22
exit
object-group service dhcp_server
  port-range 67
exit More? Enter – next line; Space – next page; Q – quit; R – show the rest.
```

show configuration changes

Данной командой осуществляется просмотр различий между конфигурационными файлами.

Синтаксис

```
show configuration changes [<CONFIG> < CONFIG>]
```

Параметры

<CONFIG> – конфигурационный файл для сравнения. Могут принимать значения:

- candidate-config;
- running-config;
- factory-config;
- default-config;
- flash:backup/FILE.

Значение по умолчанию

Без указания <CONFIG> отображается разница между running-config и candidate-config.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30(config-)# show configuration changes
+ interface gigabitethernet 1/0/1.100
+   ip firewall disable
+   ip address 10.54.22.1/24
+ exit
```

show crypto certificates

Данная команда выводит информацию о количестве сертификатов.

Синтаксис

```
show crypto certificates [ <CERTIFICATE-TYPE> ]
```

Параметры

<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения:

- ca – сертификат удостоверяющего сервера;
- crl – список отозванных сертификатов;
- dh – ключ Диффи-Хеллмана;
- server-crt – публичный сертификат сервера;
- server-key – приватный ключ сервера;
- client-crt – сертификат клиента;
- client-key – приватный ключ клиента;
- ta – HMAC-ключ.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# show crypto certificates
Type           Total
------------   -------
ca               3
dh              1
server key      2
server crt      1
ta              1
crl             1
```

show licence

Данная команда служит для просмотра информации об активной лицензии устройства.

Синтаксис

```
show licence
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

5

Командный режим

ROOT

Пример:

```
wlc-30# show licence
Licence information
-------------------
Name: X-Telecom
Version: 1.0
Type: WLC-30
S/N: NP01000046
MAC: A8:F9:4B:AA:03:20
Features:
    DHCP - Dynamic Host Configuration Protocol
    IDS - Empty description
    SWUTIL - View interface's utilization
```

show running-config

Данная команда служит для просмотра текущей конфигурации устройства.

Синтаксис

```
show running-config [<SECTION>] [ full ]
```

Параметры

<SECTION> – раздел конфигурации, описание приведено в разделе show candidate-config.

full – ключ для отображения в конфигурации значений всех параметров, в том числе и ненастроенных.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show running-config syslog
syslog max-files 3
syslog file-size 512
syslog file default info
syslog console info
```

show storage-devices

Данной командой выводится информация о подключенных внешних носителях информации (USB/MMC карт памяти).

Синтаксис

```
show storage-devices { usb | mmc }
```

Параметры

usb – USB-накопитель информации;

mmc – SD/MMC карта памяти.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show storage-devices mmc
Name                            Total, MB    Used, MB     Free, MB
------------------------------  ----------   ----------   ----------
EF28-D074                       99.79        72.64        27.15
```

show usb

Данной командой выводится информация о подключенных USB-носителях.

Синтаксис

```
show usb
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show usb
USB device   Vendor      Product ID          Product version
----------   ---------   -----------------   ---------------
1-1          Flash       USB Disk            6.80
```

show version

Данная команда служит для просмотра текущей версии программного обеспечения и аппаратной части устройства.

Синтаксис

`show version`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show version
Boot version:
  1.0.7.16 (date 18/11/2015 time 13:40:59)
SW version:
  1.0.7 build 17[d9bdbda] (date 21/11/2015 time 18:06:41)
HW version:
  1v7
```

time-period

Данной командой задаётся период времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
time-period <TIME>
no time-period
```

Параметры

<TIME> – периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..35791394].

Значение по умолчанию

720 минут

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# time-period 1440
```

type

Данной командой устанавливается тип сохранения резервных конфигураций контроллера.

При использовании отрицательной формы команды (no) устанавливается режим по умолчанию.

Синтаксис

```
type <TYPE>
no type
```

Параметры

<TYPE> – тип сохранения резервных конфигураций контроллера. Принимает значения:

- local – сохранения резервных конфигураций происходит в раздел flash:backup/ с именем файла вида "config_YYYYMMDD_HHMMSS;" где:
  - YYYY – год, согласно системным часам контроллера на момент записи резервной копии конфигурации;
  - MM – месяц, согласно системным часам контроллера на момент записи резервной копии конфигурации;
  - DD – день, согласно системным часам контроллера на момент записи резервной копии конфигурации;
  - HH – час, согласно системным часам контроллера на момент записи резервной копии конфигурации;
  - MM – минута, согласно системным часам контроллера на момент записи резервной копии конфигурации;

    - SS – секунда, согласно системным часам контроллера на момент записи резервной копии конфигурации.
- remote – сохранения резервных конфигураций происходит на удаленный сервер;
- both – сохранения резервных конфигураций в раздел flash:backup и на удаленный сервер.

Значение по умолчанию

remote

Необходимый уровень привилегий

15

Командный режим

CONFIG-ARCHIVE

Пример:

```
wlc-30(config-archive)# type both
```

7 Настройка WLC

- enable
- wlc
- Настройки сервиса Airtune
  - airtune
    - enable
    - port
    - report
  - airtune-profile
    - 802.11k disable
    - 802.11r disable
    - 802.11r over-ds disable
    - 802.11r reassoc-deadline
    - away-timeout
    - blacklist threshold high
    - blacklist threshold low
    - blacklist timeout
    - client max-age
    - client rssi-renew
    - client try-no-balance
    - dca disable
    - dca threshold
    - eltex-rrm-scan disable
    - hd-mode
    - hysteresis
    - load-balance balance-enterprise disable
    - load-balance disable
    - load-balance sta high
    - load-balance sta low
    - optimization candidate
    - optimization mode
    - optimization time
    - report days-to-live
    - report disable
    - tpc disable
    - tpc rssi threshold
  - outside-address
- Настройка добавления точки доступа
  - ap
    - airtune-disable
    - ap-location
    - ap-model
    - ap-profile-override
    - board-profile-override
    - description
- Настройка профиля локации
  - ap-location
    - airtune-profile
    - ap-profile
    - board-profile
    - description
    - ssid-profile
    - timezone
- Настройка профиля общих настроек точек доступа
  - ap-profile

        - description
        - password
- Настройка профиля точки доступа конкретного типа
    - board-profile
        - ap-model
        - description
        - radio
            - autochannel
            - band
            - bandwidth
            - channel
            - dfs
            - limit-channels
            - tx-power
            - use-limit-channels
            - work-mode
- Настройка адресного пространства
    - ip-pool
        - ap-location
        - description
        - network
- Настройка фильтрации логов
    - log-filter
- Настройка использования портала
    - portal-profile
        - description
        - redirect-url
        - virtual-portal-name
- Настройка профиля для RADIUS-сервера
    - radius-profile
        - acct-address
        - acct-enable
        - acct-interval
        - acct-password
        - acct-periodic
        - acct-port
        - auth-acct-id-send
        - auth-address
        - auth-password
        - auth-port
        - description
        - domain
        - tls-enable
- Настройка SSID
    - ssid-profile
        - 802.11kv
        - 802.11r
        - ap-models
        - band
        - band-steer-mode
        - check-signal-enable
        - check-signal-timeout
        - description
        - enable
        - general-vlan-id
        - general-vlan-mode

        - hidden
        - inactivity-timeout
        - key-wpa
        - local-switching
        - minimal-signal
        - portal
        - portal-enabled
        - priority-by-dscp
        - radius
        - roaming-siganl
        - security-mode
        - ssid
        - sta-limit
        - station-isolation
        - vlan-id
        - vlan-priority
        - vlan-trunk
- Настройка менеджера обновления ПО
    - update-manager
        - end-time
        - scheduled
        - start-time
- Команды просмотра
    - show wlc
    - show wlc configuration warnings
    - show wlc connected-ap
    - show wlc connected-ap-clients
    - show wlc connected-ap-interfaces
    - show wlc connected-ap-radios
    - show wlc journal ap
    - show wlc journal clients
- Настройка логирования на точках доступа
    - autolog address
    - autolog enable
    - autolog logfile-limit
    - autolog period
    - autolog retry
    - syslog disable
    - syslog mode
    - syslog port
    - syslog server
    - syslog size
    - trace
        - acsd debug-5g
        - acsd debug-chanim
        - acsd debug-dfsr
        - acsd enable
        - acsd logfile
        - acsd logfile-limit
        - acsd loglevel
        - no acsd all
        - airtune enable
        - airtune logfile
        - airtune logfile-limit
        - airtune loglevel
        - no airtune all

- bandsteer enable
- bandsteer logfile
- bandsteer logfile-limit
- bandsteer loglevel
- bandsteer sta-mac
- no bandsteer all
- captive-portal enable
- captive-portal logfile
- captive-portal logfile-limit
- captive-portal loglevel
- no captive-portal all
- captive-portal apbd enable
- captive-portal apbd logfile
- captive-portal apbd logfile-limit
- captive-portal apbd loglevel
- no captive-portal apbd all
- captive-portal redirector-debug
- captive-portal tinyproxy enable
- captive-portal tinyproxy logfile
- captive-portal tinyproxy logfile-limit
- no captive-portal tinyproxy all
- configd enable
- configd logfile
- configd logfile-limit
- no configd all
- dmesg enable
- dmesg logfile
- dmesg logfile-limit
- no dmesg all
- ftd enable
- ftd logfile
- ftd logfile-limit
- no ftd all
- hostapd enable
- hostapd logfile
- hostapd logfile-limit
- hostapd loglevel
- no hostapd all
- monitord enable
- monitord logfile
- monitord logfile-limit
- monitord loglevel
- no monitord all
- netconf enable
- netconf logfile
- netconf logfile-limit
- networkd enable
- networkd logfile
- networkd logfile-limit
- networkd loglevel
- no networkd all
- snmp enable
- snmp logfile
- snmp logfile-limit
- no snmp all
- wlc-activator enable

- wlc-activator logfile
- wlc-activator logfile-limit
- no wlc-activator all
- wlc-activator server enable
- wlc-activator server logfile
- wlc-activator server logfile-limit
- no wlc-activator server all

enable

Данная команда предназначена для активации функций и сервисов контроллера или точек доступа.

Использование отрицательной формы команды (no) отключает функции.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-SSID-PROFILE

CONFIG-AIRTUNE

Пример

```
wlc(config-wlc)# enable
```

wlc

Данная команда осуществляет переход к конфигурированию контроллера.

Использование отрицательной формы команды (no) удаляет сконфигурированные настройки.

Синтаксис

```
[no] wlc
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc(config)# wlc
```

Настройки сервиса Airtune

airtune

Данная команда позволяет перейти в общие настройки сервиса Airtune.

Использование отрицательной формы команды (no) сбрасывает сделанные настройки в дефолт.

Синтаксис

```
[no] airtune
```

Параметры

Отсутствует.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# airtune
wlc(config-airtune)#
```

enable

Данная команда предназначена для активации функций и сервисов контроллера или точек доступа.

Использование отрицательной формы команды (no) отключает функции.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-SSID-PROFILE

CONFIG-AIRTUNE

Пример

```
wlc(config-wlc)# enable
```

port

Данная команда указывает номер порта, на котором работает сервис.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <NUMBER>
no port
```

Параметры

<NUMBER> – номер порта, принимает значения от 1024 до 65535.

Значение по умолчанию

8099

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE

Пример

```
wlc(config-airtune)# port 8099
```

report

Данная команда задает время удаления отчета.

Использование отрицательной формы команды (no) сбрасывает параметр на значение по умолчанию.

Синтаксис

```
report delete-time <HH:MM>
no report
```

Параметры

<HH:MM> – время удаления отчета, где первые две цифры указывают час, а вторые – минуты.

Значение по умолчанию

21:00

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE

Пример

```
wlc(config-airtune)# report delete-time 21:00
```

airtune-profile

Данная команда позволяет перейти в настройки профиля Airtune.

Использование отрицательной формы команды (no) сбрасывает параметры профиля к настройкам по умолчанию.

Синтаксис

```
airtune-profile <NAME>
no airtune { <NAME> | all }
```

Параметры

<NAME> – название профиля, задается строкой до 235 символов;

all – параметр для удаления всех профилей.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# airtune-profile test
wlc(config-airtune-profile)#
```

802.11k disable

Данная команда отключает синхронизацию списков для роуминга стандарта 802.11k.

Использование отрицательной формы команды (no) включает синхронизацию списков для роуминга стандарта 802.11k.

Роуминг по протоколу 802.11k может быть организован между любыми сетями (открытые/шифрованные). Если на точке доступа настроена работа по протоколу 802.11k, то, при подключении клиента, точка доступа передает ему список «дружественных» точек доступа, на которые клиент может переключиться в процессе роуминга. Список содержит информацию о MAC-адресах точек доступа и каналах, на которых они работают.

Использование 802.11k позволяет сократить время, которое клиент затрачивает на поиск другой сети при роуминге, так как клиенту не нужно производить сканирование каналов, на которых нет целевых точек доступа доступных для переключения.

Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11k.

Синтаксис

```
[no] 802.11k disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# 802.11k disable
```

802.11r disable

Данная команда отключает отправку ключей для роуминга стандарта 802.11r.

Использование отрицательной формы команды (no) включает отправку ключей для роуминга стандарта 802.11r.

Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11r.

Роуминг 802.11r возможен только между VAP с режимом безопасности WPA2-Personal и WPA2-Enterprise.

Синтаксис

```
[no] 802.11r disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# 802.11r disable
```

802.11r over-ds disable

Данная команда выключает функционал Over-DS стандарта 802.11r. Если параметр отключен, используется Over-Air.

Использование отрицательной формы команды (no). Включает функционал Over-DS стандарта 802.11r.

Синтаксис

```
[no] 802.11r over-ds disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# 802.11k over-ds disable
```

802.11r reassoc-deadline

Данная команда настраивает максимальный период времени в течение которого ТД должны обменяться данными о попытке роуминга клиента (RRB-пакеты). Если ответ на запрос по истечению таймаута не пришел, RRB-запрос на бесшовный роуминг считается неуспешным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
802.11r reassoc-deadline <TIME>
no 802.11r reassoc-deadline
```

Параметры

<TIME> – временной промежуток, доступны значения от 1000 до 268431360 миллисекунд.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# 802.11k reassoc-deadline 1000
```

away-timeout

Данная команда устанавливает защитный интервал для определения доступности ТД сервером, то есть допустимое время ожидания ТД в случае потери связи, по истечении которого сервис будет считать ТД отключенной от сервиса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
away-timeout <TIME>
no away-timeout
```

Параметры

<TIME> – временной интервал, допустимы значения от 10 до 3600 секунд.

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# away-timeout 120
```

blacklist threshold high

Данная команда устанавливает верхнюю границу окончания зоны устойчивого приема сигнала от клиента, то есть порог уровня RSSI от клиента, при превышении которого подключенный клиент будет считаться в "уверенной" зоне и поиск новой ТД не начнется в случае, если ТД не перегружена.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
blacklist threshold high <RSSI>
no blacklist threshold high
```

Параметры

<RSSI> – порог уровня RSSI, допустимы значения от -100 до 1 Дбм.

Значение по умолчанию

-65

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# blacklist threshold high -65
```

blacklist threshold low

Данная команда устанавливает нижнюю границу окончания зоны устойчивого приема сигнала от клиента, то есть порог уровня RSSI от клиента, в случае если уровень от клиента меньше указанного в данном параметре, клиент считается находящимся в "неуверенной" зоне. Сервис будет пытаться найти для клиента ТД с "уверенным" приемом, и последующим переключением клиента на целевую ТД.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
blacklist threshold low <RSSI>
no blacklist threshold low
```

Параметры

<RSSI> – порог уровня RSSI, допустимы значения от -100 до 1 Дбм.

Значение по умолчанию

-75

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# blacklist threshold low -75
```

blacklist timeout

Данная команда устанавливает время блокировки клиента, в течение которого работает балансировка.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
blacklist timeout <TIME>
no blacklist timeout
```

Параметры

<TIME> – временной интервал, допустимы значения от 5 до 3600 секунд.

Значение по умолчанию

30

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# blacklist timeout 30
```

client max-age

Данная команда устанавливает максимально допустимое время прошедшее с момента последнего prob-запроса от клиента.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
client max-age <TIME>
no client max-age
```

Параметры

<TIME> – временной интервал, допустимы значения от 0 до 300 секунд.

Значение по умолчанию

20

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# client max-age 20
```

client rssi-renew

Данная команда устанавливает защитный интервал для определения зоны приема сигнала от клиента.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
client rssi-renew <TIME>
no  client rssi-renew
```

Параметры

<TIME> – временной интервал, допустимы значения от 1 до 300 секунд.

Значение по умолчанию

15

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# client rssi-renew 15
```

client try-no-balance

Данная команда устанавливает количество игнорируемых попыток подключения, заблокированного клиента.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
client try-no-balance <COUNT>
no client try-no-balance
```

Параметры

<COUNT> – количество попыток, допустимы значения от 1 до 10.

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# client try-no-balance 2
```

dca disable

Данная команда выключает алгоритм автоматического распределения частотных каналов каждой точки доступа в сети, чтобы избежать интерференции между ними.

Использование отрицательной формы команды (no) активирует функционал динамического распределения каналов.

Синтаксис

```
[no] dca disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# dca disable
```

dca threshold

Данная команда устанавливает порог изменения каналов при динамическом распределении каналов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dca threshold <VALUE>
no dca threshold
```

Параметры

<VALUE> – порог изменения, допустимые значения от 0 до 99%

Значение по умолчанию

25

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# dca threshold 25
```

eltex-rrm-scan disable

Данная команда выключает ускоренное сканирование.

Использование отрицательной формы команды (no) включает ускоренное сканирование.

С включенным параметром ТД в один момент времени обмениваются специальными Action-фреймами в определенном частотном канале, который сообщил им сервис. По окончанию обмена передают сообщение на сервис с полученными результатами. Весь процесс оптимизации в таком режиме будет занимать не более пары минут вне зависимости от количества ТД в домене.

В случае отключенного параметра ТД по очереди сканируют все каналы, учитывают влияние конкурентных ТД. В данном случае время требуемое для оптимизации будет увеличиваться при увеличении количества ТД (на 1 ТД – 50-60 секунд).

Синтаксис

```
[no] eltex-rrm-scan disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# eltex-rrm-scan disable
```

hd-mode

Данная команда включает режим DCA-HD. Мощность ТД управляется только на ТД работающих на одинаковых каналах.

Использование отрицательной формы команды (no) выключает режим HD.

Синтаксис

```
[no] hd-mode
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# hd-mode
```

hysteresis

Данная команда устанавливает допустимую погрешность для частотного диапазона 2,4 ГГц или 5 ГГц. Разрешенная "погрешность" от порога, если полученный сигнал лежит в диапазоне RSSI Treshold+-2dbm, оптимизацию по мощности проводить не следует.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
hysteresis { 2g <VALUE> | 2g <VALUE> }
no hysteresis { 2g | 5g }
```

Параметры

<VALUE> – допустимая погрешность, допустимы значения от 1 до 10.

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# hysteresis 2g 2
```

load-balance balance-enterprise disable

Данная команда выключает балансировку клиентов enterprise-сетей между ТД.

Использование отрицательной формы команды (no) включает балансировку.

Функционал нужен для равномерного распределения клиентов между ТД, чтобы избежать перегрузки одной из ТД, если в зоне видимости клиента есть более свободная ТД.

Синтаксис

```
[no] load-balance balance-enterprise disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# load-balance balance-enterprise disable
```

load-balance disable

Данная команда выключает балансировку по всем ТД в домене, не зависимо от их фактического расположения.

Использование отрицательной формы команды (no) включает балансировку.

Функционал нужен для равномерного распределения клиентов между ТД, чтобы избежать перегрузки одной из ТД, если в зоне видимости клиента есть более свободная ТД.

Синтаксис

```
[no] load-balance disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# load-balance disable
```

load-balance sta high

Данная команда устанавливает порог количества подключенных клиентов на радиоинтерфейсе, при превышении которого точка будет считаться перегруженной.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
load-balance sta high <COUNT>
no load-balance sta high
```

Параметры

<COUNT> – количество клиентов, допустимы значения от 1 до 100.

Значение по умолчанию

20

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# load-balance sta high 20
```

load-balance sta low

Данная команда устанавливает порог количества подключенных клиентов на радиоинтерфейсе, при превышении которого сервис будет искать для новых клиентов более свободную ТД (если таковая не найдется, клиент продолжит работу на текущей точке доступа). Если количество клиентов меньше текущего порога – точка доступа считается свободной.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
load-balance sta low <COUNT>
no load-balance sta low
```

Параметры

<COUNT> – количество клиентов, допустимы значения от 1 до 100

Значение по умолчанию

20

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# load-balance sta low 5
```

optimization candidate

Данная команда позволяет выбрать режим балансировки и роуминга между всеми ТД, независимо от их фактического расположения или только между соседствующими ТД.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
optimization candidate [ neighbors | all ]
no optimization candidate
```

Параметры

neighbors – ТД будут сканировать эфир и определять какие ТД являются соседями, чтобы балансировать клиентов и осуществлять роуминг только между рядом стоящими ТД (меньше лишнего трафика в проводной сети, но больше в радио среде);

all – сервис использует функционал в рамках всего домена, даже если ТД находятся на большом расстоянии друг от друга (больше трафика в проводной сети, меньше в радио среде).

Значение по умолчанию

all

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# optimization candidate all
```

optimization mode

Данная команда позволяет выбрать параметр, по которому будет срабатывать оптимизация.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
optimization mode [ event | time | full | none ]
no optimization mode
```

Параметры

event – включение функционала оптимизации по событию:

- Добавление новой ТД в домен;
- Удаление ТД из домена;
- Пропадание связи до одной из ТД более 5 минут;
- Изменение конфигурации радио параметров на ТД в домене;

time – включение функционала оптимизации по указанному времени;

full – включение функционала оптимизации и по событию и по указанному времени;

none – выключении функционала оптимизации.

Значение по умолчанию

event

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# optimization mode event
```

optimization time

Данная команда позволяет указать время, по которому будет срабатывать оптимизация.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
optimization time <TIME>
no optimization time
```

Параметры

<TIME> – время срабатывания оптимизации, задаются в формате ЧЧ:ММ, где первые две цифры – это часы, вторые – минуты.

Значение по умолчанию

00:00

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# optimization time 00:00
```

report days-to-live

Данная команда указывает время жизни отчётов об оптимизации RRM.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
report days-to-live <DAYS>
no report days-to-live
```

Параметры

<DAYS> – время жизни отчетов, допустимы значения от 1 до 365 дней.

Значение по умолчанию

93

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# report days-to-live 93
```

report disable

Данная команда выключает генерацию отчетов работы RRM.

Использование отрицательной формы команды (no) включает генерацию отчетов RRM.

Синтаксис

```
[no] report disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# report disable
```

tpc disable

Данная команда выключает функцию автоматического управления мощностью.

Использование отрицательной формы команды (no) включает автоматическое управления мощностью.

Синтаксис

```
[no] tpc disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# report disable
```

tpc rssi threshold

Данная команда регулирует максимальный уровень сигнала, с которым соседние ТД могут видеть друг друга в диапазоне 2.4 ГГц или 5 ГГЦ. В соответствии от полученного уровня RSSI от соседней ТД, сервер

будет сравнивать его с RSSI Treshold и рекомендовать уменьшить (RSSI_ТД > RSSI_Treshold), либо увеличить мощность передатчика (RSSI_ТД < RSSI_Treshold).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
tpc rssi threshold { 2g <RSSI> | 5g <RSSI> }
```

Параметры

<RSSI> – максимальный уровень сигнала, Дбм, допустимые значения от -100 до -1.

Значение по умолчанию

2g: -70

5g: -65

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

Пример

```
wlc(config-airtune-profile)# tpc rssi threshold 2g -70
```

outside-address

Данная команда устанавливает IP-адрес контроллера, который будет доступен точкам доступа.

Использование отрицательной формы команды (no) удаляет заданный пароль.

Синтаксис

```
outside-address <ADDR>
no outside-address
```

Параметры

<ADDR> – IP-адрес контроллера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc-ip-pool)# outside-address 192.168.1.1
```

Настройка добавления точки доступа

ap

Данная команда добавляет в систему точку доступа по MAC-адресу.

Использование отрицательной формы команды (no) удаляет точку доступа.

Синтаксис

```
ap <MAC-ADDRESS>
no ap { <MAC-ADDRESS> | all }
```

Параметры

<MAC-ADDRESS> – mac-адрес точки доступа в формате HH:HH:HH:HH:HH:HH;

all – команда удаляет все добавленные точки доступа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# ap 00:00:00:00:00:00
```

airtune-disable

Данная команда отключает работу сервиса Airtune для выбранной точки доступа.

Использование отрицательной формы команды (no) включает работу сервиса Airtune для выбранной точки доступа.

Синтаксис

```
[no] airtune-disable
```

Параметры

Отсутствует.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP

Пример

```
wlc(config-wlc-ap)# airtune-disable
```

ap-location

Данная команда создает/назначает профиль локации, который описывает используемое оборудование и SSID.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
ap-location <NAME>
no ap-location { <NAME> | all }
```

Параметры

<NAME> – название профиля локации, задается строкой до 235 символов;

all – команда удаляет все созданные профили.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-AP

CONFIG-WLC-IP-POOL

Пример

```
wlc(config-wlc)# ap-location default
```

ap-model

Данная команда указывает модель точки доступа.

Использование отрицательной формы команды (no) удаляет установленное значение.

Синтаксис

```
ap-model <BOARD-TYPE>
no ap-model
```

Параметры

<BOARD-TYPE> – тип точки доступа, доступные значения:

- WEP-1L;
- WEP-2L;
- WEP-20L:
- WEP-3ax;
- WEP-3ax-Z;
- WOP-2L;
- WOP-20L;
- WOP-3ax.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP

CONFIG-WLC-BOARD-PROFILE

Пример

```
wlc(config-wlc-ap)# ap-model WEP-1L
```

ap-profile-override

Данная команда назначает профиль общих настроек точек доступа.

Использование отрицательной формы команды (no) удаляет назначенный профиль.

Синтаксис

```
ap-profile-override <PROFILE-NAME>
no ap-profile-override
```

Параметры

<PROFILE-NAME> – название существующего профиля общих настроек ap-profile, задается строкой до 235 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP

Пример

```
wlc(config-wlc-ap)# ap-profile-override common
```

board-profile-override

Данная команда назначает профиль настроек для точек доступа конкретного типа.

Использование отрицательной формы команды (no) удаляет назначенный профиль.

Синтаксис

```
board-profile-override <PROFILE-NAME>
no board-profile-override
```

Параметры

<PROFILE-NAME> – название существующего профиля настроек для точек доступа конкретного типа board-profiles, задается строкой до 235 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP

Пример

```
wlc(config-wlc-ap)# board-profile-override common
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

Настройка профиля локации

ap-location

Данная команда создает/назначает профиль локации, который описывает используемое оборудование и SSID.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
ap-location <NAME>
no ap-location { <NAME> | all }
```

Параметры

<NAME> – название профиля локации, задается строкой до 235 символов;

all – команда удаляет все созданные профили.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-AP

CONFIG- WLC-IP-POOL

Пример

```
wlc(config-wlc)# ap-location default
```

airtune-profile

Данная команда позволяет перейти в настройки профиля Airtune.

Использование отрицательной формы команды (no) сбрасывает сделанные настройки в дефолт.

Синтаксис

```
airtune-profile <NAME>
no airtune { <NAME> | all }
```

Параметры

<NAME> – название профиля, задается строкой до 235 символов;

all – параметр для удаления всех профилей.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# airtune-profile test
wlc(config-airtune-profile)#
```

ap-profile

Данная команда создает профиль общих настроек точек доступа всех типов в выбранной локации.

Использование отрицательной формы команды (no) удаляет профиль настроек.

Синтаксис

```
ap-profile <NAME>
no ap-profile { <NAME> | all }
```

Параметры

<NAME> – название профиля, задается строкой до 235 символов;

all – команда удаляет все добавленные профили настроек.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# ap-profile test
```

board-profile

Данная команда назначает профиль, описывающий используемое оборудование.

Использование отрицательной формы команды (no) удаляет заданный профиль.

Синтаксис

```
board-profile [BOARD-TYPE] <PROFILE-ID>
no board-profile { <BOARD-TYPE> | all }
```

Параметры

<BOARD-TYPE> – тип точки доступа, доступные значения:

- WEP-1L;
- WEP-2L;
- WEP-20L:
- WEP-3ax;
- WEP-3ax-Z;
- WOP-2L;
- WOP-20L;
- WOP-3ax.

<PROFILE-ID> – идентификатор профиля, задается строкой до 235 символов, и должен совпадать с названием описанного профиля из ap-profile;

all – команда удаляет все добавленные профили.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-LOCATION

Пример

```
wlc(config-wlc-ap-location)# board-profile WEP-1L default-wep1l
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-AP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

ssid-profile

Данная команда создает/назначает профиль SSID.

Использование отрицательной формы команды (no) удаляет SSID.

Синтаксис

```
ssid-profile <NAME> [<BRIDGE>]
no ssid-profile { <NAME> | all }
```

Параметры

<BRIDGE> – название bridge location, задается строкой до 235 символов;

<NAME> – название профиля SSID, задается строкой до 235 символов;

all – команда удаляет все добавленные профили SSID.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ap-location)# ssid test_ssid
```

timezone

Данная команда устанавливает часовой пояс для выбранной локации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timezone gmt <TIMEZONE>
[no] timezone
```

Параметры

<TIMEZONE> – часовой пояс, допустимые значения от -12 до +12.

Значение по умолчанию

Часовой пояс установлен из конфигурации WLC.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-ap-location)# timezone gmt +7
```

Настройка профиля общих настроек точек доступа

ap-profile

Данная команда создает профиль общих настроек точек доступа всех типов в выбранной локации.

Использование отрицательной формы команды (no) удаляет профиль настроек.

Синтаксис

```
ap-profile <NAME>
no ap-profile { <NAME> | all }
```

Параметры

<NAME> – название профиля, задается строкой до 235 символов;

all – команда удаляет все добавленные профили настроек.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# ap-profile test
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

password

Данная команда задает пароль для управления точкой доступа. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
password { ascii-text <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символов;

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# password password
```

Настройка профиля точки доступа конкретного типа

board-profile

Данная команда создает профиль, описывающий используемое оборудование.

Использование отрицательной формы команды (no) удаляет заданный профиль.

Синтаксис

```
board-profile <PROFILE-ID>
no board-profile { <PROFILE-ID> | all }
```

Параметры

<PROFILE-ID> – идентификатор профиля, задается строкой до 235 символов;

all – команда удаляет все добавленные профили.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# board-profiles default-wep1l
```

ap-model

Данная команда указывает модель точки доступа.

Использование отрицательной формы команды (no) удаляет установленное значение.

Синтаксис

```
ap-model <BOARD-TYPE>
no ap-model
```

Параметры

<BOARD-TYPE> – тип точки доступа, доступные значения:

- WEP-1L;
- WEP-2L;
- WEP-20L:
- WEP-3ax;
- WEP-3ax-Z;
- WOP-2L;
- WOP-20L;
- WOP-3ax.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP

CONFIG-WLC-BOARD-PROFILE

Пример

```
wlc(config-wlc-ap)# ap-model WEP-1L
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

radio

Данная команда осуществляет переход в режим конфигурирования радиоинтерфейса.

Использование отрицательной формы команды (no) отменяет сконфигурированные настройки для радиоинтерфейса.

Синтаксис

```
radio {wlan0 | wlan1}
no radio { wlan0 | wlan1 | all }
```

Параметры

all – команда удаляет настройки обоих радиоинтерфейсов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BOARD-PROFILE

Пример

```
wlc(config-wlc-board-profile)# radio wlan0
```

autochannel

Данная команда активирует автовыбор канала на радиоинтерфейсе.

Использование отрицательной формы команды (no) отключает использование автовыбора канала.

Синтаксис

```
[no] autochannel
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# autochannel
```

band

Данная команда назначает диапазон частот для радиоинтерфейса точки доступа.

Использование отрицательной формы команды (no) удаляет заданное значение диапазона частот.

Синтаксис

```
band { 2g | 5g }
no band
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-board-profile-radio)# band 2g
```

bandwidth

Данная команда назначает ширину канала для радиоинтерфейса точки доступа.

Использование отрицательной формы команды (no) удаляет заданное значение ширины канала.

Синтаксис

```
bandwidth { 20 | 40L | 40U | 80 | 160 }
no bandwith
```

Параметры

Отсутствует.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# bandwidth 20
```

channel

Данная команда назначает канал для радиоинтерфейса.

Использование отрицательной формы команды (no) отменяет использование заданного канала.

Синтаксис

```
channel <CHANNEL>
no channel
```

Параметры

<CHANNEL> – номер используемого канала, доступные значения:

Для диапазона 2g:

- [1.. 13];

Для диапазона 5g:

- 36;
- 40;
- 44;
- 48;
- 52;
- 56;
- 60;
- 64;
- 100;
- 104;
- 108;
- 112;
- 116;
- 120;
- 124;
- 128;
- 132;
- 136;
- 140;
- 144;
- 149;
- 153;
- 157;
- 161;
- 165.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# channel 36
```

dfs

Данная команда переключает режимы работы динамического выбора частоты.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dfs <DFS-STATUS>
no dfs
```

Параметры

<DFS-STATUS> – режим работы функционала, доступные значения:

- auto – механизм выключен. DFS-каналы не доступны для выбора;
- disables – механизм выключен. DFS-каналы не доступны для выбора;
- forced – механизм выключен. DFS-каналы доступны для выбора.

Значение по умолчанию

auto

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# dfs disabled
```

limit-channels

Данная команда создает ограниченный список каналов для работы автовыбора каналов.

Использование отрицательной формы команды (no) удаляет элемент списка.

Синтаксис

```
limit-channels <CHANNEL> <CHANNEL> <CHANNEL>
no limit-channels { <CHANNEL> | all }
```

Параметры

<CHANNEL> – номер используемого канала, доступные значения:

Для диапазона 2g:

- [1.. 13];

Для диапазона 5g:

- 36;
- 40;
- 44;
- 48;
- 52;
- 56;
- 60;
- 64;
- 100;
- 104;
- 108;
- 112;
- 116;
- 120;
- 124;

- 128;
- 132;
- 136;
- 140;
- 144;
- 149;
- 153;
- 157;
- 161;
- 165.

all – команда удаляет все добавленные каналы.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# limit-channels 1
```

tx-power

Данная команда устанавливает уровень мощности для радиоинтерфейса.

Использование отрицательной формы команды (no) удаляет заданное значение.

Синтаксис

```
tx-power <TX-POWER>
no tx-power
```

Параметры

<TX-POWER> – уровень мощности в дБм, принимает значения в диапазоне [6.. 19].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# tx-power 6
```

use-limit-channels

Данная команда активирует использование ограниченного списка каналов.

Использование отрицательной формы команды (no) отключает использование списка.

Синтаксис

```
[no] use-limit-channels
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# use-limit-channels
```

work-mode

Данная команда назначает режим работы радиоинтерфейса.

Использование отрицательной формы команды (no) удаляет значение параметра.

Синтаксис

```
work-mode <WORK-MODE>
no work-mode
```

Параметры

<WORK-MODE> – режим работы, доступные значения:

WEP-3ax, WEP-3ax-Z, WOP-3ax:

- bgn, ax, bgnax – для диапазона 2g;
- anac, anacax, a – для диапазона 5g;

WEP-1L, WEP-2L, WOP-2L, WEP-20L, WOP-20L:

- n, bg, bgn – для диапазона 2g;
- a, an, ac – для диапазона 5g.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-BOARD-PROFILE-RADIO

Пример

```
wlc(config-wlc-board-profile-radio)# work-mode ac
```

Настройка адресного пространства

ip-pool

Данная команда создает адресное пространство со списком разрешенных IP-адресов.

Использование отрицательной формы команды (no) удаляет адресное пространство.

Синтаксис

```
ip-pool <NAME>
no ip-pool { <NAME> | all }
```

Параметры

<NAME> – название адресного пространства, задается строкой до 235 символов;

all – команда удаляет все заданные адресные пространства.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# ip-pool test
```

ap-location

Данная команда создает/назначает профиль локации, который описывает используемое оборудование и SSID.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
ap-location <NAME>
no ap-location { <NAME> | all }
```

Параметры

<NAME> – название профиля локации, задается строкой до 235 символов;

all – команда удаляет все созданные профили.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-AP

CONFIG-WLC-IP-POOL

Пример

```
wlc(config-wlc)# ap-location default
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

network

Данная команда формирует список разрешенных IP-адресов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
network <ADDR/LEN>
no network
```

Параметры

<ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Значение по умолчанию

0.0.0.0/0

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-IP-POOL

Пример

```
wlc(config-wlc-ip-pool)# network 0.0.0.0/0
```

Настройка фильтрации логов

log-filter

Данная команда активирует фильтрацию отображения логов по одной или группе точек доступа.

Использование отрицательной формы команды (no) отключает функцию.

Синтаксис

```
log-filter <OBJECT-GROUP>
[no] log-filter
```

Параметры

<OBJECT-GROUP> – название object-group, задается строкой до 31 символа, должно совпадать с существующей object-group.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# log-filter test
```

Настройка использования портала

portal-profile

Данная команда настраивает использование портала.

Использование отрицательной формы команды (no) удаляет настройки портала.

Синтаксис

```
portal-profile <PORTAL-NAME>
no portal-profile [ <PORTAL-NAME> | all ]
```

Параметры

<PORTAL-NAME> – название портала, задается строкой до 235 символов;

all – команда удаляет все созданные порталы.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc)# portal-profile test
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

redirect-url

Данная команда назначает URL перенаправления на портал.

Использование отрицательной формы команды (no) удаляет заданный параметр.

Синтаксис

```
redirect-url <URL>
no redirect-url
```

Параметры

<URL> – URL перенаправления, задается строкой [8-255] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-PORTAL-PROFILE

Пример

```
wlc(config-wlc-portal-profile)#redirect-url http://softwlc.eltex.loc:8080/eltex_portal/
```

virtual-portal-name

Данная команда устанавливает имя портала.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
virtual-portal-name <PORTAL-NAME>
no virtual-portal-name
```

Параметры

<PORTAL-NAME> – имя портала, задается строкой до 235 символов.

Значение по умолчанию

default

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-PORTAL-PROFILE

Пример

```
wlc(config-wlc-portal-profile)# virtual-portal-name default
```

Настройка профиля для RADIUS-сервера

radius-profile

Данная команда назначает/настраивает использование RADIUS-сервера.

Использование отрицательной формы команды (no) отменяет назначение/настройки RADIUS-сервера.

Синтаксис

```
radius-profile <RADIUS-ID>
no radius-profile { <RADIUS-ID> | all }
```

Параметры

<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов;

all – команда удаляет все созданные RADIUS-сервера.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc)# radius-profile test
```

acct-address

Данная команда определяет IP-адрес RADIUS-сервера, используемого для аккаунтинга.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес.

Синтаксис

```
acct-address <ADDR>
no acct-address
```

Параметры

<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-address 192.168.1.1
```

acct-enable

Данная команда активирует отправку аккаунтинга на RADIUS-сервер.

Использование отрицательной формы команды (no) отключает отправку аккаунтинга.

Синтаксис

```
[no] acct-enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-enable
```

acct-interval

Данная команда задает временной интервал обновления аккаунтинга.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acct-interval <TIME>
no acct-interval
```

Параметры

<TIME> – промежуток времени в секундах, через который аккаунтинг будет обновлен, принимает значения [1.. 86400].

Значение по умолчанию

600 секунд.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-interval 600
```

acct-password

Данная команда указывает пароль авторизации для RADIUS-сервера, используемого для аккаунтинга. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет заданный пароль.

Синтаксис

```
acct-password {ascii-text <CLEAR-TEXT> | encrypted <HASH_SHA512>}
no acct-password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символа.

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-password password
```

acct-periodic

Данная команда активирует периодическое обновление аккаунтинга.

Использование отрицательной формы команды (no) отключает обновление аккаунтинга.

Синтаксис

```
[no] acct-periodic
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-periodic
```

acct-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аутентификации и авторизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acct-port <PORT>
no acct-port
```

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1813

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# acct-port 1813
```

auth-acct-id-send

Данная команда активирует передачу идентификатора сессии в запросах аккаунтинга.

Использование отрицательной формы команды (no) деактивирует функцию.

Синтаксис

```
[no] auth-acct-id-send
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# auth-acct-id-send
```

auth-address

Данная команда определяет IP-адрес RADIUS-сервера авторизации.

Использование отрицательной формы команды (no) удаляет заданный адрес.

Синтаксис

```
auth-address <ADDR>
no auth-address
```

Параметры

<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# auth-address 192.168.1.1
```

auth-password

Данная команда указывает пароль авторизации для RADIUS-сервера, который используется для авторизации и аутентификации. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет заданный пароль.

Синтаксис

```
auth-password { ascii-text <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no auth-password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символа;

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# auth-password password
```

auth-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аутентификации и авторизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
auth-port <PORT>
no auth-port
```

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1813

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# auth-port 1812
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

domain

Данная команда создает/назначает домен.

Использование отрицательной формы команды (no) удаляет домен.

Синтаксис

```
domain <DOMAIN>
no domain
```

Параметры

<DOMAIN> – идентификатор домена, задается строкой до 235 символов.

Значение по умолчанию

root

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# domain root
```

tls-enable

Данная команда активирует использование TLS при авторизации.

Использование отрицательной формы команды (no) отключает функцию.

Синтаксис

```
[no] tls-enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-RADIUS-PROFILE

Пример

```
wlc(config-wlc-radius-profile)# tls-enable
```

Настройка SSID

ssid-profile

Данная команда создает/назначает профиль SSID.

Использование отрицательной формы команды (no) удаляет SSID.

Синтаксис

```
ssid-profile <NAME> [<BRIDGE>]
no ssid-profile { <NAME> | all }
```

Параметры

<BRIDGE> – название bridge location, задается строкой до 235 символов;

<NAME> – название профиля SSID, задается строкой до 235 символов;

all – команда удаляет все добавленные профили SSID.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC
CONFIG-WLC-AP-LOCATION
CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ap-location)# ssid test_ssid
```

802.11kv

Данная команда активирует работу по стандартам 802.11k/v.
Использование отрицательной формы команды (no) отключает работу по стандартам 802.11k/v.

Синтаксис

`[no] 802.11kv`

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# 802.11kv
```

802.11r

Данная команда активирует работу по стандарту 802.11k.
Использование отрицательной формы команды (no) включает отключает работу по стандарту 802.11r.

Синтаксис

```
[no] 802.11r
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# 802.11r
```

ap-models

Данная команда ограничивает список моделей точек доступа, на которые будет применен ssid-profile. Список моделей определяется в профиле object-group ap-models.

Использование отрицательной формы команды (no) удаляет список.

Синтаксис

```
ap-models <OBJECT-GROUP>
no ap-models
```

Параметры

<OBJECT-GROUP> – название списка моделей, определенных в object-group ap-models, задается строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# ap-models group_models
```

band

Данная команда назначает диапазон частот для радиоинтерфейса точки доступа.

Использование отрицательной формы команды (no) удаляет заданное значение диапазона частот.

Синтаксис

```
band { 2g | 5g }
no band
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-RADIO

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ap-profile-radio)# band 2g
```

band-steer-mode

Данная команда активирует на точках доступа функцию приоритетного подключения двухдиапазонных беспроводных клиентов к сети в 5 ГГц. Для работы функции необходимо, чтобы в ssid-profile были включены оба диапазона: band 5g и band 2g.

Использование отрицательной формы команды (no) деактивирует функцию.

Синтаксис

```
[no] band-steer-mode
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc-30(config-wlc-ssid-profile)# band-steer-mode
```

check-signal-enable

Данная команда включает периодическую проверку сигнала.

Использование отрицательной формы команды (no) отменяет периодическую проверку сигнала.

Синтаксис

```
[no] check-signal-enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# check-signal-enable
```

check-signal-timeout

Данная команда устанавливает время, через которое будет производиться периодическая проверка сигнала.

Использование отрицательной формы команды (no) отменяет периодическую проверку сигнала.

Синтаксис

```
[no] check-signal-enable
```

Параметры

Отсутствуют.

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ddid)# check-signal-timeout 10
```

description

Данная команда добавляет описание для блоков конфигурации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
[no] description <DESCRIPTION>
```

Параметры

<DESCRIPTION> – произвольное описание задается строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AIRTUNE-PROFILE

CONFIG-WLC-AP

CONFIG-WLC-AP-PROFILE

CONFIG-WLC-IP-POOL

CONFIG-WLC-AP-LOCATION

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-RADIUS-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ip-pool)# description default_test_pool
```

enable

Данная команда предназначена для активации функций и сервисов контроллера или точек доступа.

Использование отрицательной формы команды (no) отключает функции.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-SSID-PROFILE

CONFIG-AIRTUNE

Пример

```
wlc(config-wlc)# enable
```

general-vlan-id

Данная команда устанавливает идентификатор General VLAN.

Использование отрицательной формы команды (no) удаляет заданный идентификатор.

Синтаксис

```
general-vlan-id <ID>
no general-vlan-id
```

Параметры

<ID> – идентификатор General VLAN, принимает значения в диапазоне [0-4094] ("0" предназначен для удаления параметра).

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# general-vlan-id 1
```

general-vlan-mode

Данная команда активирует использование General VLAN.

Использование отрицательной формы команды (no) деактивирует использование General VLAN.

Синтаксис

```
[no] general-vlan-mode
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# general-vlan-mode
```

hidden

Данная команда скрывает SSID.

Использование отрицательной формы команды (no) деактивирует функционал.

Синтаксис

```
[no] hidden
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# hidden
```

inactivity-timeout

Данная команда устанавливает время бездействия, после которого пользователь будет считаться неактивным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
inactivity-timeout <TIMEOUT>
no inactivity-timeout
```

Параметры

<TIMEOUT> – временной промежуток, принимает значения в диапазоне [0-86400].

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# inactivity-timeout 120
```

key-wpa

Данная команда устанавливает ключ/пароль для подключения к виртуальной точке доступа. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет заданный ключ.

Синтаксис

```
key-wpa { ascii-text <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no key-wpa
```

Параметры

<CLEAR-TEXT> – ключ, задаётся строкой [8-63] символа;

<HASH_SHA512> – хеш ключа по алгоритму sha512, задаётся строкой [16-126] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# key-wpa password
```

local-switching

Данная команда активирует функцию local-switching.

Использование отрицательной формы команды (no) отключает функцию.

Синтаксис

`[no] local-switching`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# local-switching
```

minimal-signal

Данная команда устанавливает пороговое значение RSSI, при достижении которого точка доступа будет отключать клиента от виртуальной точки доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
minimal-signal <RSSI>
no minimal-signal
```

Параметры

<RSSI> – пороговое значение RSSI, принимает значения в диапазоне [-100.. 0].

Значение по умолчанию

-100

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# minimal-signal -100
```

portal

Данная команда настраивает использование портала.

Использование отрицательной формы команды (no) удаляет настройки портала.

Синтаксис

```
portal <PORTAL-NAME>
no portal [ <PORTAL-NAME> | all ]
```

Параметры

<PORTAL-NAME> – название портала, задается строкой до 235 символов;

all – команда удаляет все созданные порталы.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc)# portal test
```

portal-enabled

Данная команда активирует портальную авторизацию.

Использование отрицательной формы команды (no) деактивирует функцию.

Синтаксис

```
[no] portal-enabled
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# portal-enabled
```

priority-by-dscp

Данная команда активирует на точках доступа анализ приоритета из поля DSCP заголовка IP-пакета для распределения трафика, передающегося в радиоинтерфейс, по очередям WMM. Если значение DSCP в тегированных кадрах равно 0, то анализироваться будет приоритет из поля CoS (Class of Service).

Использование отрицательной формы команды (no) отключает анализ приоритета по полю DSCP. В таком случае будет анализироваться приоритет из поля CoS (802.1p) тегированных кадров.

Синтаксис

```
[no] priority-by-dscp
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# priority-by-dscp
```

radius

Данная команда назначает/настраивает использование RADIUS-сервера.

Использование отрицательной формы команды (no) отменяет назначение/настройки RADIUS-сервера.

Синтаксис

```
radius <RADIUS-ID>
no radius { <RADIUS-ID> | all }
```

Параметры

<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов;

all – команда удаляет все созданные RADIUS-сервера.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

CONFIG-WLC-PORTAL-PROFILE

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc)# radius test
```

roaming-siganl

Данная команда устанавливает уровень RSSI, при достижении которого будет срабатывать роуминг.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
roaming-siganl <RSSI>
no roaming-siganl
```

Параметры

<RSSI> – уровень RSSI, принимает значения от -100 до -1.

Значение по умолчанию

-100

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# roaming-signal -100
```

security-mode

Данная команда устанавливает режим безопасности на виртуальной точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security-mode <MODE>
no security-mode
```

Параметры

<MODE> – режим безопасности, доступные значения:

- WPA;
- WPA2;
- WPA2_1X;
- WPA3;
- WPA_1X;
- WPA_WPA2;
- WPA_WPA2_1X;
- off.

Значение по умолчанию

off

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# security-mode WPA
```

ssid

Данная команда задает имя SSID, которое будет вещаться пользователям.

Использование отрицательной формы команды (no) удаляет название SSID.

Синтаксис

```
ssid <NAME>
no ssid
```

Параметры

<NAME> – название SSID, задается строкой до 32 символов. Названия, содержащие пробел, необходимо заключать в кавычки.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# ssid 'test ssid'
```

sta-limit

Данная команда задает максимальное число пользователей, которые могут подключиться к виртуальной точке доступа.

Использование отрицательной формы команды (no) назначает значение по умолчанию.

Синтаксис

```
sta-limit <LIMIT>
no sta-limit
```

Параметры

<LIMIT> – максимальное число пользователей, принимает значения в диапазоне [0-64] ("0" служит для отключения ограничения).

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# sta-limit 64
```

station-isolation

Данная команда активирует изоляцию трафика между клиентами в пределах одной виртуальной точки доступа.

Использование отрицательной формы команды (no) отключает изоляцию.

Синтаксис

```
[no] station-isolation
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# station-isolation
```

vlan-id

Данная команда назначает vlan на виртуальную точку доступа.

Использование отрицательной формы команды (no) применяет значение по умолчанию.

Синтаксис

```
vlan-id <ID>
no vlan-id
```

Параметры

<ID> – идентификатор vlan-a, принимает значения в диапазоне [0-4094].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# vlan-id 1111
```

vlan-priority

Данная команда назначает приоритет на клиентский трафик.

Использование отрицательной формы команды (no) применяет значение по умолчанию.

Синтаксис

```
vlan-priority <PRIORITY>
no vlan-priority
```

Параметры

<PRIORITY> – приоритет, доступные значения:

- auto;
- значения из диапазона [0.. 7].

Значение по умолчанию

auto

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# vlan-priority auto
```

vlan-trunk

Данная команда активирует функцию Vlan Trunk.

Использование отрицательной формы команды (no) деактивирует функцию.

Синтаксис

```
[no] vlan-trunk
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-SSID-PROFILE

Пример

```
wlc(config-wlc-ssid-profile)# vlan-trunk
```

Настройка менеджера обновления ПО

update-manager

Данная команда осуществляет переход в режим настройки менеджера обновления ПО точек доступа по расписанию.

Использование отрицательной формы команды (no) удаляет сконфигурированные настройки.

Синтаксис

```
[no] update-mgr
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC

Пример

```
wlc(config-wlc)# update-mgr
```

end-time

Данная команда задает окончание временного интервала, в котором производится обновление ПО точек доступа, когда включен менеджер обновления ПО по расписанию (update-mgr).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
end-time <TIME>
no end-time
```

Параметры

<TIME> – окончание интервала времени, в который производится обновление ПО точек доступа, задаётся в виде HH:MM, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59].

Значение по умолчанию

04:00

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-UPDATE-MANAGER

Пример

scheduled

Данная команда активирует работу менеджера обновления ПО точек доступа по расписанию.

Использование отрицательной формы команды (no) отключает менеджер обновления ПО по расписанию.

Синтаксис

```
[no] scheduled
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-UPDATE-MANAGER

Пример

```
wlc(config-wlc-update-manager)# scheduled
```

start-time

Данная команда задает начало временного интервала, в котором производится обновление ПО точек доступа, когда включен менеджер обновления ПО по расписанию (update-mgr).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
start-time <TIME>
no start-time
```

Параметры

<TIME> – начало интервала времени, в который производится обновление ПО точек доступа, задаётся в виде HH:MM, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59].

Значение по умолчанию

03:00

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-UPDATE-MANAGER

Пример

```
wlc(config-wlc-update-manager)# start-time 05:00
```

Команды просмотра

show wlc

Данная команда используется для просмотра общей информации о работе WLC. В выводе содержится общее количество точек доступа; количество точек доступа, находящихся в определенном статусе; общее количество беспроводных клиентов, подключенных ко всем точкам доступа, находящимся под управлением контроллера, и количество клиентов, подключенных в каждом частотном диапазоне; общее количество SSID и количество SSID, работающих в каждом частотном диапазоне.

Синтаксис

```
show wlc
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh wlc
    AP Status          Count
    ---------------    --------
    Active             2
    Failed             0
    Applying cfg       0
    Cfg Failed         0
    Ready              0
    Rebooting          0
    Registering        0
    Sandboxed          0
    Updating creds     0
    Upgrading FW       0
    ---------------    --------
    Total              2


    Clients            Count
    ---------------    --------
    Clients 2g         0
    Clients 5g         0
    ---------------    --------
    Total              0


    SSIDs              Count
    ---------------    --------
    SSIDs 2g           4
    SSIDs 5g           3
   ---------------    --------
    Total              7
```

show wlc configuration warnings

Данная команда используется для просмотра предупреждений о проблемах, связанных с применением заданной конфигурации на точки доступа.

Синтаксис

```
show wlc configuration warnings
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc configuration warnings
No     Message
----   ------------------------------------------------------------
  0    Cannot apply ssid 'test' to radio 'wlan0' on
       'cc:9d:a2:c7:c6:50'
  1    Cannot apply ssid 'test' to radio 'wlan1' on
       'cc:9d:a2:c7:c6:50'
```

show wlc connected-ap

Данная команда используется для просмотра информации о точках доступа, обслуживаемых контроллером. Вывод содержит MAC-адрес, IP-адрес точки доступа, модель точки доступа, версию программного обеспечения, статус, количество клиентов и другую информацию.

Синтаксис

```
show wlc connected-ap [<AP-MAC>] [detailed] [detailed <AP-MAC>]
```

Параметры

<AP-MAC> – MAC-адрес точки доступа. При указании данного параметра будет отображена информация только по заданной точке доступа.

detailed – просмотр подробной информации по одной или всем точкам доступа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh wlc connected-ap
MAC address         IP address        Board type         SW version         State
Uptime             Clients
-----------------   ---------------   ----------------   ----------------   ----------------
----------------   -------
cc:9d:a2:c7:c6:50   192.168.1.4       WEP-3ax            1.8.0 build 59     Active
000d, 01:50:42     0
e8:28:c1:da:c9:b0   192.168.1.3       WEP-1L             1.6.0 build 112    Upgrading FW
000d, 00:00:28     0
wlc-30#
wlc-30# sh wlc connected-ap detailed cc:9d:a2:c7:c6:50
AP cc:9d:a2:c7:c6:50:
    MAC address:              cc:9d:a2:c7:c6:50
    IP address:               192.168.1.4
    Board type:               WEP-3ax
    SW version:               1.8.0 build 59
    Serial number:            WP42001853
    HW version:               2v1
    State:                    Active
    State description:        --
    First activity at:        2022.10.19 18:42
    Connected at:             2022.10.19 18:42
    Last activity at:         2022.10.19 18:42
    Clients:                  0
    Configured as:            ip-pool default-ip-pool
    Netconf connection state: Alive
    Description:              default-ip-pool
    Uptime:                   1 hour, 51 minutes and 3 seconds
```

show wlc connected-ap-clients

Данная команда используется для просмотра информации о подключенных к точке доступа беспроводных клиентах.

Синтаксис

```
show wlc connected-ap-clients <AP-MAC> [detailed | <CLIENT-MAC>]
```

Параметры

<AP-MAC> – MAC-адрес точки доступа в формате HH:HH:HH:HH:HH:HH. Будет выведен список клиентов указанной точки доступа;

detailed – просмотр подробной информации о всех беспроводных клиентах указанной точки доступа;

<CLIENT-MAC> – MAC-адрес беспроводного клиента в формате HH:HH:HH:HH:HH:HH. При указании данного параметра будет отображена информация только об указанном клиенте.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc connected-ap-clients cc:9d:a2:c7:c6:50
MAC address         IP address          SSID              Uptime       RSSI      SNR       Mode
LQ     Username
-----------------   -----------------   ---------------   ----------   -------   -------   ----
----   ---------------
72:34:84:e4:d2:05   192.168.2.3         default-ssid      00:00:03     -45 -41   49 55     ac
100    tester
60:ab:67:ba:89:24   192.168.2.2         default-ssid      00:16:10     -35 -40   59 56     ac
100    tester

wlc-30# show wlc connected-ap-clients cc:9d:a2:c7:c6:50  60:ab:67:ba:89:24
Client client-1:
    MAC address:              60:ab:67:ba:89:24
    IP address:               192.168.2.2
    Hostname:                 Redmi-Note-8-Pro
    SSID:                     default-ssid
    Interface:                wlan1-vap0
    RSSI:                     -39 -44
    SNR:                      57 52
    Transmit rate:            VHT NSS1-MCS8 SGI 86.7
    Receive rate:             OFDM 6
    Wireless mode:            ac
    Authorized:               false
    Username:                 tester
    Domain:                   default
    Link Quality:             100
    Link Quality Common:      0
    Actual transmit rate:     0
    Actual receive rate:      0
    Transmit bytes:           269583
    Receive bytes:            389565
    Transmit packets:         1262
    Receive packets:          2670
    Uptime:                   00:16:31
    Transmit bandwidth:       20
    Receive bandwidth:        20
```

show wlc connected-ap-interfaces

Данная команда используется для просмотра информации и счетчиков по интерфейсам точки доступа.

Синтаксис

```
show wlc connected-ap-interfaces <AP-MAC> [<IF-NAME>]
```

Параметры

<AP-MAC> – MAC-адрес точки доступа в формате HH:HH:HH:HH:HH:HH. Будет выведена информация и статистика по интерфейсам указанной точки доступа;

<IF-NAME> – название интерфейса точки доступа, задается строкой до 15 символов. При указании данного параметра будет отображена статистика только по указанному интерфейсу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc connected-ap-interfaces e8:28:c1:da:c9:b0
Interface    MAC address         State     RX bytes   RX packets    RX errors   RX drops
----------   ------------        -------   --------   -----------   ----------  ---------
br0          e8:28:c1:da:c9:b0   Up        0          0             0           0
eth0         e8:28:c1:da:c9:b0   Up        33691      299           0           0
lsw          e8:28:c1:da:c9:b1   Up        0          0             0           0
user-gre     e8:28:c1:da:c9:b2   Up        0          0             0           0
wlan0        e8:28:c1:da:c9:b0   Up        0          0             0           0
wlan0-va0    e8:28:c1:da:c9:b1   Up        0          0             0           0
wlan0-va1    00:e0:4c:81:86:86   Down      0          0             0           0
wlan0-va2    00:e0:4c:81:86:86   Down      0          0             0           0
wlan0-va3    00:e0:4c:81:86:86   Down      0          0             0           0
wlan1        e8:28:c1:da:c9:b5   Up        0          0             0           0
wlan1-va0    e8:28:c1:da:c9:b6   Up        0          0             0           0
wlan1-va1    00:e0:4c:81:86:86   Down      0          0             0           0
wlan1-va2    00:e0:4c:81:86:86   Down      0          0             0           0
wlan1-va3    00:e0:4c:81:86:86   Down      0          0             0           0

Interface     MAC address          State     TX bytes   TX packets   TX errors    TX drops
-----------   -----------------    -------   ---------  ----------   ----------   ---------
br0           e8:28:c1:da:c9:b0    Up        0          0            0             0
eth0          e8:28:c1:da:c9:b0    Up        88245      273          0             0
lsw           e8:28:c1:da:c9:b1    Up        0          0            0             0
user-gre      e8:28:c1:da:c9:b2    Up        0          0            0             0
wlan0         e8:28:c1:da:c9:b0    Up        0          0            0             0
wlan0-va0     e8:28:c1:da:c9:b1    Up        0          0            0             0
wlan0-va1     00:e0:4c:81:86:86    Down      0          0            0             0
wlan0-va2     00:e0:4c:81:86:86    Down      0          0            0             0
wlan0-va3     00:e0:4c:81:86:86    Down      0          0            0             0
wlan1         e8:28:c1:da:c9:b5    Up        0          0            0             0
wlan1-va0     e8:28:c1:da:c9:b6    Up        0          0            0             0
wlan1-va1     00:e0:4c:81:86:86    Down      0          0            0             0
wlan1-va2     00:e0:4c:81:86:86    Down      0          0            0             0
wlan1-va3     00:e0:4c:81:86:86    Down      0          0            0             0
```

```
wlc-30# show wlc connected-ap-interfaces e8:28:c1:da:c9:b0 wlan0-va0
Interface wlan0-va0:
    MAC address:              e8:28:c1:da:c9:b1
    Operational state:        Up
    Link speed:               144444444
    Duplex:                   unavailable
    Actual transmit rate:     0
    Actual receive rate:      0
    Transmit bytes:           0
    Receive bytes:            0
    Transmit packets:         0
    Receive packets:          0
    Transmit errors:          0
    Receive errors:           0
    Transmit drops:           0
    Receive drops:            0
```

show wlc connected-ap-radios

Данная команда используется для просмотра основных параметров радиоинтерфейсов точки доступа.

Синтаксис

```
show wlc connected-ap-radios <AP-MAC> [<IF-NAME>]
```

Параметры

<AP-MAC> – MAC-адрес точки доступа в формате HH:HH:HH:HH:HH:HH. Будет выведена информация о радиоинтерфейсах указанной точки доступа;

<IF-NAME> – название радиоинтерфейса точки доступа, задается строкой до 15 символов. При указании данного параметра будет отображена информация только по указанному радиоинтерфейсу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc connected-ap-radios e8:28:c1:da:c9:b0
Radio wlan0:
    Band:                       2.4
    MAC address:                e8:28:c1:da:c9:b0
    Status:                     Enabled
    Channel:                    11
    Frequency:                  2462
    Bandwidth:                  20
    TX power:                   16
--------------------------------------------------------------------------------
Radio wlan1:
    Band:                       5
    MAC address:                e8:28:c1:da:c9:b5
    Status:                     Enabled
    Channel:                    48
    Frequency:                  5240
    Bandwidth:                  20
    TX power:                   19

wlc-30# show wlc connected-ap-radios e8:28:c1:da:c9:b0 wlan1
Radio wlan1:
    Band:                       5
    MAC address:                e8:28:c1:da:c9:b5
    Status:                     Enabled
    Channel:                    48
    Frequency:                  5240
    Bandwidth:                  20
    TX power:                   19
```

show wlc journal ap

Данная команда используется для просмотра информации о процессе подключения к контроллеру, обновлении и конфигурировании точек доступа.

Синтаксис

```
show wlc journal ap [<AP-MAC>]
```

Параметры

<AP-MAC> – MAC-адрес точки доступа в формате HH:HH:HH:HH:HH:HH. Будет выведен журнал с информацией об указанной точки доступа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc journal ap
2022-08-11T15:28:10+00:00 AP e8:28:c1:da:c9:b0 changed state to 'Registering'
2022-08-11T15:28:11+00:00 AP e8:28:c1:da:c9:b0 changed state to 'Registering'
2022-08-11T15:28:12+00:00 AP e8:28:c1:da:c9:b0 changed state to 'Ready'
2022-08-11T15:28:13+00:00 AP e8:28:c1:da:c9:b0 connected, board 'WEP-1L' sw version '1.2.6
build 5' ipaddr '192.168.1.2'
2022-08-11T15:28:13+00:00 AP e8:28:c1:da:c9:b0 changed state to 'Applying cfg'
2022-08-11T15:28:13+00:00 AP e8:28:c1:da:c9:b0 changed state to 'Active'
```

show wlc journal clients

Данная команда используется для просмотра журнала подключений клиентов.

Синтаксис

```
show wlc journal clients [<CLIENT-MAC>]
```

Параметры

<CLIENT-MAC> – MAC-адрес беспроводного клиента в формате HH:HH:HH:HH:HH:HH. При указании данного параметра будет отображена информация в журнале только об указанном клиенте.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wlc journal clients
2022-09-14T13:30:17+00:00 client 60:ab:67:ba:89:24 Failed on AP cc:9d:a2:c7:c6:50 SSID test
reason 69, 'Incorrect password'
2022-09-14T13:30:34+00:00 client 60:ab:67:ba:89:24 Connected on AP cc:9d:a2:c7:c6:50 SSID test
RSSI: -46,-48
2022-09-14T13:30:52+00:00 client 60:ab:67:ba:89:24 Disconnected on AP cc:9d:a2:c7:c6:50 SSID
test reason 3, 'Sending station is leaving (or has left) IBSS or ESS'
```

Настройка логирования на точках доступа

autolog address

Данной командой задается IP-адрес TFTP-сервера для автоматической выгрузки логов с точки доступа.

Использование отрицательной формы команды (no) удаляет IP-адрес TFTP-сервера для автовыгрузки логов.

Синтаксис

```
address <ADDR>
no address
```

Параметры

<ADDR> – IP-адрес TFTP-сервера задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

config-wlc-ap-profile

Пример

```
wlc(config-wlc-ap-profile)# address 192.168.1.1
```

autolog enable

Данная команда включает автовыгрузку логов с точки доступа.

Использование отрицательной формы команды (no) отключает автовыгрузку.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# enable
```

autolog logfile-limit

Данная команда устанавливает пороговое значение размера папки с логами на точке доступа (/var/log/), при превышении которого логи будут автоматически выгружены на заданный TFTP-сервер при включенной опции autolog.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
logfile-limit <LIMIT>
no logfile-limit
```

Параметры

<LIMIT> – пороговое значение размера папки с логами на точке доступа, принимает значение в диапазоне [0..20000] КБ.

Значение по умолчанию

10000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# logfile-limit 5000
```

autolog period

Данная команда устанавливает период отправки логов с точки доступа на TFTP-сервер при включенной опции autolog.

Использование отрицательной формы команды (no) сбрасывает параметр на значение по умолчанию.

Синтаксис

```
period <TIME>
no period <TIME>
```

Параметры

<TIME> – интервал времени в секундах, через который будет происходить автоматическая выгрузка логов, принимает значения [1.. 86400].

Значение по умолчанию

600

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# period 3600
```

autolog retry

Данная команда устанавливает количество повторов отправки логов с точки доступа на TFTP-сервер при включенной опции autolog.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
retry <COUNT>
no retry
```

Параметры

<COUNT> – количество повторов отправки логов, допустимые значения [0..5].

Значение по умолчанию

3

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# retry 5
```

syslog disable

Данная команда отключает syslog на точке доступа.

Использование отрицательной формы команды (no) включает syslog.

Синтаксис

```
[no] disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# disable
```

syslog mode

Данная команда устанавливает режим работы сервиса syslog на точках доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
mode { File | ServerAndFile }
no mode
```

Параметры

File – запись syslog будет производиться только в локальный файл на точке доступа в директории /var/log/;

ServerAndFile – syslog будет записываться в файл на точке доступа и отправляться на заданный syslog сервер.

Значение по умолчанию

File

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# mode ServerAndFile
```

syslog port

Данная команда указывает номер порта сервера для отправки syslog.

Использование отрицательной формы команды (no) сбрасывает параметр на значение по умолчанию.

Синтаксис

```
port <NUMBER>
no port
```

Параметры

<NUMBER> – номер порта, принимает значения от 1 до 65535.

Значение по умолчанию

514

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# port 5555
```

syslog server

Данной командой задается адрес syslog сервера для отправки лога с точки доступа.

Использование отрицательной формы команды (no) удаляет адрес сервера.

Синтаксис

```
server <ADDR>
no server
```

Параметры

<ADDR> – IP-адрес или доменное имя сервера syslog.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# server 192.168.1.1
```

syslog size

Данная команда устанавливает размер файла syslog на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
size <LIMIT>
no size
```

Параметры

<LIMIT> – максимальный размер файла syslog на точке доступа, принимает значение в диапазоне [0..1000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# size 500
```

trace

Данная команда осуществляет переход к настройке трассировок точек доступа.

Использование отрицательной формы команды (no) удаляет сконфигурированные настройки.

Синтаксис

```
[no] trace
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE

Пример

```
wlc(config-wlc-ap-profile)# trace
```

acsd debug-5g

Данная команда включает дополнительное логирование для модуля 5 GHz подсистемы автовыбора радиочастотного канала на точке доступа.

Использование отрицательной формы команды (no) отключает дополнительное логирование.

Синтаксис

```
[no] acsd debug-5g
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd debug-5g
```

acsd debug-chanim

Данная команда включает дополнительное логирование для модуля chanim подсистемы автовыбора радиочастотного канала на точке доступа.

Использование отрицательной формы команды (no) отключает дополнительное логирование.

Синтаксис

```
[no] acsd debug-chanim
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd debug-chanim
```

acsd debug-dfsr

Данная команда включает дополнительное логирование для модуля DFSr подсистемы автовыбора радиочастотного канала на точке доступа.

Использование отрицательной формы команды (no) отключает дополнительное логирование.

Синтаксис

```
[no] acsd debug-dfsr
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd debug-dfsr
```

acsd enable

Данная команда включает логирование подсистемы автовыбора радиочастотного канала на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] acsd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd enable
```

acsd logfile

Данная команда задает название файла лога подсистемы автовыбора радиочастотного канала на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acsd logfile <FILENAME>
no acsd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

acsd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd logfile acsd.log
```

acsd logfile-limit

Данная команда устанавливает размер файла лога подсистемы автовыбора радиочастотного канала на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acsd logfile-limit <LIMIT>
no acsd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd logfile-limit 2000
```

acsd loglevel

Данная команда устанавливает уровень логирования для подсистемы автовыбора радиочастотного канала на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acsd loglevel { error | warn | info | debug }
no acsd loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# acsd loglevel error
```

no acsd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы автовыбора радиочастотного канала на точке доступа.

Синтаксис

```
no acsd all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no acsd all
```

airtune enable

Данная команда включает логирование агента централизованного радиопланирования на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] airtune enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# airtune enable
```

airtune logfile

Данная команда задает название файла лога агента централизованного радиопланирования на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
airtune logfile <FILENAME>
no airtune logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

airtune.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# airtune logfile airtune.log
```

airtune logfile-limit

Данная команда устанавливает размер файла лога агента централизованного радиопланирования на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
airtune logfile-limit <LIMIT>
no airtune logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# airtune logfile-limit 2000
```

airtune loglevel

Данная команда устанавливает уровень логирования агента централизованного радиопланирования на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
airtune loglevel { error | warn | info | debug }
no airtune loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# airtune loglevel error
```

no airtune all

Данная команда устанавливает значения по умолчанию для всех параметров логирования агента централизованного радиопланирования на точке доступа.

Синтаксис

```
no airtune all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no airtune all
```

bandsteer enable

Данная команда включает логирование подсистемы band steer, определяющей для клиента Wi-FI приоритетным диапазон 5 ГГц при подключении к сети на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] bandsteer enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# bandsteer enable
```

bandsteer logfile

Данная команда задает название файла лога подсистемы band steer на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
bandsteer logfile <FILENAME>
no bandsteer logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

bandsteerd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# bandsteer logfile bandsteerd.log
```

bandsteer logfile-limit

Данная команда устанавливает размер файла лога подсистемы band steer на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
bandsteer logfile-limit <LIMIT>
no bandsteer logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# bandsteer logfile-limit 2000
```

bandsteer loglevel

Данная команда устанавливает уровень логирования подсистемы band steer на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
bandsteer loglevel { error | warn | debug }
no bandsteer loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# bandsteer loglevel error
```

bandsteer sta-mac

Данная команда задает MAC-адрес клиентской станции Wi-Fi, для которой будет записываться лог подсистемы band steer на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
bandsteer sta-mac <MAC-ADDRESS>
no bandsteer sta-mac
```

Параметры

<MAC-ADDRESS> – MAC-адрес клиентской станции Wi-Fi в формате HH:HH:HH:HH:HH:HH.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# bandsteer sta-mac 00:00:00:00:00:00
```

no bandsteer all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы band steer на точке доступа.

Синтаксис

```
no bandsteer all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no bandsteer all
```

captive-portal enable

Данная команда включает логирование подсистемы портальной авторизации на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] captive-portal enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal enable
```

captive-portal logfile

Данная команда задает название файла лога подсистемы портальной авторизации на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal logfile <FILENAME>
no captive-portal logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

cportald.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal logfile cportald.log
```

captive-portal logfile-limit

Данная команда устанавливает размер файла лога подсистемы портальной авторизации на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal logfile-limit <LIMIT>
no captive-portal logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal logfile-limit 2000
```

captive-portal loglevel

Данная команда устанавливает уровень логирования подсистемы портальной авторизации на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal loglevel { error | warn | debug }
no captive-portal loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal loglevel error
```

no captive-portal all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы портальной авторизации на точке доступа.

Синтаксис

```
no captive-portal all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no captive-portal all
```

captive-portal apbd enable

Данная команда включает логирование подсистемы роуминга для портальной авторизации на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] captive-portal apbd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal apbd enable
```

captive-portal apbd logfile

Данная команда задает название файла лога подсистемы роуминга для портальной авторизации на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal apbd logfile <FILENAME>
no captive-portal apbd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

apbd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal apbd logfile apbd.log
```

captive-portal apbd logfile-limit

Данная команда устанавливает размер файла лога подсистемы роуминга для портальной авторизации на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal apbd logfile-limit <LIMIT>
no captive-portal apbd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal apbd logfile-limit 2000
```

captive-portal apbd loglevel

Данная команда устанавливает уровень логирования подсистемы роуминга для портальной авторизации на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal apbd loglevel { error | warn | info | debug }
no captive-portal apbd loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal apbd loglevel error
```

no captive-portal apbd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы роуминга для портальной авторизации на точке доступа.

Синтаксис

```
no captive-portal apbd all
```

no Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no captive-portal apbd all
```

captive-portal redirector-debug

Данная команда включает логирование модуля перенаправления запросов HTTP на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] captive-portal redirector-debug
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal redirector-debug
```

captive-portal tinyproxy enable

Данная команда включает логирование вспомогательного HTTP proxy-сервера на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] captive-portal tinyproxy enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal tinyproxy enable
```

captive-portal tinyproxy logfile

Данная команда задает название файла лога вспомогательного HTTP proxy-сервера на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal tinyproxy logfile <FILENAME>
no captive-portal tinyproxy logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

tinyproxy.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal tinyproxy logfile tinyproxy.log
```

captive-portal tinyproxy logfile-limit

Данная команда устанавливает размер файла лога вспомогательного HTTP proxy-сервера на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
captive-portal tinyproxy logfile-limit <LIMIT>
no captive-portal tinyproxy logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# captive-portal tinyproxy logfile-limit 2000
```

no captive-portal tinyproxy all

Данная команда устанавливает значения по умолчанию для всех параметров логирования вспомогательного HTTP proxy-сервера на точке доступа.

Синтаксис

```
no captive-portal tinyproxy all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no captive-portal tinyproxy all
```

configd enable

Данная команда включает логирование менеджера конфигурации на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] configd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# configd enable
```

configd logfile

Данная команда задает название файла лога менеджера конфигурации на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
configd logfile <FILENAME>
no configd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

configd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# configd logfile configd.log
```

configd logfile-limit

Данная команда устанавливает размер файла лога менеджера конфигурации на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
configd logfile-limit <LIMIT>
no configd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# configd logfile-limit 2000
```

no configd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования менеджера конфигурации на точке доступа.

Синтаксис

```
no configd all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no configd all
```

dmesg enable

Данная команда включает запись лога ядра в файл на точке доступа.

Использование отрицательной формы команды (no) отключает запись лога в файл.

Синтаксис

```
[no] dmesg enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# dmesg enable
```

dmesg logfile

Данная команда задает название файла лога ядра на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dmesg logfile <FILENAME>
no dmesg logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

dmesg.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# dmesg logfile dmesg.log
```

dmesg logfile-limit

Данная команда устанавливает размер файла лога ядра на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dmesg logfile-limit <LIMIT>
no dmesg logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# dmesg logfile-limit 2000
```

no dmesg all

Данная команда устанавливает значения по умолчанию для всех параметров записи лога ядра в файл на точке доступа.

Синтаксис

```
no dmesg all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no dmesg all
```

ftd enable

Данная команда включает логирование подсистемы роуминга 802.11r на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] ftd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# ftd enable
```

ftd logfile

Данная команда задает название файла лога подсистемы роуминга 802.11r на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ftd logfile <FILENAME>
no ftd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

ftd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# ftd logfile ftd.log
```

ftd logfile-limit

Данная команда устанавливает размер файла лога подсистемы роуминга 802.11r на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ftd logfile-limit <LIMIT>
no ftd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# ftd logfile-limit 2000
```

no ftd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы роуминга 802.11r на точке доступа.

Синтаксис

```
no ftd all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no ftd all
```

hostapd enable

Данная команда включает логирование подсистемы управления радиоинтерфейсами на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] hostapd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# hostapd enable
```

hostapd logfile

Данная команда задает название файла лога подсистемы управления радиоинтерфейсами на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
hostapd logfile <FILENAME>
no hostapd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

hostapd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# hostapd logfile hostapd.log
```

hostapd logfile-limit

Данная команда устанавливает размер файла лога подсистемы управления радиоинтерфейсами на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
hostapd logfile-limit <LIMIT>
no hostapd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# hostapd logfile-limit 2000
```

hostapd loglevel

Данная команда устанавливает уровень логирования для подсистемы управления радиоинтерфейсами на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
hostapd loglevel { error | warn | info | debug | msgdump | excessive }
no hostapd loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug;

msgdump – лог будет записываться с уровнем msgdump;

excessive – лог будет записываться с уровнем excessive;

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# hostapd loglevel error
```

no hostapd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы управления радиоинтерфейсами на точке доступа.

Синтаксис

```
no hostapd all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no hostapd all
```

monitord enable

Данная команда включает логирование подсистемы мониторинга на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] monitord enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# monitord enable
```

monitord logfile

Данная команда задает название файла лога подсистемы мониторинга на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
monitord logfile <FILENAME>
no monitord logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

monitord.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# monitord logfile monitord.log
```

monitord logfile-limit

Данная команда устанавливает размер файла лога подсистемы мониторинга на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
monitord logfile-limit <LIMIT>
no monitord logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# monitord logfile-limit 2000
```

monitord loglevel

Данная команда устанавливает уровень логирования для подсистемы мониторинга на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
monitord loglevel { error | warn | info | debug }
no monitord loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# monitord loglevel error
```

no monitord all

Данная команда устанавливает значения по умолчанию для всех параметров логирования подсистемы мониторинга на точке доступа.

Синтаксис

```
no monitord all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no monitord all
```

netconf enable

Данная команда включает логирование агента NETCONF на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] netconf enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# netconf enable
```

netconf logfile

Данная команда задает название файла лога агента NETCONF на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netconf logfile <FILENAME>
no netconf logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

netconf.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# netconf logfile netconf.log
```

netconf logfile-limit

Данная команда устанавливает размер файла лога агента NETCONF на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netconf logfile-limit <LIMIT>
no netconf logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# netconf logfile-limit 2000
```

no netconf all

Данная команда устанавливает значения по умолчанию для всех параметров логирования агента NETCONF на точке доступа.

Синтаксис

```
no netconf all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no netconf all
```

networkd enable

Данная команда включает логирование системного менеджера на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] networkd enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# networkd enable
```

networkd logfile

Данная команда задает название файла лога системного менеджера на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
networkd logfile <FILENAME>
no networkd logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

networkd.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# networkd logfile networkd.log
```

networkd logfile-limit

Данная команда устанавливает размер файла лога системного менеджера на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
networkd logfile-limit <LIMIT>
no networkd logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# networkd logfile-limit 2000
```

networkd loglevel

Данная команда устанавливает уровень логирования системного менеджера на точке доступа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
networkd loglevel { error | warn | info | debug }
no networkd loglevel
```

Параметры

error – лог будет записываться с уровнем error;

warn – лог будет записываться с уровнем warning;

info – лог будет записываться с уровнем info;

debug – лог будет записываться с уровнем debug.

Значение по умолчанию

debug

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# networkd loglevel error
```

no networkd all

Данная команда устанавливает значения по умолчанию для всех параметров логирования системного менеджера на точке доступа.

Синтаксис

```
no networkd all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no networkd all
```

snmp enable

Данная команда включает логирование агента SNMP на точке доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] snmp enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# snmp enable
```

snmp logfile

Данная команда задает название файла лога агента SNMP на точке доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
snmp logfile <FILENAME>
no snmp logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

snmp.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# snmp logfile snmp.log
```

snmp logfile-limit

Данная команда устанавливает размер файла лога агента SNMP на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
snmp logfile-limit <LIMIT>
no snmp logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# snmp logfile-limit 2000
```

no snmp all

Данная команда устанавливает значения по умолчанию для всех параметров логирования агента SNMP на точке доступа.

Синтаксис

```
no snmp all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no snmp all
```

wlc-activator enable

Данная команда включает логирование на точке доступа для сервиса инициализации точек доступа .

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] wlc-activator enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator enable
```

wlc-activator logfile

Данная команда задает название файла лога сервиса инициализации точек доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wlc-activator logfile <FILENAME>
no wlc-activator logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

service-activator-wlc.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator logfile service-activator-wlc.log
```

wlc-activator logfile-limit

Данная команда устанавливает размер файла лога сервиса инициализации точек доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wlc-activator logfile-limit <LIMIT>
no wlc-activator logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator logfile-limit 2000
```

no wlc-activator all

Данная команда устанавливает значения по умолчанию для всех параметров логирования сервиса и вспомогательного сервера HTTPS для инициализации точек доступа.

Синтаксис

```
no wlc-activator all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no wlc-activator all
```

wlc-activator server enable

Данная команда включает логирование на точке доступа вспомогательного сервера HTTPS для инициализации точек доступа.

Использование отрицательной формы команды (no) отключает логирование.

Синтаксис

```
[no] wlc-activator server enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator server enable
```

wlc-activator server logfile

Данная команда задает название файла лога вспомогательного сервера HTTPS для инициализации точек доступа. Файл будет располагаться в директории /var/log/.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wlc-activator server logfile <FILENAME>
no wlc-activator server logfile
```

Параметры

<FILENAME> – название файла лога в директории /var/log/ на точке доступа.

Значение по умолчанию

service-activator-server-wlc.log

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator server logfile service-activator-server-wlc.log
```

wlc-activator server logfile-limit

Данная команда устанавливает размер файла лога вспомогательного сервера HTTPS для инициализации точек доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wlc-activator server logfile-limit <LIMIT>
no wlc-activator server logfile-limit
```

Параметры

<LIMIT> – максимальный размер файла лога на точке доступа, принимает значение в диапазоне [1..30000] КБ.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# wlc-activator server logfile-limit 2000
```

no wlc-activator server all

Данная команда устанавливает значения по умолчанию для всех параметров логирования вспомогательного сервера HTTPS для инициализации точек доступа.

Синтаксис

```
no wlc-activator server all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WLC-AP-PROFILE-TRACE

Пример

```
wlc(config-wlc-ap-profile-trace)# no wlc-activator server all
```

8 Настройка DNS

- domain ip host
- domain lookup enable
- domain name
- domain name-server

domain ip host

Данная команда определяет статическую DNS-запись.

Использование отрицательной формы команды (no) удаляет запись.

Синтаксис

```
[no] domain ip host <NAME> <IP>
```

Параметры

<NAME> – имя хоста, задаётся строкой до 255 символов;

<IP> – IP-адрес хоста, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..253].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# domain ip host eltex.loc 172.16.0.3
```

domain lookup enable

Данная команда включает разрешение DNS-имен.

Использование отрицательной формы команды (no) выключает разрешение DNS-имен.

Синтаксис

```
[no] domain lookup enable [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет включено разрешение DNS-имен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# domain lookup enable
```

domain name

Команда позволяет назначить имя домена для контроллера.

Использование отрицательной формы команды (no) удаляет имя домена для контроллера.

Синтаксис

```
domain name <NAME>
no domain name
```

Параметры

<NAME> – имя домена контроллера, задаётся строкой от 1 до 31 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# domain name eltex-co.ru
```

domain name-server

Данная команда определяет IP-адрес DNS-сервера, используемого для разрешения DNS-имен.

Использование отрицательной формы команды (no) удаляет адрес DNS-сервера.

Синтаксис

```
[no] domain name-server <IP> [vrf <VRF>]
```

Параметры

<IP> – IP-адрес используемого DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которой будет происходить взаимодействие с DNS-сервером.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# domain name-server 172.16.0.1
```

9 Настройка mDNS-reflector

- clear ip mdns-reflector
- ip mdns-reflector
- ip mdns-reflector services
- show ip mdns-reflector

clear ip mdns-reflector

Данная команда обновляет данные в кэше mDNS-reflector.

Синтаксис

```
clear ip mdns-reflector
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# clear ip mdns-reflector
```

ip mdns-reflector

Данная команда добавляет интерфейс в конфигурацию сервиса mDNS-reflector. Для запуска сервиса нужно включить в конфигурацию минимум два интерфейса.

Использование отрицательной команды (no) удаляет интерфейс из конфигурации сервиса mDNS-reflector.

Синтаксис

```
ip mdns-reflector
no ip mdns-reflector
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip mdns-reflector
```

ip mdns-reflector services

Данная команда активирует фильтрацию сервисов mDNS. Сервисы, указанные в object-group <NAME>, будут разрешены, все остальные будут запрещены. Если список фильтрации пуст, то будут доступны все сервисы.

Использование отрицательной команды (no) отключает фильтрацию сервисов mDNS.

Синтаксис

```
ip mdns-reflector services <OBJ-GROUP-URL-NAME>
no ip mdns-reflector services
```

Параметры

<OBJ-GROUP-URL-NAME> – имя профиля url-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30 (config)# object-group url test
wlc-30 (config-object-group-url)# url_ssh._tcp.local
wlc-30 (config-object-group-url)# exit
wlc-30 (config)#
wlc-30 (config)# ip mdns-reflector services test
```

show ip mdns-reflector

Данная команда выводит список сервисов из кэша mDNS-reflector.

Синтаксис

```
show ip mdns-reflector [ interfaces <IF> | service <NAME> ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<NAME> – имя профиля url-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip mdns-reflector
Interface IP address Hostname Service Port
----------- --------------- -------------------- ------------------ ------
br21 172.21.0.10 WEP-12ac.local _brcm-sb._tcp 80
br21 172.21.0.10 WEP-12ac.local _telnet._tcp 23
br21 172.21.0.10 WEP-12ac.local _ssh._tcp 22
br21 172.21.0.10 WEP-12ac.local _http._tcp 80
br21 172.21.0.10 WEP-12ac.local _https._tcp 443
gi1/0/2.20 172.20.0.11 Book-tester-7.local _ssh._tcp 22
gi1/0/2.20 172.20.0.11 Book-tester-7.local _sftp-ssh._tcp 22
gi1/0/2.20 172.20.0.11 Book-tester-7.local _eppc._tcp 3031
gi1/0/2.20 172.20.0.11 Book-tester-7.local _rfb._tcp 5900
gi1/0/2.20 172.20.0.11 Book-tester-7.local _smb._tcp 445
gi1/0/2.20 172.20.0.11 Book-tester-7.local _airplay._tcp 7000
gi1/0/2.20 172.20.0.11 Book-tester-7.local _raop._tcp 5000
gi1/0/2.20 172.20.0.11 Book-tester-7.local _teamviewer._tcp 2020
```

```
wlc-30# show ip mdns-reflector service ssh
Interface IP address Hostname Service Port
---------- --------------- -------------------- ------------------ ------
br21 172.21.0.10 WEP-12ac.local _ssh._tcp 22
gi1/0/2.20 172.20.0.11 Book-tester-7.local _ssh._tcp 22
gi1/0/2.20 172.20.0.11 Book-tester-7.local _sftp-ssh._tcp 22
```

10 Настройка общесистемных параметров

- alias
- hostname
- show cpu network-load
- show cpu history
- show cpu processes
- show cpu utilization
- show system
- show system id
- system config-confirm timeout
- system utilization softgre disable

alias

Данная команда дает возможность настроить укороченные/специфичные команды в различных командных режимах.

Использование отрицательной формы команды (no) удаляет запись.

⚠ Для активации настроенных alias необходимо переподключиться к CLI контроллера.

Синтаксис

```
alias {<ALIAS_NAME>} {<MODE>} {<COMMAND>}
no alias <ALIAS_NAME>
```

Параметры

<ALIAS_NAME> – имя новой команды.

<MODE> – названия командного режима в котором присутствует новая команда:

- change-expired-password;
- config;
- config-aaa-das-profile;
- config-aaa-radius-profile;
- config-accsess-profile;
- config-acl;
- config-acl-rule;
- config-archive;
- config-bgp;
- config-bgp-af;
- config-bgp-group;
- config-bgp-neighbor;
- config-bridge;
- config-cellular-modem;
- config-cellular-profile;
- config-class-map;
- config-class-policy-map;
- config-das-server;
- config-dhcp-server;
- config-dhcp-vendor-id;
- config-dnat;
- config-dnat-pool;
- config-dnat-rule;
- config-dnat-ruleset;

- config-e1;
- config-gre;
- config-if-gi;
- config-if-te;
- config-ike-gw;
- config-ike-policy;
- config-ike-proposal;
- config-ip4ip4;
- config-ipsec-policy;
- config-ipsec-proposal;
- config-ipsec-vpn;
- config-ipv6-bgp-af;
- config-ipv6-bgp-group;
- config-ipv6-bgp-neighbor;
- config-ipv6-dhcp-server;
- config-ipv6-ospf;
- config-ipv6-ospf-area;
- config-ipv6-ospf-vlink;
- config-ipv6-pl;
- config-ipv6-wan-rule;
- config-ipv6-wan-target;
- config-ipv6-wan-target-list;
- config-keychain;
- config-keychain-key;
- config-l2tp-server;
- config-l2tpv3;
- config-ldap-server;
- config-line-console;
- config-line-ssh;
- config-line-telnet;
- config-loopback;
- config-lt;
- config-mst;
- config-multilink;
- config-netflow-host;
- config-network-policy;
- config-ntp;
- config-object-group-application;
- config-object-group-mac;
- config-object-group-network;
- config-object-group-service;
- config-object-group-url;
- config-openvpn;
- config-openvpn-server;
- config-ospf;
- config-ospf-area;
- config-ospf-vlink;
- config-pl;
- config-policy-map;
- config-pool;
- config-port-channel;
- config-ppp-user;
- config-pppoe;
- config-pptp;
- config-pptp-server;
- config-profile;
- config-qinq-if;

- config-radius-server;
- config-rip;
- config-route-map;
- config-route-map-rule;
- config-service-port;
- config-sflow-host;
- config-snat;
- config-snat-pool;
- config-snat-rule;
- config-snat-ruleset;
- config-snmp-host;
- config-snmp-user;
- config-softgre;
- config-subif;
- config-subscriber-control;
- config-subscriber-default-service;
- config-subtunnel;
- config-tacacs-server;
- config-tracking;
- config-user;
- config-vlan;
- config-vrf;
- config-vti;
- config-wan-rule;
- config-wan-target;
- config-wan-target-list;
- config-wireless;
- config-zone;
- config-zone-pair;
- config-zone-pair-rule;
- debug;
- root.

<COMMAND> – строка размером 96 символов. Команда CLI. Вводится полностью, без сокращений. Для ввода команды из нескольких слов обрамляется двойными кавычками.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# alias qwe root "show version"
```

hostname

Команда позволяет назначить сетевое имя для контроллера.

Использование отрицательной формы команды (no) устанавливает имя контроллера по умолчанию.

Синтаксис

```
hostname <NAME>
no hostname
```

Параметры

<NAME> – сетевое имя контроллера, задаётся строкой до 63 символов.

Необходимый уровень привилегий

10

Значение по умолчанию

wlc-30

Командный режим

CONFIG

Пример:

```
wlc-30(config)# hostname router-1.eltex-co.ru
```

show cpu network-load

Данной командой осуществляется просмотр нагрузки, производимой сетевым трафиком.

Синтаксис

```
show cpu network-load
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show cpu network-load
CPU ID    CPU load    Heaviest session          Session
                                                weight
-------   ---------   ----------------------   -------
0         0           --                       0
1         49413       80.88.157.57 ->          9826
                      172.129.22.57
2         46812       80.88.157.75 ->          9895
                      172.129.22.75
3         49229       172.129.22.41 ->         9851
                      80.88.157.41
4         0           --                       0
5         53019       80.88.157.77 ->          9989
                      172.129.22.77
6         39699       80.88.157.79 ->          9863
                      172.129.22.79
7         49726       172.129.22.45 ->         9804
                      80.88.157.45
8         39789       172.129.22.61 ->         9779
                      80.88.157.61
9         36876       80.88.157.59 ->          9775
                      172.129.22.59
10        53041       172.129.22.5 ->          9679
                      80.88.157.5
11        49010       172.129.22.47 ->         9896
                      80.88.157.47
12        53082       172.129.22.13 ->         9650
                      80.88.157.13
13        63027       80.88.157.69 ->          9617
                      172.129.22.69
172       52722       80.88.157.73 ->          10001
                      172.129.22.73
15        55165       80.88.157.71 ->          9924
```

show cpu history

Данной командой осуществляется просмотр истории использования ресурсов CPU.

Синтаксис

```
show cpu history [ average | max ] [cpu {<CPU>}] [timer {<TIMER>}]
```

Параметры

average | max – указывает, историю какой статистики необходимо выводить, усредненную или максимальную за интервал. Без указания данного ключа выводится история усредненной статистики (average);

<CPU> – возможно указать номер конкретного CPU по которому будет выводиться история статистики использования ресурсов CPU. Без указания номера CPU будет выводиться информация по всем CPU использующимися системой.

<TIMER> в качестве параметров для данного ключа могут выступать:

- hours – отображает историю за последние 72 часа;
- minutes – отображает историю за последние 60 минут;
- seconds – отображает историю за последние 60 секунд;

- При отсутствии ключа timer, выводятся 3 таблицы истории статистики использования CPU.

Необходимый уровень привилегий

5

Командный режим

ROOT

Пример:

```
wlc-30# show cpu history max cpu 0
CPU0
Last 60 seconds:
utilization, %
100
 90    #
 80    #
 70    #
 60    #
 50    ##
 40    ##
 30   # ##
 20   # ##
 10 ############
  ....|....|..
 0 25 50
  time, 5 sec.
Last 60 minutes:
utilization, %
100             #
 90             #
 80             #
 70 #            #
 60 ##           #
 50 ##           #
 40 ##           #
 30 ## #    #    #    #    #    #
 20 ## #    #    #    #    #    #
 10 ############################################################
  ....|....|....|....|....|....|....|....|....|....|....|....|
 0  5 10 15 20 25 30 35 40 45 50 55 60
                           time, min.
```

```
Last 72 hours:
utilization, %
100 #       # #           ##
 90 #       # ###           ##
 80 #       # ###           ##
 70 #       #####           ##
 60 #       #####           ##
 50 #       #####           ##
 40 #       #####           ##
 30 ##########################################
 20 ##########################################
 10 ##########################################
  ....|....|....|....|....|....|....|....|....|....|....|....|....|....|..
 0  5 10 15 20 25 30 35 40 45 50 55 60 65 70
                                time, hours
```

show cpu processes

Данной командой осуществляется просмотр использования ресурсов CPU-процессами.

Синтаксис

```
show cpu processes [ active | name <PROCESS_NAME> ]
```

Параметры

active – список активных процессов;

name – имя конкретного процесса.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# show cpu processes
PID  Name                        CPU 5s    CPU 1m    CPU 5m    Memory    Runtime
---  --------------------------  -------   -------   -------   -------   --------
2013    CLI                       0.00%     0.00%     0.00%     0.40%       --
525    Cp-mgr                     0.00%     0.00%     0.00%     0.08%       --
535    Service-mgr                0.00%     0.00%     0.00%     0.08%       --
532    Env-mgr                    0.00%     0.03%     0.05%     0.11%   14 seconds
530    Alarm-mgr                  0.00%     0.00%     0.00%     0.08%       --
529    Lb                         0.00%     0.00%     0.00%     0.09%       --
528    Session-mgr                0.00%     0.00%     0.00%     0.11%       --
521    Ipc-hub                    0.20%     0.03%     0.04%     0.09%   10 seconds
533    E1                         0.00%     0.00%     0.00%     0.11%       --
522    Syslog-mgr                 0.00%     0.00%     0.00%     0.09%       --
524    If-mgr                     0.40%     0.35%     0.34%     0.17%  1 minute and 31 second
534    Systemdb                   0.00%     0.02%     0.02%     0.14%    3 seconds
526    Oi-mgr                     0.40%     0.40%     0.43%     1.14%  1 minute and 57 second
527    Cfgsync-mgr                0.00%     0.00%     0.00%     10.07%    1 second
531    Switch                     0.00%     0.10%     0.11%     1.08%    34 seconds
1877   IPv6 Routing               0.00%     0.02%     0.01%     0.10%     1 second
1885   Routing                    0.00%     0.00%     0.00%     0.10%     1 second
```

show cpu utilization

Данной командой осуществляется просмотр использования ресурсов CPU.

Синтаксис

```
show cpu utilization
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show cpu utilization
CPU   Last      Last      Last
      5 sec     1 min     5 min
---   -------   -------   -------
0     1.98%     6.75%     20.02%
1     67.50%    15.62%    6.88%
2     65.43%    15.53%    6.94%
3     69.29%    16.08%    7.08%
4     89.90%    20.79%    9.14%
5     74.95%    17.14%    7.49%
6     87.61%    20.18%    8.85%
7     87.41%    20.17%    8.85%
8     81.84%    19.03%    8.40%
9     84.82%    19.79%    8.73%
10    84.53%    19.78%    8.75%
11    83.02%    19.40%    8.58%
12    83.73%    19.55%    8.63%
13    76.56%    16.99%    7.25%
14    70.47%    16.00%    6.95%
15    68.39%    15.07%    6.40%
```

show system

Данной командой осуществляется просмотр параметров окружения устройства.

Синтаксис

```
show system
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show system
System type:           Eltex WLC-30 Wi-Fi Controller
System name:           WLC-30
Software version:      1.0.7 build 118[53264b8] (date 22/12/2015 time 10:23:23)
Hardware version:      1v3
System uptime:         4 minutes and 5 seconds
System MAC address:    A8:F9:4B:AA:03:A0
System serial number:  NP01000050
Main power supply installed:     Present
Main power supply status:        Ok
Reserve power supply installed:  Absent
Fan Level:                        46%
   Fan Table
   ~~~~~~~~~
         Fan 1   Fan 2   Fan 3   Fan 4
------   -----   -----   -----   -----
Status   Ok      Ok      Ok      Ok
   Temperature Table
   ~~~~~~~~~~~~~~~~~
                CPU         Sensor 1   Sensor 2   Sensor 3
--------------   --------   --------   --------   --------
Temperature, C   63         39         37         49
   Memory Table
   ~~~~~~~~~~~~
         Total, MB          Used, MB           Free, MB
-----    ----------------   ----------------   ----------------
RAM      3798.25            1643.50 (44%)      2154.75 (56%)
FLASH    20.00              1.06 (6%)          18.94 (94%)
```

show system id

Данной командой осуществляется просмотр серийного номера устройства.

Синтаксис

```
show system id
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show system id
Serial number:
  NP01000023
```

system config-confirm timeout

Данная команда определяет интервал времени ожидания для подтверждения текущей конфигурации. Если конфигурация не будет подтверждена, то после истечения времени ожидания произойдет откат на предыдущую примененную конфигурацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`system config-confirm timeout <TIME>`

`no system config-confirm timeout`

Параметры

<TIME> – интервал времени ожидания подтверждения резервирования конфигурации, принимает значение в секундах [120..86400].

Значение по умолчанию

600

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# system config-confirm timeout 1200
```

system utilization softgre disable

Данная команда используется для отключения подсчета загруженности SoftGRE-туннелей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`[no] system utilization softgre disable`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Подсчет включен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# system utilization softgre disable
```

11 Управление системными часами

- clock timezone
- key
- maxpoll
- minpoll
- ntp access-addresses
- ntp authentication enable
- ntp authentication key-chain
- ntp authentication trusted-key
- ntp broadcast-client enable
- ntp dscp
- ntp enable
- ntp ipv6 source address
- ntp object-group query-only
- ntp object-group serve-only
- ntp peer
- ntp server
- ntp source address
- prefer
- set date
- show date
- show ntp configuration
- show ntp peers
- version

clock timezone

Данной командой устанавливается часовой пояс.

Использование отрицательной формы команды (no) устанавливает часовой пояс по умолчанию.

Синтаксис

```
clock timezone <OFFSET>
no clock timezone
```

Параметры

<OFFSET> – обозначение зоны, содержащее сдвиг в часах относительно Greenwich Mean Time, принимает значения [gmt -12 .. gmt +12].

Значение по умолчанию

gmt 0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# clock timezone gmt +7
```

key

Данной командой определяется ключ из списка доверенных ключей.

Использование отрицательной формы команды (no) удаляет привязку к указанному ключу.

Синтаксис

`key <ID>`

`no key`

Параметры

<ID> – идентификатор ключа, задается в диапазоне [1..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-NTP

Пример:

```
wlc-30(config-ntp)# key 245
```

maxpoll

Данная команда устанавливает максимальное значение интервала времени между отправкой сообщений NTP-серверу.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`maxpoll <INTERVAL>`

`no maxpoll`

Параметры

<INTERVAL> – максимальное значение интервала опроса. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах, вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [10..17].

Значение по умолчанию

10 (2^{10} = 1024 секунды или 17 минут 4 секунды)

Необходимый уровень привилегий

10

Командный режим

CONFIG-NTP

Пример:

```
wlc-30(ntp-remote)# maxpoll 11
```

minpoll

Данная команда устанавливает минимальное значение интервала времени между отправкой сообщений NTP-серверу.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`minpoll <INTERVAL>`

`no minpoll`

Параметры

<INTERVAL> – минимальное значение интервала опроса в секундах, вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [4..6].

Значение по умолчанию

6 (2^{6} = 64 секунды или 1 минута 4 секунды)

Необходимый уровень привилегий

10

Командный режим

CONFIG-NTP

Пример:

```
wlc-30(ntp-remote)# minpoll 4
```

ntp access-addresses

Данной командой определяется список доверенных IP-адресов, с которыми может происходить обмен ntp-пакетами.

Использование отрицательной формы команды (no) удаляет указанный список.

Синтаксис

```
ntp access-addresses <NAME>
no ntp access-addresses
```

Параметры

<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Фильтрация отключена.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp access-addresses 192.168.16.33
```

ntp authentication enable

Данная команда включает аутентификацию для NTP-протокола.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ntp authentication enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp authentication enable
```

ntp authentication key-chain

Данная команда определяет набор паролей для аутентификации через алгоритм хеширования md5 с сервером, пиром.

Использование отрицательной формы команды (no) удаляет привязку к набору паролей.

Синтаксис

`ntp authentication key-chain <KEYCHAIN>`

`no ntp authentication key-chain`

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp authentication key-chain lock
```

ntp authentication trusted-key

Данной командой определяется список доверенных ключей из набора ключей.

Использование отрицательной формы команды (no) удаляет указанный ключ.

Синтаксис

`[no] ntp authentication trusted-key <ID>`

Параметры

<ID> – идентификатор ключа, задается в диапазоне [1..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp authentication trusted-key 25
```

ntp broadcast-client enable

Данной командой включается режим приёма широковещательных сообщений NTP-серверов для глобальной конфигурации и всех существующих VRF. контроллер работает в качестве NTP-клиента. Если в конфигурации устройства заданы NTP-пиры и серверы, то в широковещательном режиме они игнорируются.

Использование отрицательной формы команды (no) выключает широковещательный режим.

Синтаксис

```
[no] ntp broadcast-client enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp broadcast-client enable
```

ntp dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов NTP-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ntp dscp <DSCP>
no ntp dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

46

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp dscp 40
```

ntp enable

Данной командой включается синхронизация системных часов с удаленными серверами по протоколу NTP для глобальной конфигурации и всех созданных VRF.

Использование отрицательной формы команды (no) выключает синхронизацию по протоколу NTP.

Синтаксис

```
[no] ntp enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp enable
```

ntp ipv6 source address

Данная команда используется для указания source-IPv6-адреса для NTP-пакетов для всех peer.

Использование отрицательной формы команды (no) устанавливает source-IPv6-адрес для NTP-пакетов по умолчанию.

Синтаксис

```
ntp ipv6 source address <IPV6-ADDR>
no ntp ipv6 source address
```

Параметры

<IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Значение по умолчанию

IPv6-адрес интерфейса, с которого отправляется NTP-пакет.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp ipv6 source address fc00::1
```

ntp object-group query-only

Данная команда включает режим query-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов. Разрешается обмен только control messages.

Использование отрицательной формы команды (no) отключает данные ограничения.

Синтаксис

```
ntp object-group query-only <NAME>
no ntp object-group query-only
```

Параметры

<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Работа с NTP-пирами ничем не ограничивается.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp object-group query-only OG-NTP-QO
```

ntp object-group serve-only

Данная команда включает режим serve-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов. Разрешено отвечать только на NTP-запросы; синхронизация от других хостов и обмен control messages запрещены.

Использование отрицательной формы команды (no) отключает данные ограничения.

Синтаксис

```
ntp object-group serve-only <NAME>
no ntp object-group serve-only
```

Параметры

<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Работа с NTP-пирами ничем не ограничивается

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp object-group serve-only OG-NTP-SO
```

ntp peer

Данная команда используется для установления партнерских отношений между NTP-серверами и перехода в командный режим CONFIG-NTP.

NTP-сервер на контроллере работает в режиме двусторонней активности с удаленным NTP-сервером, указанным в команде. В случае потери связи одного из партнеров с вышестоящим NTP-сервером, он сможет синхронизировать время по серверу-партнеру.

Использование отрицательной формы команды (no) удаляет заданного NTP-партнера.

Синтаксис

```
[no] ntp peer { <ADDR> | <IPV6-ADDR> } [ vrf <VRF> ]
```

Параметры

<ADDR> – IP-адрес партнера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес партнера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать NTP-партнер.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp peer 10.100.100.1
wlc-30(ntp-remote)#
```

ntp server

Данная команда используется для создания NTP-сервера и перехода в командный режим CONFIG-NTP.

Контроллер работает с указанным NTP-сервером в режиме односторонней активности. В данном режиме локальные часы контроллера могут синхронизироваться с удаленным NTP-сервером.

Использование отрицательной формы команды (no) удаляет заданный NTP-сервер.

Синтаксис

```
[no] ntp server { <ADDR> | <IPV6-ADDR> } [ vrf <VRF> ]
```

Параметры

<ADDR> – IP-адрес сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать NTP-сервер.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp server 10.100.100.2
wlc-30(ntp-remote)#
```

ntp source address

Данная команда используется для указания source-IP-адреса для NTP-пакетов для всех peer.

Использование отрицательной формы команды (no) устанавливает source-IP-адрес для NTP-пакетов по умолчанию.

Синтаксис

```
ntp source address <ADDR>
no ntp source address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

IP-адрес интерфейса, с которого отправляется NTP-пакет.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ntp source address 10.100.100.2
```

prefer

Команда отмечает данный NTP-сервер как предпочтительный. При прочих равных условиях данный NTP-сервер будет выбран для синхронизации среди всех рабочих NTP-серверов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] prefer
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-NTP

Пример:

```
wlc-30(ntp-remote)# prefer
```

set date

Данной командой устанавливается вручную системное время и дата.

Синтаксис

```
set date <TIME> [<DAY> <MONTH> [ <YEAR> ] ]
```

Параметры

<TIME> – устанавливаемое системное время, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

<DAY> – день месяца, принимает значения [1..31];

<MONTH> – месяц, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December];

<YEAR> – год, принимает значения [2001..2037].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# set date 16:35:00 15 May 2014
```

show date

Данная команда позволяет посмотреть текущие системное время и дату.

Синтаксис

`show date`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show date
Thursday 23:48:33 GMT+7 May 15 2014
```

show ntp configuration

Данная команда отображает действующую (RUNNING) конфигурацию протокола NTP.

Синтаксис

`show ntp configuration`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show ntp configuration
 NTP status: Enabled
 NTP mode:   client/server
Address          Type     Prefer   NTP version   Min poll          Max poll
--------------   ------   ------   -----------   ---------------   ---------------
10.100.100.1      peer     yes      NTPv4          6(1m 4s)          11(34m 8s)
10.100.100.2      peer     yes      NTPv4          6(1m 4s)          10(17m 4s)
1.2.3.4           server   no       NTPv4          6(1m 4s)          10(17m 4s)
```

show ntp peers

Данная команда позволяет посмотреть текущее состояние NTP-серверов (пиров). В следующих таблицах приведен перечень отображаемых параметров и их описание.

Таблица 6 – Состояние удаленного сервера (пира)

Параметр	Описание
remote	DNS-имя или IP-адрес сервера (пира). Первый символ в таблице используется для обозначения состояния сервера (пира), состояния описаны в таблице 7.
refid	Идентификатор связи или IP-адрес того, с кем синхронизирован удаленный сервер (пир). Типы идентификаторов связи описаны в таблице 8.
st	Стратум.
t	Отношение контроллера к удаленному серверу (пиру), типы описаны в таблице 9.
when	Период времени с момента, когда сервер (пир) последний раз опрашивался, в секундах (“h” часы,“d” дни).
poll	Частота опроса сервера (пира).
reach	Восьмибитный сдвигаемый влево регистр, содержащий результаты опросов (1 = успешно, 0 = неуспешно), отображается в восьмеричной системе счисления.
delay	Время прохождения пакета до сервера (пира) и обратно, в миллисекундах.

Параметр	Описание
offset	Среднее постоянное смещение времени контроллера относительно сервера (пира).
jitter	Средний разброс отклонения времени (джиттер).

Таблица 7 − Состояние удаленного сервера (пира)

Тип	Описание
пробел	Указывает на то, что: • не было ответов от удаленного сервера (пира); • сервер не используется, так как стратум имеет большое значение; • сервер (пир) использует данный контроллер для синхронизации своих часов.
x	Сервер (пир) не используется для синхронизации времени, отброшен алгоритмом пересечения.
-	Сервер (пир) не используется для синхронизации времени, отброшен кластерным алгоритмом.
#	Рабочий удаленный сервер (пир), но не используется, так как не вошел в число первых шести серверов (пиров), отсортированных по расстоянию синхронизации, является резервным.
+	Рабочий и предпочитаемый удаленный сервер (пир), включен алгоритмом объединения.
*	Сервер (пир), который в настоящее время является первичным источником времени.

Таблица 8 − Типы идентификаторов соединения с удаленным сервером (пиром)

Тип	Описание
.ACST.	Manycast-сервер.
.AUTH.	Ошибка аутентификации.
.AUTO.	Ошибка последовательности автоматического ключа.
.BCST.	Broadcast-сервер.
.CRYPT.	Ошибка протокола автоматического ключа.

Тип	Описание
.DENY.	Сервер отказал в доступе.
.INIT.	Инициализация соединения с сервером.
.MCST.	Multicast-сервер.
.TIME.	Таймаут соединения с сервером.
.STEP.	Ступенчатое изменение времени, смещение меньше предельного порога (1000 миллисекунд), но больше, чем шаг порога (125 миллисекунд).
.RATE.	Превышение частоты опросов.

Таблица 9 – Типы отношений контроллера к удаленному серверу (пиру)

Тип	Описание
u	Unicast или manycast-клиент.
b	Broadcast или unicast-клиент.
s	Двусторонняя связь (пир).
A	Manycast-сервер.
B	Broadcast-сервер.
M	Multicast-сервер.

Синтаксис

```
show ntp peers
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# sh ntp peers
Clock is synchronized, stratum 3, reference is 192.168.1.1
     remote           refid           st t when poll reach  delay   offset  jitter
---------------------- --------------- -- - ---- ---- ----- ------- -------- -------
*192.168.1.1          192.168.1.2      2 u   45  128  377   0.283   0.204   0.049
```

version

Данной командой устанавливается версия NTP-протокола.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`version <VERSION>`

`no version`

Параметры

<VERSION> – версия NTP-протокола, принимает значения [1..4].

Значение по умолчанию

4

Необходимый уровень привилегий

15

Командный режим

CONFIG-NTP

Пример:

```
wlc-30(ntp-remote)# version 3
```

12 Настройка AAA

- aaa accounting commands
- aaa accounting login
- aaa authentication attempts max-fail
- aaa authentication enable
- aaa authentication login
- aaa authentication mode
- aaa das-profile
- aaa disable
- aaa radius-profile
- acct-port
- auth-port
- clear users blocked
- clear user-session
- clients
- das-server
- das-server
- dead-interval
- description
- disable
- enable
- enable authentication
- enable password
- exec-timeout
- ip sftp enable
- key
- ldap-server base-dn
- ldap-server bind authenticate root-dn
- ldap-server bind authenticate root-password
- ldap-server bind timeout
- ldap-server dscp
- ldap-server host
- ldap-server naming-attribute
- ldap-server privilege-level-attribute
- ldap-server search filter user-object-class
- ldap-server search scope
- ldap-server search timeout
- ldap-server ssl certificate
- ldap-server ssl check-peer disable
- ldap-server ssl enable
- line
- login authentication
- password
- port
- priority
- privilege
- privilege
- radius-server dscp
- radius-server host
- radius-server host
- radius-server retransmit
- radius-server timeout
- retransmit
- security passwords default-expired
- security passwords history
- security passwords lifetime

- security passwords lower-case
- security passwords max-length
- security passwords min-length
- security passwords numeric-count
- security passwords special-case
- security passwords symbol-types
- security passwords upper-case
- security snmp-community max-length
- security snmp-community min-length
- show aaa accounting
- show aaa authentication
- show aaa ldap-servers
- show aaa radius-servers
- show aaa tacacs-servers
- show users
- show users accounts
- show users blocked
- source-address
- source-interface
- system configuration-exclusively
- tacacs-server dscp
- tacacs-server host
- tacacs-server timeout
- tech-support login enable
- timeout
- usage
- username

aaa accounting commands

Данной командой конфигурируется список способов учета команд, введённых в CLI.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
aaa accounting commands stop-only <METHOD>
no aaa accounting commands stop-only
```

Параметры

<METHOD> – способы учета:

- tacacs – учет введенных команд по протоколу TACACS.

Значение по умолчанию

Учёт не ведется.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa accounting commands stop-only tacacs
```

aaa accounting login

Данной командой конфигурируется список способов учета сессий пользователей. Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям «start» и «stop» в сообщениях протоколов RADIUS и TACACS.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
aaa accounting login start-stop <METHOD 1> [ <METHOD 2> ]
no aaa accounting login start-stop
```

Параметры

<METHOD> – способы учета:

- tacacs – учет сессий по протоколу TACACS;
- radius – учет сессий по протоколу RADIUS.

Значение по умолчанию

Учет сессий ведется в локальный журнал.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa accounting login start-stop tacacs
```

aaa authentication attempts max-fail

Данной командой устанавливается максимальное количество неудачных попыток аутентификации до блокировки пользователя и время, на которое происходит блокировка.

Использование отрицательной формы команды (no), значения количества попыток и период блокировки устанавливает по умолчанию.

Синтаксис

```
aaa authentication attempts max-fail <COUNT> <TIME>
no aaa authentication attempts max-fail
```

Параметры

<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];

<TIME> – интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535].

Значение по умолчанию

Количество неудачных попыток – 5

Период блокировки – 300

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa authentication attempts max-fail 5 30
```

aaa authentication enable

Данной командой создаются списки способов аутентификации повышения привилегий пользователей. При неудачной попытке аутентификации по одному способу происходит попытка аутентификации по следующему в списке.

В конфигурации по умолчанию существует список с именем «default». Список «default» содержит один способ аутентификации – «enable». Чтобы использовать список для аутентификации повышения привилегий пользователей, необходимо выполнить его привязку командой, описанной в разделе enable authentication.

Использование отрицательной формы команды (no) удаляет список способов аутентификации.

Синтаксис

```
aaa authentication enable <NAME> <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]
no aaa authentication enable <NAME>
```

Параметры

<NAME> – имя списка: строка до 31 символа;

- default – имя списка «default».

<METHOD> – способы аутентификации:

- enable – аутентификация с помощью enable-паролей;
- tacacs – аутентификация по протоколу TACACS;
- radius – аутентификация по протоколу RADIUS;
- ldap – аутентификация по протоколу LDAP.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa authentication enable enable-test tacacs enable
```

aaa authentication login

Данной командой создаются списки способов аутентификации входа пользователей в систему. При неудачной попытке аутентификации по одному способу происходит попытка аутентификации по следующему в списке.

В конфигурации по умолчанию существует список с именем «default», данный список содержит один способ аутентификации – «local». Чтобы использовать список для аутентификации входа пользователей, необходимо выполнить его активацию командой, описанной в разделе login authentication.

Использование отрицательной формы команды (no) удаляет список способов аутентификации.

Синтаксис

```
aaa authentication login { default | <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]
```

```
no aaa authentication login { default | <NAME> }
```

Параметры

<NAME> – имя списка, задаётся строкой до 31 символа.

Способы аутентификации:

- local – аутентификация с помощью локальной базы пользователей;
- tacacs – аутентификация по списку TACACS-серверов;
- radius – аутентификация по списку RADIUS-серверов;
- ldap – аутентификация по списку LDAP-серверов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa authentication login login-test tacacs local
```

aaa authentication mode

Данной командой определяется режим работы со списками методов аутентификации.

Использование отрицательной формы команды (no) удаляет список способов аутентификации.

Синтаксис

```
[no] aaa authentication mode { break | chain }
```

Параметры

break – при аутентификации будут использоваться последующие методы в случае недоступности более приоритетного;

chain – при аутентификации будут использоваться последующие методы в случае получения отказа от более приоритетного.

Значение по умолчанию

chain

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa authentication mode break
```

aaa das-profile

Данная команда используется для добавления профиля серверов динамической авторизации (DAS) и перехода в командный режим DAS SERVER PROFILE.

Использование отрицательной формы команды (no) удаляет заданный профиль серверов динамической авторизации (DAS).

Синтаксис

```
[no] aaa das-profile <NAME>
```

Параметры

<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa das-profile profile1
wlc-30(config-aaa-das-profile)#
```

aaa disable

Данной командой отключает доступ на контроллер через консольный интерфейс.

При использовании отрицательной формы команды (no) доступ на контроллер через консольный интерфейс включается.

Синтаксис

```
[no] aaa disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Доступ на контроллер через консольный интерфейс включен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LINE-CONSOLE

Пример:

```
wlc-30(config-line-console)# aaa disable
```

aaa radius-profile

Данная команда используется для добавления профиля RADIUS-серверов и перехода в командный режим RADIUS SERVER PROFILE.

Использование отрицательной формы команды (no) удаляет заданный профиль RADIUS-серверов.

Синтаксис

```
[no] aaa radius-profile <NAME>
```

Параметры

<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# aaa radius-profile profile1
wlc-30(config-aaa-radius-profile)#
```

acct-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аккаунтинга.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`acct-port <PORT>`

`no acct-port`

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1813

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# acct-port 4444
```

auth-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аутентификации и авторизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
auth-port <PORT>
no auth-port
```

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1812

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# auth-port 4444
```

clear users blocked

Данной командой удаляется информация о неправильных попытках аутентификации различных пользователей.

Синтаксис

```
clear users blocked <NAME>
```

Параметры

<NAME> – имя пользователя, для которого необходимо очистить статистику неправильных попытках аутентификации, задаётся строкой до 31 символа.

Без указания имени пользователя очищается вся таблица неправильных попыток аутентификации.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# clear users blocked
```

clear user-session

Данной командой закрывается рабочая сессия пользователя CLI.

Синтаксис

```
clear user-session [ <USERNAME> | <SESSION> ]
```

Параметры

<NAME> – имя пользователя сессию которого необходимо закрыть, задаётся строкой до 31 символа;

<SESSION> – номер терминальной сессии которую необходимо закрыть, задаётся число в диапазоне [1..10].

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# clear users-session
```

clients

Данной командой определяется список клиентов динамической авторизации (DAC), на запросы которых будет отвечать сервер динамической авторизации (DAS).

Использование отрицательной формы команды (no) удаляет список клиентов динамической авторизации (DAC).

Синтаксис

```
clients object-group <NAME>
```

```
no clients
```

Параметры

<NAME> – имя профиля IP-адресов, содержащий адреса клиентов динамической авторизации, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-DAS-SERVER

Пример:

```
wlc-30(config-das-server)# clients object-group pcrf
```

das-server

Данная команда используется для добавления сервера динамической авторизации (DAS) и перехода в командный режим DAS SERVER. Сервера динамической авторизации (DAS) принимают RADIUS CoA запросы от клиентов динамической авторизации (DAC), например отключение или повторный запрос списка сервисов пользователя.

Использование отрицательной формы команды (no) удаляет заданный сервер динамической авторизации (DAS).

Синтаксис

[no] das-server <NAME>

Параметры

<NAME> – имя сервера динамической авторизации (DAS), задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# das-server main
wlc-30(config-das-server)#
```

das-server

Данная команда используется для добавления сервера динамической авторизации (DAS) в конфигурируемый профиль серверов динамической авторизации.

Использование отрицательной формы команды (no) удаляет заданный сервер динамической авторизации (DAS).

Синтаксис

```
[no] das-server <NAME>
```

Параметры

<NAME> – имя сервера динамической авторизации (DAS), задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-AAA-DAS-PROFILE

Пример

```
wlc-30(config-aaa-das-profile)# das-server mainesr
```

dead-interval

Данной командой задаётся интервал, в течении которого на RADIUS-сервер не будут отправляться пакеты. В данное состояние RADIUS-сервер переводится по истечении таймаута ожидания ответа на запрос последнего допустимого повтора (см. раздел radius-server retransmit).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dead-interval <SEC>
no dead-interval
```

Параметры

<SEC> – период времени в секундах, принимает значения [0..3600].

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# dead-interval 600
```

description

Команда используется для изменения описания профиля серверов динамической авторизации (DAS) или профиля RADIUS-серверов.

Использование отрицательной формы команды (no) удаляет описание профиля.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DAS-SERVER-PROFILE

CONFIG-RADIUS-SERVER-PROFILE

Пример:

Установить описание для профиля IP-адресов:

```
wlc-30(config-aaa-das-profile)# description "Main profile"
```

disable

Данной командой производится понижение уровня привилегий пользователя до первоначальных.

Синтаксис

```
disable
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

2

Командный режим

ROOT

Пример:

```
wlc-30# disable
wlc-30>
```

enable

Данной командой производится повышение уровня привилегий пользователя. Способы аутентификации повышения привилегий пользователей задаются с помощью команды, описанной в разделе aaa authentication attempts max-fail.

По умолчанию в конфигурации установлен метод аутентификации по паролю «enable». При этом пароли не заданы, то есть любой системный пользователь может получить 15 необходимый уровень привилегий.

Для аутентификации повышения привилегий по протоколам TACACS/RADIUS/LDAP на сервере должны быть созданы пользователи $enab<PRIV>$, где <PRIV> – необходимый уровень привилегий пользователя, который должен быть аутентифицирован.

Синтаксис

enable [<PRIV>]

Параметры

<PRIV> – необходимый уровень привилегий, принимает значение [2..15].

Значение по умолчанию

15

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30> enable 10
wlc-30#
```

enable authentication

Данной командой осуществляется активация списка аутентификации повышения привилегий пользователей, который будет использоваться в конфигурируемом терминале.

В конфигурации по умолчанию активным является список с именем «default», данный список содержит один способ аутентификации – «enable».

Использование отрицательной формы команды (no) делает список с именем «default» активным.

Синтаксис

```
enable authentication <NAME>
no enable authentication
```

Параметры

<NAME> – имя списка, задаётся строкой до 31 символа.

Значение по умолчанию

default

Необходимый уровень привилегий

15

Командный режим

CONFIG-LINE-CONSOLE

CONFIG-LINE-TELNET

CONFIG-LINE-SSH

Пример:

```
wlc-30(config-line-console)# enable authentication enable-test
```

enable password

Данной командой устанавливается пароль, который будет запрашиваться при повышении уровня привилегий пользователя.

По умолчанию в конфигурации пароли не заданы, то есть любой системный пользователь может получить 15 необходимый уровень привилегий.

Использование отрицательной формы команды (no) удаляет пароль из системы.

Синтаксис

```
enable password { <CLEAR-TEXT> | encrypted <HASH_SHA512> } [ privilege <PRIV> ]
no enable password [ privilege <PRIV> ]
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [1 .. 32] символов, принимает значения [0-9a-fA-F];

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов;

<PRIV> – необходимый уровень привилегий, принимает значение [2..15], значение по умолчанию 15.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# enable password 12345678 privilege 10
```

exec-timeout

Данной командой задаётся интервал, по истечении которого будет разрываться бездействующая сессия.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`exec-timeout <SEC>`

`no exec-timeout`

Параметры

<SEC> – период времени в минутах, принимает значения [1..65535].

Значение по умолчанию

30 минут

Необходимый уровень привилегий

15

Командный режим

CONFIG-LINE-CONSOLE

CONFIG-LINE-SSH

CONFIG-LINE-TELNET

Пример:

```
wlc-30(config-line-ssh)# exec-timeout 600
```

ip sftp enable

Данной командой на контроллере включается доступ по sftp для конфигурируемого пользователя.

При использовании отрицательной формы команды (no) отключает доступ по sftp для конфигурируемого пользователя.

Синтаксис

```
[no] ip sftp enable
```

Параметры

Отсутствуют

Значение по умолчанию

Выключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-USER

Пример:

```
wlc-30(config-user)# ip sftp enable
```

key

Данной командой задаётся пароль для аутентификации на удаленном сервере.

Использование отрицательной формы команды (no) удаляет заданный пароль для аутентификации на удаленном сервере.

Синтаксис

```
key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }
no key
```

Параметры

<TEXT> – строка [8..16] ASCII-символов (для TACACS-сервера – до 60 символов);

<ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов (для TACACS-сервера – до 120 символов).

Необходимый уровень привилегий

15

Командный режим

CONFIG-TACACS-SERVER

CONFIG-RADIUS-SERVER

CONFIG-DAS-SERVER

Пример:

```
wlc-30(config-tacacs-server)# key ascii-text 12345678
```

ldap-server base-dn

Данной командой задаётся базовый DN (Distinguished name), который будет использоваться при поиске пользователей.

Использование отрицательной формы команды (no) удаляет заданный базовый DN.

Синтаксис

`ldap-server base-dn <NAME>`

`no ldap-server base-dn`

Параметры

<NAME> – базовый DN, задается строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server base-dn “dc=example,dc=com”
```

ldap-server bind authenticate root-dn

Данной командой задаётся DN (Distinguished name) пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.

Использование отрицательной формы команды (no) удаляет заданный DN пользователя.

Синтаксис

`ldap-server bind authenticate root-dn <NAME>`

`no bind authenticate root-dn`

Параметры

<NAME> – DN пользователя с правами администратора, задается строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server bind authenticate root-dn “cn=admin,dc=example,dc=com”
```

ldap-server bind authenticate root-password

Данной командой задаётся пароль пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.

Использование отрицательной формы команды (no) удаляет заданный пароль пользователя.

Синтаксис

```
ldap-server bind authenticate root-password ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }
```

```
no bind authenticate root-password
```

Параметры

<TEXT> – строка [8..16] ASCII-символов;

<ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server bind authenticate root-password ascii-text 12345678
```

ldap-server bind timeout

Данной командой задаётся интервал, по истечении которого устройство считает, что LDAP-сервер недоступен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ldap-server bind timeout <SEC>
no ldap-server bind timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [1..30].

Значение по умолчанию

3 секунды

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server bind timeout 5
```

ldap-server dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов LDAP-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ldap-server dscp <DSCP>
no ldap-server dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

63

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server dscp 40
```

ldap-server host

Данная команда используется для добавления LDAP-сервера в список используемых серверов и перехода в командный режим LDAP SERVER.

Использование отрицательной формы команды (no) удаляет заданный LDAP-сервер.

Синтаксис

```
[no] ldap-server host { <ADDR> | <IPV6-ADDR> | <LDAP-HOST-NAME> } [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес LDAP-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<LDAP-HOST-NAME> – DNS-имя LDAP-сервера, задаётся строкой до 31 символа. Для корректного сопоставления DNS-имени хоста с ip-адресом на контроллере должен быть запущен и настроен функционал domain lookup enable.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server host 10.100.100.1
wlc-30(config-ldap-server)#
```

ldap-server naming-attribute

Данной командой задаётся имя атрибута объекта, со значением которого идет сравнение имени искомого пользователя на LDAP-сервере.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ldap-server naming-attribute <NAME>
no ldap-server naming-attribute
```

Параметры

<NAME> – имя атрибута объекта, задаётся строкой до 127 символов.

Значение по умолчанию

uid

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server naming-attribute displayName
```

ldap-server privilege-level-attribute

Данной командой задаётся имя атрибута объекта, значение которого будет определять начальные привилегии пользователя на устройстве. Атрибут должен принимать значения [1..15]. Если указанный атрибут отсутствует или содержит недопустимое значение, то начальные привилегии пользователя будут соответствовать привилегиям пользователя «remote».

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ldap-server privilege-level-attribute <NAME>
no ldap-server privilege-level-attribute
```

Параметры

<NAME> – имя атрибута объекта, задаётся строкой до 127 символов.

Значение по умолчанию

priv-lvl

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server privilege-level-attribute title
```

ldap-server search filter user-object-class

Данной командой задаётся имя класса объектов, среди которых необходимо выполнять поиск пользователей на LDAP-сервере.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ldap-server search filter user-object-class <NAME>
no ldap-server search filter user-object-class
```

Параметры

<NAME> – имя класса объектов, задаётся строкой до 127 символов.

Значение по умолчанию

posixAccount

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server search filter user-object-class shadowAccount
```

ldap-server search scope

Данной командой задаётся область поиска пользователей в дереве LDAP-сервера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ldap-server search scope <SCOPE>
no ldap-server search scope
```

Параметры

<SCOPE> – область поиска пользователей на LDAP-сервере, принимает следующие значения:

- onelevel – выполнять поиск в объектах на следующем уровне после базового DN в дереве LDAP-сервера;

- subtree – выполнять поиск во всех объектах поддерева базового DN в дереве LDAP-сервера.

Значение по умолчанию

subtree

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server search scope onelevel
```

ldap-server search timeout

Данной командой задаётся интервал, по истечении которого устройство считает, что LDAP-сервер не нашел записей пользователей, подходящих под условие поиска.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ldap-server search timeout <SEC>`

`no ldap-server search timeout`

Параметры

<SEC> – период времени в секундах, принимает значения [0..30].

Значение по умолчанию

0 – устройство ожидает завершения поиска и получения ответа от LDAP-сервера.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server search timeout 10
```

ldap-server ssl certificate

Данной командой указывается сертификат, который будет использоваться для установления SSL-соединения с LDAP-сервером.

Использование отрицательной формы команды (no) удаляет из конфигурации сертификат для установления SSL-соединения с LDAP-сервером.

Синтаксис

```
ldap-server ssl certificate <FILE-NAME>
no ldap-server ssl certificate
```

Параметры

Отсутствуют.

Значение по умолчанию

Сертификат не указан.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server ssl certificate ldap-ssl.crt
```

ldap-server ssl check-peer disable

Данной командой отключается верификация LDAP-сервера по сертификату.

Использование отрицательной формы команды (no) включает верификацию LDAP-сервера по сертификату.

Синтаксис

```
[no] ldap-server ssl check-peer disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server ssl check-peer disable
```

ldap-server ssl enable

Данной командой включается использование SSL-соединения для LDAP-подключения (LDAP over SSL).

Использование отрицательной формы команды (no) отключается использование SSL-соединения для LDAP-подключения (LDAP over SSL).

Синтаксис

```
[no] ldap-server ssl enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# ldap-server ssl enable
```

line

Данной командой осуществляется переход в режим конфигурирования соответствующего терминала: локальная консоль, удаленная консоль (Telnet), удаленная защищенная консоль (SSH).

Использование отрицательной формы команды (no) устанавливает параметры терминала по умолчанию. Параметры по умолчанию описаны в разделах login authentication и enable authentication.

Синтаксис

```
[no] line <TYPE>
```

Параметры

<TYPE> – тип консоли:

- console – локальная консоль;
- telnet – удаленная консоль;
- ssh – защищенная удаленная консоль.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# line console
wlc-30(config-line-console)#
```

login authentication

Данной командой осуществляется активация списка аутентификации входа пользователей в систему, который будет использоваться в конфигурируемом терминале.

В конфигурации по умолчанию активным является список с именем «default», данный список содержит один способ аутентификации – «local».

Использование отрицательной формы команды (no) делает список с именем «default» активным.

Синтаксис

```
login authentication <NAME>
no login authentication
```

Параметры

<NAME> – имя списка, задаётся строкой до 31 символа.

Значение по умолчанию

default

Необходимый уровень привилегий

15

Командный режим

CONFIG-LINE-CONSOLE

CONFIG-LINE-TELNET

CONFIG-LINE-SSH

Пример:

```
wlc-30(config-line-console)# login authentication login-test
```

password

Команда для установки пароля определенному пользователю для входа в систему. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет пароль пользователя из системы.

Синтаксис

```
password { <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [1 .. 32] символов, принимает значения [0-9a-fA-F];

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-USER

CHANGE-EXPIRED-PASSWORD

Пример:

```
wlc-30(config-user) password test
```

port

Данной командой задаётся номер порта для обмена данными с удаленным сервером.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер TCP/UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

49 для TACACS-сервера

389 для LDAP-сервера

Не установлено для DAS-сервера

Необходимый уровень привилегий

15

Командный режим

CONFIG-TACACS-SERVER

CONFIG-LDAP-SERVER

CONFIG-DAS-SERVER

Пример:

```
wlc-30(config-tacacs-server)# port 4444
```

priority

Данной командой задаётся приоритет использования удаленного сервера. Чем ниже значение, тем приоритетнее сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
priority <PRIORITY>
no priority
```

Параметры

<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-TACACS-SERVER

CONFIG-RADIUS-SERVER

CONFIG-LDAP-SERVER

Пример:

```
wlc-30(config-tacacs-server)# priority 5
```

privilege

Данной командой производится установка уровня привилегий пользователя. Набор команд, который доступен пользователю, зависит от уровня привилегий. Пользователям с уровнями привилегий от 1 до 9 доступен только просмотр информации. Пользователям с уровнем привилегий от 10 до 15 доступна большая часть команд конфигурирования. Пользователям с уровнем привилегий 15 доступен полный набор команд. Требуемый необходимый уровень привилегий команд может быть изменен, описание в разделе description.

Использование отрицательной формы команды (no) устанавливает необходимый уровень привилегий по умолчанию.

Назначение начального уровня привилегий пользователям происходит следующим образом:

- необходимый уровень привилегий пользователям из локальной базы назначается указанной командой;
- необходимый уровень привилегий для пользователей, авторизовавшихся по протоколу RADIUS, берется из атрибута cisco-avpair = "shell:priv-lvl=<PRIV>";
- необходимый уровень привилегий для пользователей, авторизовавшихся по протоколу TACACS, берется из атрибута priv-lvl=<PRIV>;
- уровень привилегии для пользователей авторизовавшихся по протоколу LDAP берется из атрибута заданного командой **privilege-level-attribute**, описанной в разделе line, по умолчанию **priv-lvl=<PRIV>**;

Если при аутентификации пользователя через протоколы TACACS/RADIUS/LDAP не была получена вышеуказанная опция или была получена опция с некорректным значением, то пользователю будут назначены привилегии пользователя «remote», по умолчанию 1. Необходимый уровень привилегий пользователя «remote» можно изменить аналогично любому другому пользователю из локальной базы с помощью указанной команды.

Синтаксис

```
privilege <PRIV>
no privilege
```

Параметры

<PRIV> – необходимый уровень привилегий, принимает значение [1..15].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-USER

Пример:

```
wlc-30(config-user)# privilege 15
```

privilege

Данной командой производится установка минимального уровня привилегий пользователя, необходимого для выполнения команды из указанного поддерева команд.

Использование отрицательной формы команды (no) устанавливает необходимый уровень привилегий по умолчанию.

Синтаксис

```
privilege <COMMAND-MODE> level <PRIV> <COMMAND>
no privilege <COMMAND-MODE> <COMMAND>
```

Параметры

<COMMAND-MODE> – командный режим, может принимать значения:

- change-expired-password;
- config;
- config-aaa-das-profile;
- config-aaa-radius-profile;
- config-accsess-profile;
- config-acl;
- config-acl-rule;
- config-archive;
- config-bgp;
- config-bgp-af;
- config-bgp-group;
- config-bgp-neighbor;
- config-bridge;
- config-cellular-modem;
- config-cellular-profile;
- config-class-map;
- config-class-policy-map;
- config-das-server;
- config-dhcp-server;
- config-dhcp-vendor-id;
- config-dnat;
- config-dnat-pool;
- config-dnat-rule;
- config-dnat-ruleset;
- config-e1;
- config-gre;

- config-if-gi;
- config-if-te;
- config-ike-gw;
- config-ike-policy;
- config-ike-proposal;
- config-ip4ip4;
- config-ipsec-policy;
- config-ipsec-proposal;
- config-ipsec-vpn;
- config-ipv6-bgp-af;
- config-ipv6-bgp-group;
- config-ipv6-bgp-neighbor;
- config-ipv6-dhcp-server;
- config-ipv6-ospf;
- config-ipv6-ospf-area;
- config-ipv6-ospf-vlink;
- config-ipv6-pl;
- config-ipv6-wan-rule;
- config-ipv6-wan-target;
- config-ipv6-wan-target-list;
- config-keychain;
- config-keychain-key;
- config-l2tp-server;
- config-l2tpv3;
- config-ldap-server;
- config-line-console;
- config-line-ssh;
- config-line-telnet;
- config-loopback;
- config-lt;
- config-mst;
- config-multilink;
- config-netflow-host;
- config-network-policy;
- config-ntp;
- config-object-group-application;
- config-object-group-mac;
- config-object-group-network;
- config-object-group-service;
- config-object-group-url;
- config-openvpn;
- config-openvpn-server;
- config-ospf;
- config-ospf-area;
- config-ospf-vlink;
- config-pl;
- config-policy-map;
- config-pool;
- config-port-channel;
- config-ppp-user;
- config-pppoe;
- config-pptp;
- config-pptp-server;
- config-profile;
- config-qinq-if;
- config-radius-server;
- config-rip;

- config-route-map;
- config-route-map-rule;
- config-service-port;
- config-sflow-host;
- config-snat;
- config-snat-pool;
- config-snat-rule;
- config-snat-ruleset;
- config-snmp-host;
- config-snmp-user;
- config-softgre;
- config-subif;
- config-subscriber-control;
- config-subscriber-default-service;
- config-subtunnel;
- config-tacacs-server;
- config-tracking;
- config-user;
- config-vlan;
- config-vrf;
- config-vti;
- config-wan-rule;
- config-wan-target;
- config-wan-target-list;
- config-wireless;
- config-zone;
- config-zone-pair;
- config-zone-pair-rule;
- debug;
- root.

<PRIV> – необходимый уровень привилегий, принимает значение [1..15];

<COMMAND> – поддерево команд, задается строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

Установить для поддерева команд «show» корневого командного режима необходимый уровень привилегий 2. Команды поддерева «show interfaces» оставить с уровнем привилегий 1.

```
wlc-30(config)# privilege root level 2 "show"
wlc-30(config)# privilege root level 1 "show interfaces"
```

radius-server dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов RADIUS-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
radius-server dscp <DSCP>
no radius-server dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

63

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# radius-server dscp 40
```

radius-server host

Данная команда используется для добавления RADIUS-сервера в список используемых серверов и перехода в командный режим RADIUS SERVER.

Использование отрицательной формы команды (no) удаляет заданный RADIUS-сервер.

Синтаксис

```
[no] radius-server host { <ADDR> | <IPV6-ADDR> } [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# radius-server host 10.100.100.1
wlc-30(config-radius-server)#
```

radius-server host

Данная команда используется для добавления RADIUS-сервера в профиль RADIUS-серверов.

Использование отрицательной формы команды (no) удаляет заданный RADIUS-сервер из профиля.

Синтаксис

```
[no] radius-server host { <ADDR> | <IPV6-ADDR> } [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER-PROFILE

Пример:

```
wlc-30(config-aaa-radius-profile)# radius-server host 10.100.100.1
```

radius-server retransmit

Данной командой задаётся количество перезапросов к последнему активному RADIUS-серверу, которое будет выполнено перед выполнением запросов к следующим RADIUS-серверам в списке.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
radius-server retransmit <COUNT>
no radius-server retransmit
```

Параметры

<COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# radius-server retransmit 5
```

radius-server timeout

Данной командой задаётся интервал, по истечении которого устройство считает, что RADIUS-сервер недоступен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`radius-server timeout <SEC>`

`no radius-server timeout`

Параметры

<SEC> – период времени в секундах, принимает значения [1..30].

Значение по умолчанию

3 секунды

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# radius-server timeout 5
```

retransmit

Данной командой задаётся количество перезапросов к RADIUS-серверу, которое будет выполнено перед выполнением запросов к следующим RADIUS-серверам в списке.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
retransmit <COUNT>
no retransmit
```

Параметры

<COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10].

Значение по умолчанию

Не задан, используется значение глобального параметра, описанного в разделе radius-server retransmit.

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config)# retransmit 5
```

security passwords default-expired

Данной командой включается запрос на смену пароля по умолчанию для пользователя admin.

Использование отрицательной формы команды (no) отключает запрос на смену пароля по умолчанию.

Синтаксис

```
[no] security passwords default-expired
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Запрос на смену пароля по умолчанию отключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords default-expired
```

security passwords history

Данной командой включается режим запрета на использование ранее установленных паролей локальных пользователей. В качестве параметра указывается количество паролей сохраняемых в памяти контроллера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords history <COUNT>
no security passwords history
```

Параметры

<COUNT> – количество паролей, сохраняемых в памяти контроллера [0..15]. При уменьшении данного значения лишние более старые пароли удаляются.

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords history 5
```

security passwords lifetime

Данной командой устанавливается время действия пароля локального пользователя. При попытке подключения пользователя с истекшим паролем пользователь будет направлен в режим принудительной смены пароля.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords lifetime <TIME>
no security passwords lifetime
```

Параметры

<TIME> – интервал времени действия пароля в днях, принимает значения [1..365].

Значение по умолчанию

Время действия пароля локального пользователя не ограничено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords lifetime 30
```

security passwords lower-case

Данной командой устанавливается минимальное количество строчных букв в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords lower-case <COUNT>
no security passwords lower-case
```

Параметры

<COUNT> – минимальное количество строчных букв в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити [0..32].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords lower-case 2
```

security passwords max-length

Данной командой устанавливается ограничение на максимальную длину пароля локального пользователя и ENABLE-пароля.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords max-length <NUM>
no security passwords max-length
```

Параметры

<NUM> – максимальное количество символов в пароле, задается в диапазоне [1..32].

Значение по умолчанию

128

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords max-length 30
```

security passwords min-length

Данной командой устанавливается ограничение на минимальную длину пароля локального пользователя и ENABLE-пароля.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords min-length <NUM>
no security passwords min-length
```

Параметры

<NUM> – минимальное количество символов в пароле, задается в диапазоне [1..32].

Значение по умолчанию

8

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords min-length 10
```

security passwords numeric-count

Данной командой устанавливается минимальное количество цифр в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords numeric-count <COUNT>
no security passwords numeric-count
```

Параметры

<COUNT> – минимальное количество цифр в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити [0..32].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords numeric-count 2
```

security passwords special-case

Данной командой устанавливается минимальное количество специальных символов в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords special-case <COUNT>
no security passwords special-case
```

Параметры

<COUNT> – минимальное количество специальных символов в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити [0..32].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords special-case 2
```

security passwords symbol-types

Данной командой устанавливается минимальное количество типов символов, которые должны присутствовать в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords symbol-types <COUNT>
no security passwords symbol-types
```

Параметры

<COUNT> – минимальное количество типов символов в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити [1..4].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords symbol-types 2
```

security passwords upper-case

Данной командой устанавливается минимальное количество прописных (заглавных) букв в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2c комьюнити.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords upper-case <COUNT>
no security passwords upper-case
```

Параметры

<COUNT> – минимальное количество прописных (заглавных) букв в пароле локального пользователя, ENABLE-пароле, имени SMNPv3-пользователя и SMNPv1/SMNPv2 с комьюнити [0..32].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security passwords upper-case 2
```

security snmp-community max-length

Данной командой устанавливается ограничение на максимальную длину SMNPv1/SMNPv2 с комьюнити. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security snmp-community max-length <NUM>
no security snmp-community max-length
```

Параметры

<NUM> – максимальное количество символов в комьюнити, задается в диапазоне [1..128].

Значение по умолчанию

128

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security snmp-community max-length 30
```

security snmp-community min-length

Данной командой устанавливается ограничение на минимальную длину SMNPv1/SMNPv2 с комьюнити. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security passwords min-length <NUM>
no security passwords min-length
```

Параметры

<NUM> – минимальное количество символов в комьюнити, задается в диапазоне [1..128].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# security snmp-community min-length 10
```

show aaa accounting

Данная команда позволяет просмотреть настроенные параметры учета.

Синтаксис

```
show aaa accounting
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show aaa accounting
Login :          radius
Commands :       tacacs
```

show aaa authentication

Данная команда позволяет просмотреть списки способов аутентификации пользователей, а также активные списки каждого типа терминалов.

Синтаксис

```
show aaa authentication
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show aaa authentication
   Login Authentication Method Lists
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
List               Methods
----------------   --------------------------------
default            local
   Enable Authentication Method Lists
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
List               Methods
----------------   --------------------------------
default            enable
   Lines configuration
   ~~~~~~~~~~~~~~~~~~~
Line        Login method list                 Enable method list
---------   -------------------------------   -------------------------------
console     default                           default
telnet      default                           default
ssh         default                           default
```

show aaa ldap-servers

Данная команда позволяет просмотреть параметры LDAP-серверов.

Синтаксис

```
show aaa ldap-servers
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# show aaa ldap-servers
Base DN:                        dc=example,dc=com
Root DN:                        cn=admin,dc=example,dc=com
Root password:                  CDE65039E5591FA3
Naming attribute:               uid
Privilege level attribute:      priv-lvl
User object class:              posixAccount
DSCP:                           63
Bind timeout:                   3
Search timeout:                 0
Search scope:                   subtree
IP Address                           Port           Priority
-------------------------------   ------------   ------------
10.100.100.1                         389            1
```

show aaa radius-servers

Данная команда позволяет просмотреть параметры RADIUS-серверов.

Синтаксис

```
show aaa radius-servers
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# show aaa radius-servers
Timeout:     3
Retransmit:  1
DSCP:        63
IP Addres        Timeout      Priority     Usage        Key
------------    ----------   ----------   ----------   ----------------------------
2.2.2.2             --           1            all          9DA7076CA30B5FFE0DC9C4
2.4.4.4             --           1            all          9DA7076BA30B4EFCE5
```

show aaa tacacs-servers

Данная команда позволяет просмотреть параметры TACACS-серверов.

Синтаксис

```
show aaa tacacs-servers
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример:

```
wlc-30# show aaa tacacs-servers
Timeout :       3
DSCP:          63
IP Address               Port           Priority       Key
----------------------   ------------   ------------   --------------------------------
10.100.100.1             49             1              CDE65039E5591FA3
10.100.100.5             49             10             CDE65039E5591FA3
```

show users

Данная команда позволяет просмотреть активные сессии пользователей системы.

Синтаксис

```
show users
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show users
User name         Logged in at        Host             Timers Login/Priv   level
--------------    -----------------   --------------   -----------------   -----
admin             13/02/15 01:14:25   Console          00:29:57/00:00:00   15
1 user sessions.
```

show users accounts

Данная команда позволяет просмотреть конфигурацию пользователей системы.

Синтаксис

```
show users accounts
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show user accounts
Name                              Password                          Privilege
--------------------------------  --------------------------------  ---------
admin                             $6$1sxrvGaV8Za8oX/K$YNel5xYPZ4cj  15
                                  bemYWYNpQBQKDxWE9v0aoKgQ
                                  kRCEb0EMNuusO9Kmg7UBs7nA3buEM87e
                                  Eu.rA6tZq0
techsupport                       $6$YfwntIwU$ah7UxPZTemKhjpSWvVsV  15
                                  9jHcp. 9lweQaSldw7ZtUr
                                  uH66uZx9.EBASff//hUj8ObUaC484TNR
                                  x.
remote                            $6$YfwntIwU$ah7UxPZTemKhjpSWvVsV  1
                                  9jHcp.kqFAK.vmvyY9lweQaSldw7ZtUr
                                  uH66uZx9.EBASff//hUj8ObUaC484TNR
                                  x.
operator                          $6$eILpbbyRxedCzvVD$4RHP08mjXvNf  1
                                  urX7V/ULCZ1oHIWMwE6h5f
                                  zgwZQUZcPoZCEyaqQQqCicRMRuPwhxrQ
                                  bvGChWreW1
```

show users blocked

Данная команда позволяет просматривать список пользователей, для которых был введен неправильный пароль. Пользователь удаляется из списка после ввода правильного пароля при аутентификации.

Синтаксис

```
show users blocked [ <NAME> ]
```

Параметры

<NAME> – имя пользователя, для которого необходимо отобразить статистику неправильных попыток аутентификации, задаётся строкой до 31 символа.

Без указания имени пользователя, отображается вся таблица неправильных попыток аутентификации.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show users blocked
User name              Failures   Latest failure      From
--------------------   --------   ------------------   ----------------
tester                 4          10/09/17 08:29:42   0.0.0.0
```

source-address

Данной командой определяется IPv4/IPv6-адрес контроллера, который будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых пакетах на конфигурируемый AAA-сервер.

Использование отрицательной формы команды (no) удаляет указанный IPv4/IPv6-адрес источника.

Синтаксис

```
source-address { <ADDR> | <IPV6-ADDR> }
no source-address
```

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

CONFIG-TACACS-SERVER

CONFIG-LDAP-SERVER

Пример:

```
wlc-30(config-radius-server)# source-address 220::71
```

source-interface

Данной командой определяется интерфейс или туннель контроллера, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых пакетах на конфигурируемый AAA-сервер.

Использование отрицательной формы команды (no) удаляет указанный интерфейс или туннель.

Синтаксис

```
source-interface { <IF> | <TUN> }
```

```
no source-interface
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# source-interface gigabitethernet 1/0/1
```

system configuration-exclusively

Данной командой включается ограничение количества сессий CLI до одной.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
[no] system configuration-exclusively
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# system configuration-exclusively
```

tacacs-server dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов TACACS-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
tacacs-server dscp <DSCP>
no tacacs-server dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

63

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# tacacs-server dscp 40
```

tacacs-server host

Данная команда используется для добавления TACACS-сервера в список используемых серверов и перехода в командный режим TACACS SERVER.

Использование отрицательной формы команды (no) удаляет заданный TACACS-сервер.

Синтаксис

```
[no] tacacs-server host { <ADDR> | <IPV6-ADDR> } [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес TACACS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# tacacs-server host 10.100.100.1
wlc-30(config-tacacs-server)#
```

tacacs-server timeout

Данной командой задаётся интервал, по истечении которого устройство считает, что TACACS-сервер недоступен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
tacacs-server timeout <SEC>
```

```
no tacacs-server timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [1..30].

Значение по умолчанию

3 секунды.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# tacacs-server timeout 5
```

tech-support login enable

Данной командой включается низкоуровневый удаленный доступ к системе с помощью пользователя «techsupport». Низкоуровневый доступ к системе позволит получить технической поддержке всю необходимую информацию, когда это необходимо.

Использование отрицательной формы команды (no) выключает низкоуровневый удаленный доступ к системе с помощью пользователя «techsupport».

Синтаксис

```
[no] tech-support login enable
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# tech-support login enable
```

timeout

Данной командой задаётся интервал, по истечении которого устройство считает, что RADIUS-сервер недоступен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timeout <SEC>
no timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [1..30].

Значение по умолчанию

Не задан, используется значение глобального таймера, описанного в разделе radius-server timeout.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# timeout 7
```

usage

Данная команда определяет тип соединений для аутентификации которых будет использоваться RADIUS-сервера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
usage { all | aaa | auth | acct | pptp | l2tp }
no usage
```

Параметры

all – все типы соединений;

aaa – RADIUS-сервер будет использоваться для аутентификации, авторизации и учета telnet, ssh console сессий;

auth – RADIUS-сервер будет использоваться для аутентификации и авторизации telnet, ssh console сессий;

acct – RADIUS-сервер будет использоваться для учета telnet, ssh console сессий;

pptp – RADIUS-сервер будет использоваться для аутентификации, авторизации и учета удаленных пользователей, подключающихся по протоколу PPTP;

l2tp – RADIUS-сервер будет использоваться для аутентификации, авторизации и учета удаленных пользователей, подключающихся по протоколу L2TP over IPsec.

Значение по умолчанию

all

Необходимый уровень привилегий

15

Командный режим

CONFIG-RADIUS-SERVER

Пример:

```
wlc-30(config-radius-server)# usage pptp
```

username

Данной командой выполняется добавление пользователя в локальную базу пользователей и осуществляется переход в режим настройки параметров пользователя.

Использование отрицательной формы команды (no) удаляет пользователя из системы.

Синтаксис

`[no] username <NAME>`

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа. Если использовать команду для удаления, то при указании значения «all» будут удалены все пользователи.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример:

```
wlc-30(config)# username test
wlc-30(config-user)#
```

Настройка RADIUS-сервера

- acct-port
- auth-port
- domain
- enable
- host
- key
- nas
- network
- password
- port
- priority
- proxy-mode
- radius-server local
- server-type
- upstream-server
- user
- virtual-server

acct-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аккаунтинга.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
acct-port <PORT>
no acct-port
```

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1813

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-VSERVER

Пример

```
wlc-30(config-radius-vserver)# acct-port 1813
```

auth-port

Данной командой задаётся номер порта для обмена данными с удаленным RADIUS-сервером при выполнении аутентификации и авторизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
auth-port <PORT>
no auth-port
```

Параметры

<PORT> – номер UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

1812

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-VSERVER

Пример:

```
wlc-30(config-radius-vserver)# auth-port 1812
```

domain

Данная команда создает/назначает домен.

Использование отрицательной формы команды (no) удаляет домен.

Синтаксис

```
domain <DOMAIN>
no domain { <DOMAIN> | all }
```

Параметры

<DOMAIN> – идентификатор домена, задается строкой до 235 символов;

all – команда удаляет все созданные домены.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS

Пример

```
wlc-30(config-radius)# domain test
```

enable

Данная команда предназначена для активации функций сервера.

Использование отрицательной формы команды (no) отключает функции.

Синтаксис

`[no] enable`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS

CONFIG-RADIUS-VSERVER

Пример

```
wlc-30(config-radius)# enable
```

host

Данной командой задаётся IP-адрес удаленного хоста для аутентификациии и авторизации.

Использование отрицательной формы команды (no) удаляет хост.

Синтаксис

```
host <ADDR>
no host
```

Параметры

<ADDR> - IP-адрес удаленного хоста, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-UPSTREAM-SERVER

Пример:

```
wlc-30(config-radius-upstream-server)# host 192.168.1.1
```

key

Данной командой задаётся ключ аутентификации.

Использование отрицательной формы команды (no) удаляет заданный ключ.

Синтаксис

```
key ascii-text { <KEY> | encrypted <ENCRYPTED-KEY> }
no key
```

Параметры

<KEY> – строка из [4..64] ASCII-символов;

<ENCRYPTED-KEY> – зашифрованный ключ, задаётся строкой [8..128] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-NAS

CONFIG-RADIUS-UPSTREAM-SERVER

Пример:

```
wlc-30(config-radius-upstream-server)# key ascii-text password
```

nas

Данной командой задаётся NAS.

Использование отрицательной формы команды (no) удаляет NAS.

Синтаксис

```
nas <NAME>
no nas { <NAME> | all }
```

Параметры

<NAME> – название, задается строкой до 235 символов;

all – команда удаляет все NAS.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS

Пример:

```
wlc-30(config-radius)# nas test
```

network

Данной командой задаётся доступное сетевое пространство.

Использование отрицательной формы команды (no) удаляет сеть.

Синтаксис

```
network <ADDR/LEN>
no network
```

Параметры

<ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-NAS

Пример:

```
wlc-30(config-radius-nas)# network 192.168.1.0/24
```

password

Команда для установки пароля определенному пользователю.

Использование отрицательной формы команды (no) удаляет пароль пользователя.

Синтаксис

```
password ascii-text { <PASSWORD> | encrypted <ENCRYPTED-PASSWORD> }
no password
```

Параметры

<PASSWORD> – пароль, задаётся строкой [8.. 64] символа.

<ENCRYPTED-PASSWORD> – зашифрованный пароль, задается строкой [16-128] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-USER

Пример

```
wlc-30(config-radius-user)# password ascii-text password
```

port

Данной командой задаётся номер порта для обмена данными с удаленным сервером.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер TCP/UDP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-UPSTREAM-SERVER

Пример:

```
wlc-30(config-radius-upstream-server)# port 1812
```

priority

Данной командой задаётся приоритет использования удаленного сервера. Чем ниже значение, тем приоритетнее сервер.

Использование отрицательной формы команды (no) удаляет параметр.

Синтаксис

```
priority <PRIORITY>
no priority
```

Параметры

<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..100].

Значение по умолчанию

Отсутствует

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-UPSTREAM-SERVER

Пример:

```
wlc-30(config-radius-upstream-server)# priority 1
```

proxy-mode

Данной командой активируется режим проксирования RADIUS-сервера.

Использование отрицательной формы команды (no) отключает режим проксирования.

Синтаксис

`[no] proxy-mode`

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-VSERVER

Пример:

```
wlc-30(config-radius-vserver)# proxy-mode
```

radius-server local

Данной командой осуществляется переход в настройки локального RADIUS-сервера.

Использование отрицательной формы команды (no) удаляет сконфигурированные настройки.

Синтаксис

`[no] radius-server local`

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# radius-server local
```

server-type

Данная команда указывает тип сервера.

Использование отрицательной формы команды (no) возвращает значение по умолчанию.

Синтаксис

```
server-type { auth | acct | auth+acct }
no server-type
```

Параметры

auth – RADIUS-сервер будет использоваться для аутентификации, авторизации;

acct – RADIUS-сервер будет использоваться для сбора акаунтинга;

auth+acct – RADIUS-сервер будет выполнять обе функции.

Значение по умолчанию

auth

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-UPSTREAM-SERVER

Пример:

```
wlc-30(config-radius-upstream-server)# server-type auth+acct
```

upstream-server

Данная команда добавляет upstream RADIUS-сервер.

Использование отрицательной формы команды (no) удаляет upstream RADIUS-сервер.

Синтаксис

```
upstream-server <NAME>
no upstream-server { <NAME> | all }
```

Параметры

<NAME> – название upstream RADIUS-сервера, задается строкой до 246 символов;

all – команда удаляет все upstream RADIUS-сервера.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-VSERVER

Пример:

```
wlc-30(config-radius-vserver)# upstream-server test
```

user

Данной командой выполняется добавление пользователя в локальную базу пользователей и осуществляется переход в режим настройки параметров пользователя.

Использование отрицательной формы команды (no) удаляет конкретного пользователя или сразу всех пользователей из системы.

Синтаксис

```
user <USER>
no user { <USER> | all }
```

Параметры

<NAME> – имя пользователя, задается строкой до 246 символов;

all – команда удаляет всех созданных пользователей.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS-DOMAIN

Пример

```
wlc-30(config-radius-domain)# user test
```

virtual-server

Данной командой выполняется добавление виртуального RADIUS-сервера и осуществляется переход в режим настройки его параметров.

Использование отрицательной формы команды (no) удаляет виртуальный RADIUS-сервер.

Синтаксис

```
virtual-server <NAME>
no virtual-server { <NAME> | all }
```

Параметры

<NAME> – название виртуального RADIUS-сервера, задается строкой до 235 символов;

all – команда удаляет все созданные RADIUS-сервера.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RADIUS

Пример

```
wlc-30(config-radius)# virtual-server test
```

13 Конфигурирование и мониторинг интерфейсов

- Общие команды
  - clear interfaces counters
  - description
  - history statistics
  - interface
  - ip tcp adjust-mss
  - load-average
  - mode
  - mtu
  - rate-limit arp-broadcast
  - rate-limit arp-broadcast pps
  - show interfaces counters
  - show interfaces description
  - show interfaces history
  - show interfaces status
  - show interfaces utilization
  - shutdown
  - speed
  - switchport dot1q ethertype egress stag
  - switchport mode
  - system jumbo-frames
- Физические интерфейсы
  - snmp trap link-status
  - show interfaces sfp
  - show interfaces switch-port status
  - threshold rx-utilization
  - threshold rx-utilization monitoring
  - threshold tx-utilization
  - threshold tx-utilization monitoring
- Агрегированные интерфейсы
  - channel-group
  - lacp port-priority
  - lacp system-priority
  - lacp timeout
  - port-channel load-balance
  - show interfaces port-channel
  - show lacp interfaces
  - show lacp parameters
- E1/multilink
  - enable
  - ip tcp header-compression
  - ip tcp compression-connections
  - mrru
  - password
  - ppp authentication chap
  - ppp chap hostname
  - ppp chap password
  - ppp chap refuse
  - ppp chap username
  - ppp ipcp accept-address
  - ppp ipcp remote-address
  - ppp max-configure
  - ppp max-failure
  - ppp max-terminate

    - ppp mru
    - ppp multilink
    - ppp multilink-group
    - ppp timeout keepalive
    - ppp timeout retry
    - show controllers e1
    - switchport e1 slot
    - switchport e1 clock source
    - switchport e1 crc
    - switchport e1 framing
    - switchport e1 invert data
    - switchport e1 linecode
    - switchport e1 timeslots
    - switchport e1 unframed
    - switchport mode e1
- Беспроводные модемы
    - allowed-auth
    - allowed-mode
    - apn
    - cellular modem
    - cellular profile
    - device
    - enable
    - ip-version
    - mru
    - number
    - password
    - pin
    - preferred-mode
    - profile
    - show cellular configuration modem
    - show cellular configuration profile
    - show cellulas status modem
    - user

Порядок именования интерфейсов контроллера описан в разделе Типы и порядок именования интерфейсов контроллера.

Команды, введенные в режиме конфигурирования интерфейса (группы интерфейсов), применяются к выбранному интерфейсу (группе интерфейсов).

Общие команды

clear interfaces counters

Данной командой осуществляется сброс счетчиков заданного системного интерфейса или группы интерфейсов.

Синтаксис

```
clear interfaces counters [<IF>]
```

Параметры

<IF> – наименование системного интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Можно указать несколько интерфейсов перечислением через «,» либо указать диапазон интерфейсов через «-». Если не указывать индексы интерфейсов, то будут очищены счетчики всех интерфейсов заданной группы. При выполнении команды без параметра будут очищены счетчики всех системных интерфейсов.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# clear interfaces counters gigabitethernet 1/0/5
```

description

Данная команда используется для изменения описания конфигурируемого интерфейса.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

`description <DESCRIPTION>`

`no description`

Параметры

<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-MULTILINK

CONFIG-SERVICE-PORT

CONFIG-CELLULAR-PROFILE

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-if-gi)# description "Uplink interface"
```

history statistics

Данной командой включается запись статистики использования текущего интерфейса.

Использование отрицательной формы команды (no) отключает запись статистики использования текущего интерфейса.

Синтаксис

```
[no] history statistics
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-LOOPBACK

CONFIG-MULTILINK

CONFIG-E1

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-if-gi)# history statistics
```

interface

Данная команда позволяет перейти в режим конфигурирования одного или более интерфейсов.

Использование отрицательной формы команды (no) восстанавливает настройки интерфейса по умолчанию.

Синтаксис

```
[no] interface <IF>
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример 1

Переход в режим конфигурирования Ethernet-интерфейса gi 1/0/20:

```
wlc-30(config)# interface gigabitethernet 1/0/20
wlc-30(config-if-gi)#
```

Пример 2

Переход в режим конфигурирования Ethernet-интерфейса te 1/0/2:

```
wlc-30(config)# interface tengigabitethernet 1/0/2
wlc-30(config-if-te)#
```

Пример 3

Переход в режим конфигурирования виртуального интерфейса:

```
wlc-30(config)# interface loopback 5
wlc-30(config-loopback)#
```

Пример 4

Переход в режим конфигурирования сабинтерфейса:

```
wlc-30(config)# interface gigabitethernet 1/0/20.20
wlc-30(config-subif)#
```

Пример 5

Переход в режим конфигурирования интерфейса port-channel 2:

```
wlc-30(config)# interface port-channel 2
wlc-30(config-port-channel)#
```

Пример 6

Переход в режим конфигурирования интерфейса e1 1/0/1:

```
wlc-30(config)# interface e1 1/0/1
wlc-30(config-e1)#
```

Пример 7

Переход в режим конфигурирования интерфейса multilink 1:

```
wlc-30(config)# interface multilink 1
wlc-30(config-multilink)#
```

ip tcp adjust-mss

Данной командой переопределяется значение поля MSS (Maximum segment size) во входящих TCP-пакетах.

Использование отрицательной формы команды (no) отключает корректировку значение поля MSS.

Синтаксис

`ip tcp adjust-mss <MSS>`

`no ip tcp adjust-mss`

Параметры

<MSS> – значение MSS, принимает значения в диапазоне [500..1460].

Значение по умолчанию

1460

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ip tcp adjust-mss 1400
```

load-average

Данной командой устанавливается интервал времени, по которому происходит расчет утилизации интерфейса.

Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

`load-average <TIME>`

`no load-average`

Параметры

<TIME> – интервал в секундах, принимает значения [5..150].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-E1

CONFIG-MULTILINK

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-if-gi)# load-average 30
```

mode

Данной командой устанавливается режим работы физического/агрегированного интерфейса.

Использование отрицательной формы команды (no) устанавливает значение режима по умолчанию.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – режим работы физического/агрегированного интерфейса, принимает значения:

- switchport – устанавливает L2-режим. Возможно разрешение vlan, но запрещено назначение IP-адреса и создание саб/qinq-интерфейсов;
- routerport – устанавливает L3-режим. Возможно назначение IP-адреса и создание саб/qinq-интерфейсов, но запрещено разрешение vlan на интерфейсе.

Значение по умолчанию

routerport

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# mode switchport
```

mtu

Данной командой указывается размер MTU (Maximum Transmition Unit) для интерфейсов.

Использование отрицательной формы команды (no) устанавливает значение MTU по умолчанию.

Синтаксис

```
mtu <MTU>
no mtu
```

Параметры

<MTU> – значение MTU в байтах, принимает значения в диапазоне:

WLC-30 – [552..9500]

Для Serial, E1 и multilink-интерфейсов – [552-1500].

Значения MTU более 1500 можно выставлять только при включенной поддержке Jumbo-фреймов, описанной в разделе system jumbo-frames.

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-if-gi)# mtu 1400
```

rate-limit arp-broadcast

Данной командой включается ограничение приема arp-запросов на bridge-интерфейсе.

При использовании отрицательной формы команды (no) отключается ограничение приема arp-запросов на bridge-интерфейсе.

Синтаксис

```
[no] rate-limit arp-broadcast
```

Параметры

Отсутствуют.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример:

```
wlc-30(config-bridge)# rate-limit arp-broadcast
```

rate-limit arp-broadcast pps

Данной командой устанавливается максимальный порог приема arp-запросов на bridge-интерфейсе. Данный параметр работает только при включенном режиме ограничения приема arp-запросов на bridge-интерфейсе.

При использовании отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
rate-limit arp-broadcast pps <PPS>
no rate-limit arp-broadcast pps
```

Параметры

<PPS> – количество arp-запросов, задается в диапазоне [1..65535].

Значение по умолчанию

100

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример:

```
wlc-30(config-bridge)# rate-limit arp-broadcast pps 2000
```

show interfaces counters

Командой выполняется просмотр счетчиков на системных интерфейсах: портах, сабинтерфейсах, группах агрегации, сетевых мостах.

Синтаксис

```
show interfaces counters [ <IF> ]
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Команда отображает счётчики для портов контроллера, сабинтерфейсов и туннельных интерфейсов.

Можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены счетчики всех интерфейсов заданной группы. Если задан определённый интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны счетчики всех системных интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces counters gigabitethernet 1/0/4-6
Interface       UC recv         Bytes recv      Errors recv     MC recv
-------------   -------------   -------------   -------------   -------------
gi1/0/4         0               0               0               0
gi1/0/5         0               0               0               0
gi1/0/6         0               0               0               0
Interface       UC sent         Bytes sent      Errors sent
-------------   -------------   -------------   -------------
gi1/0/4         0               0               0
gi1/0/5         1138            393748          0
gi1/0/6         0               0               0
wlc-30# show interfaces counters gigabitethernet 1/0/4
 Packets received:               0
 Bytes received:                 0
 Dropped on receive:             0
 Receive errors:                 0
 Multicasts received:            0
 Receive length errors:          0
 Receive buffer overflow errors: 0
 Receive CRC errors:             0
 Receive frame errors:           0
 Receive FIFO errors:            0
```

```
Receive missed errors:          0
Receive compressed:             0
Packets transmitted:            0
Bytes transmitted:              0
Dropped on transmit:            0
Transmit errors:                0
Transmit aborted errors:        0
Transmit carrier errors:        0
Transmit FIFO errors:           0
Transmit heartbeat errors:      0
Transmit window errors:         0
Transmit comressed:             0
Collisions:                     0
```

show interfaces description

Команда используется для просмотра описания системных интерфейсов.

Синтаксис

```
show interfaces description [ <IF> ]
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы. При выполнении команды без параметра будут показаны описания всех системных интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces description gigabitethernet 1/0/4-5
Interface       Admin   Link    Description
                State   State
-------------   -----   -----   ------------------------------------------------------
gi1/0/4         Up      Down    Link to NSK
gi1/0/5         Up      Down    Link to MSK
```

show interfaces history

Команда используется для просмотра статистики использования интерфейса.

Синтаксис

```
show interfaces history [<IF>] [timer <TIMER>]
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

<TIMER> – не обязательный ключ timer. В качестве параметров для данного ключа могут выступать:

- hours отображает историю за последние 72 часа;
- minutes отображает историю за последние 60 минут;
- seconds отображает историю за последние 60 секунд;
- При отсутствии ключа timer выводятся 3 таблицы истории использования туннеля (туннелей).

Необходимый уровень привилегий

5

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces history gi 1/0/1 timer minutes
gi1/0/1
Last 60 minutes:
Timer  Recv utilization,    Sent utilization,   Recv errors  Sent errors   Output drops
       Kbit/s               Kbit/s
------ -----------------    ----------------    ------------ ------------  -----------
0-1   240                   16                  0            0             0
1-2   961                   64                  0            0             0
2-3   962                   64                  0            0             0
3-4   962                   64                  0            0             0
4-5   960                   64                  0            0             0
5-6   961                   64                  0            0             0
6-7   719                   64                  0            0             0
7-8   960                   64                  0            0             0
8-9   800                   65                  0            0             0
9-10  962                   64                  0            0             0
10-11 865                   64                  0            0             0
11-12 962                   64                  0            0             0
12-13 817                   65                  0            0             0
13-14 962                   65                  0            0             0
14-15 961                   65                  0            0             0
15-16 880                   60                  0            0             0
16-17 960                   63                  0            0             0
17-18  0                    0                   0            0             0
18-19  0                    0                   0            0             0
19-20  0                    0                   0            0             0
20-21  0                    0                   0            0             0
21-22  0                    0                   0            0             0
```

show interfaces status

Команда используется для просмотра состояния системных интерфейсов.

Синтаксис

```
show interfaces status [<IF>]
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы. Если задан конкретный интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны статусы всех системных интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces status gigabitethernet 1/0/1-2
Interface       Admin   Link    MTU      MAC address          Uptime
                state   state
-------------   -----   -----   ------   ------------------   -------------------------
gi1/0/1         Up      Down    1500     a8:f9:4b:aa:53:fc    --
gi1/0/2         Up      Up      1500     a8:f9:4b:aa:53:fd    15 hours, 17 minutes and 52
seconds
```

show interfaces utilization

Команда используется для просмотра текущей нагрузки на физических интерфейсах.

Синтаксис

```
show interfaces utilization [ <IF> ]
```

Параметры

<IF> – имя физического интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Можно указать несколько интерфейсов перечислением через запятую «,» либо указать диапазон интерфейсов через дефис «-». Если не указывать индексы интерфейсов, то будет отображена текущая нагрузка для всех интерфейсов заданной группы. При выполнении команды без параметра будет показана текущая нагрузка для всех физических интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces utilization gigabitethernet 1/0/3-5,1/0/9
Port       Period, s     Sent,         Recv,         Frames Sent   Frames Recv
                         Kbit/s        Kbit/s
--------   -----------   -----------   -----------   -----------   -----------
gi1/0/3    5             0             0             0             0
gi1/0/4    5             0             0             0             0
gi1/0/5    5             0             0             0             0
gi1/0/9    5             0             0             0             0
```

shutdown

Данной командой отключается конфигурируемый интерфейс.

Использование отрицательной формы команды (no) включает конфигурируемый интерфейс.

Синтаксис

```
[no] shutdown
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-if-gi)# shutdown
```

Конфигурируемый интерфейс отключен.

speed

Данной командой устанавливается значение скорости для конфигурируемого интерфейса, группы интерфейсов. Командой могут быть установлены следующие режимы: 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с, 10 Гбит/с или auto.

Использование отрицательной (no) формы команды устанавливает значение по умолчанию.

Синтаксис

```
speed <SPEED> <DUPLEX>
no speed
```

Параметры

<SPEED> – значение скорости:

- 10M – значение скорости 10 Мбит/с;
- 100M – значение скорости 100 Мбит/с;
- 1000M – значение скорости 1000 Мбит/с;
- 10G – значение скорости 10 Гбит/с;
- auto – автоматический выбор режима (недоступно для 10G-интерфейсов).

<DUPLEX> – режим работы приемопередатчика, принимает значения:

- full-duplex – дуплекс;
- half-duplex – полудуплекс.

Значение по умолчанию

auto

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример 1

```
wlc-30(config-if-te)# speed 10G
```

Установлен скоростной режим интерфейса 10 Гбит/с.

Пример 2

```
wlc-30(config-if-gi)# speed 10M full-duplex
```

Установлен скоростной режим интерфейса 10 Мбит/с, дуплекс.

switchport dot1q ethertype egress stag

Данной командой настраивается EtherType для сервисного VLAN в исходящих пакетах.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] switchport dot1q ethertype egress stag { 802.1q | 802.1ad }
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

802.1q (0x8100)

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# switchport dot1q ethertype egress stag 802.1ad
```

switchport mode

Данная команда используется для задания режима работы интерфейса с VLAN.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport mode <MODE>
no switchport mode
```

Параметры

<MODE> – режим работы:

- access – интерфейс доступа, нетегированный интерфейс для одной VLAN;
- trunk – интерфейс, принимающий только тегированный трафик за исключением одного VLAN, который может быть добавлен с помощью команды **switchport trunk native vlan**, описанной в switchport trunk native-vlan;
- e1 – физический интерфейс переключается в режим E1 (не применима для агрегированных интерфейсов).

Значение по умолчанию

access

general

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# switchport mode trunk
```

system jumbo-frames

Данной командой включается поддержка Jumbo-фреймов. Для вступления изменений в силу требуется перезагрузка устройства.

Использование отрицательной формы команды (no) выключает поддержку Jumbo-фреймов.

Синтаксис

```
[no] system jumbo-frames
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# system jumbo-frames
```

Физические интерфейсы

snmp trap link-status

Данная команда используется для включения отправки snmp-trap о включении/выключении туннеля.

Использование отрицательной формы команды (no) отключает отправку snmp-trap о включении/выключении туннеля.

Синтаксис

```
[no] snmp trap link-status
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# snmp trap link-status
```

show interfaces sfp

Команда используется для просмотра информации об SFP-трансиверах.

Синтаксис

```
show interfaces sfp [ <IF> ]
```

Параметры

<IF> – имя физического интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера. В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы. Если задан определенный интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны статусы всех системных интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces sfp
Interface 'te1/0/1':
 SFP present:       Yes
 Connector Type:    LC
 Type:              SFP/SFP+
 Compliance code:   10G BASE-SR
 Laser wavelength:  850 nm
 Transfer distance: 300.00 m
 Vendor OUI:        24:00:00
 Vendor name:       Modultech
 Vendor PN:         MT-PP-85192-SR
 Vendor SN:         M1204011007
 Vendor date:       04.05.12
 Vendor revision:   1.0
 DDM supported:     Yes
 Temperature:       40.562 C
 Voltage:           3.3364 V
 Current:           6.004 mA
 RX Power:          0.0001 mW / -40.0000 dBm
 TX Power:          0.4398 mW / -3.5674 dBm
 RX LOS:            Yes
 TX Fault:          No
 TX Disable:        No
 Soft TX Disable:   No
Interface 'te1/0/2':
 SFP present:       Yes
 Connector Type:    SC
 Type:              SFP/SFP+
 Compliance code:   1000BASE-LX
 Laser wavelength:  1310 nm
 Transfer distance: 20.00 km
 Vendor OUI:        --
 Vendor name:       OEM
 Vendor PN:         APSB35123CXS20
 Vendor SN:         SG35224701333
 Vendor date:       12.12.12
 Vendor revision:   1.00
 DDM supported:     No
```

show interfaces switch-port status

Команда используется для просмотра состояния физических интерфейсов.

Синтаксис

```
show interfaces switch-port status [ <IF> ]
```

Параметры

<IF> – имя физического или агрегированного интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

Можно указать несколько интерфейсов перечислением через запятую «,» либо указать диапазон интерфейсов через дефис «-». Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы. Если задан определенный интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны статусы всех физических интерфейсов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces switch-port status
Port       Media    Duplex   Speed   Neg        Flow   Link    Back       MDI       Port
                                                ctrl   State   Pressure   Mode      Mode
--------   ------   ------   -----   --------   ----   -----   --------   -------   -------
gi1/0/1    --       --       --      Enabled    --     Down    --         --        access
gi1/0/2    --       --       --      Enabled    --     Down    --         --        access
gi1/0/3    --       --       --      Enabled    --     Down    --         --        access
gi1/0/4    --       --       --      Enabled    --     Down    --         --        access
gi1/0/5    --       --       --      Enabled    --     Down    --         --        access
gi1/0/6    --       --       --      Enabled    --     Down    --         --        access

wlc-30# show interfaces switch-port status gigabitethernet 1/0/2
Interface       gigabitethernet 1/0/2
  Status:       up
  Media:        copper
  Speed:        100 Mbps
  Duplex:       full
  Flow control: no
  MAC address:  a8:f9:b5:00:00:25
MAC status:
  Buffers full:            no
  Doing back pressure:     no
  Sending PAUSE frames:    no
  Receiving PAUSE frames:  no
  Auto-Negotiation done:   yes
  Sync fail:               no
```

threshold rx-utilization

Данная команда используется для задания порога входящей нагрузки интерфейса для отправки snmp-trap eltexInterfaceRxUtilizationHigh и eltexInterfaceRxUtilizationHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
threshold rx-utilization <TH-HIGH> clear <TH-LOW>
no threshold rx-utilization
```

Параметры

<TH-HIGH> – порог в процентах для отправки snmp-trap eltexInterfaceRxUtilizationHigh;

<TH-LOW> – порог в процентах для отправки snmp-trap eltexInterfaceRxUtilizationHighOk.

Значение по умолчанию

<TH-HIGH> – 90%;

<TH-LOW> – 85%.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# threshold rx-utilization 90 clear 80
```

threshold rx-utilization monitoring

Данная команда используется для включения отправки snmp-trap eltexInterfaceRxUtilizationHigh и eltexInterfaceRxUtilizationHighOk.

Использование отрицательной формы команды (no) отключает отправку snmp-trap eltexInterfaceRxUtilizationHigh и eltexInterfaceRxUtilizationHighOk.

Синтаксис

```
[no] threshold rx-utilization monitoring
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# threshold rx-utilization monitoring
```

threshold tx-utilization

Данная команда используется для задания порогов исходящей нагрузки интерфейса для отправки snmp-trap eltexInterface TxUtilizationHigh и eltexInterface TxUtilizationHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
threshold tx-utilization <TH-HIGH> clear <TH-LOW>
no threshold tx-utilization
```

Параметры

<TH-HIGH> – порог в процентах для отправки snmp-trap eltexInterfaceTxUtilizationHigh ;

<TH-LOW> – порог в процентах для отправки snmp-trap eltexInterfaceTxUtilizationHighOk.

Значение по умолчанию

<TH-HIGH> – 90%;

<TH-LOW> – 85%.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# threshold tx-utilization 90 clear 80
```

threshold tx-utilization monitoring

Данная команда используется для включения отправки snmp-trap eltexInterface TxUtilizationHigh и eltexInterface TxUtilizationHighOk.

Использование отрицательной формы команды (no) отключает отправку snmp-trap eltexInterface TxUtilizationHigh и eltexInterface TxUtilizationHighOk.

Синтаксис

```
[no] threshold tx-utilization monitoring
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример:

```
wlc-30(config-if-gi)# threshold tx-utilization monitoring
```

Агрегированные интерфейсы

channel-group

Данной командой физический интерфейс включается в группу агрегации каналов.

Использование отрицательной формы команды (no) удаляет интерфейс из группы агрегации каналов.

Синтаксис

```
channel-group <ID> mode <MODE>
no channel-group
```

Параметры

<ID> – порядковый номер группы агрегации каналов, принимает значения [1..12];

<MODE> – режим формирования группы агрегации каналов:

- auto – добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP;
- on – добавить интерфейс в статическую группу агрегации.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# channel-group 6 mode auto
```

lacp port-priority

Данной командой устанавливается LACP-приоритет интерфейса Ethernet.

Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
lacp port-priority <PRIORITY>
no lacp port-priority
```

Параметры

<PRIORITY> – приоритет, указывается в диапазоне [1..65535].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# lacp port-priority 5000
```

lacp system-priority

Данной командой устанавливается приоритет системы для протокола LACP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
lacp system-priority <PRIORITY>
no lacp system-priority
```

Параметры

<PRIORITY> – приоритет, указывается в диапазоне [1..65535].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# lacp system-priority 5000
```

lacp timeout

Данной командой устанавливается административный таймаут протокола LACP.

Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
lacp timeout { short | long }
no lacp timeout
```

Параметры

long – длительное время таймаута (90 секунд);

short – короткое время таймаута (3 секунды).

Значение по умолчанию

long

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# lacp timeout short
```

port-channel load-balance

Данной командой устанавливается механизм балансировки нагрузки для групп агрегации каналов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`port-channel load-balance {src-dst-mac-ip|src-dst-mac|src-dst-ip|src-dst-mac-ip-port}`

`no port-channel load-balance`

Параметры

active-backup – весь трафик отправляется в один интерфейс и перенаправляется в другой, если первый перешел в состояние down;

src-dst-mac – механизм балансировки основывается на MAC-адресах отправителя и получателя;

src-dst-mac-ip – механизм балансировки основывается на MAC-адресах и IP-адресах отправителя и получателя;

src-dst-ip-port – механизм балансировки основывается на IP-адресах и tcp/udp-портах отправителя и получателя.

Значение по умолчанию

src-dst-mac

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# port-channel load-balance src-dst-mac-ip
```

show interfaces port-channel

Данная команда используется для просмотра информации о членах группы агрегации каналов.

Синтаксис

```
show interfaces port-channel [<ID>]
```

Параметры

<ID> – порядковый номер группы агрегации каналов, принимает значения в диапазоне [1..12].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show interfaces port-channel 1
load-balance: src-dst-mac
Channels   Ports
--------   ---------------------------------------
po1        gi1/0/21
```

show lacp interfaces

Данная команда используется для просмотра информации о протоколе LACP.

Синтаксис

```
show lacp interfaces [ <IF> ]
```

Параметры

<IF> – имя физического или агрегированного интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будет отображена информация о LACP-протоколе для всех интерфейсов заданной группы.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show lacp interfaces port-channel 2
port-channel 2 [aggregator 1, active] ports count: 1
                   Actor Port             Partner Port
----------------   --------------------   --------------------
System Priority    32768                  1
System MAC         a8:f9:4b:aa:12:40      a8:f9:4b:83:01:80
Key                8000                   1
port-channel 2 [aggregator 2, backup] ports count: 1
                   Actor Port             Partner Port
----------------   --------------------   --------------------
System Priority    32768                  65535
System MAC         a8:f9:4b:aa:12:40      00:00:00:00:00:00
Key                8000                   FFFF
wlc-30# show lacp interfaces gigabitethernet 1/0/1
gigabitethernet 1/0/1 [active] up
                   Actor Port     Partner Port
----------------   ------------   ------------
Port Priority      32768          1
LACP Activity      Active         Active
```

show lacp parameters

Данная команда используется для просмотра параметров настройки протокола LACP для интерфейса Ethernet.

Синтаксис

```
show lacp parameters [ <IF> ]
```

Параметры

<IF> – имя физического интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера. Возможно использование только физических интерфейсов.

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены параметры всех интерфейсов заданной группы. Если задан конкретный интерфейс, то будет отображена детальная информация по данному интерфейсу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show lacp parameters tengigabitethernet 1/0/2
   LACP parameters
   ~~~~~~~~~~~~~~~
Interface   Port Priority   Timeout   Mode
---------   -------------   -------   -------
te1/0/2    32768           Short     Active
```

E1/multilink

enable

Данной командой включается PPP-пользователь.

Использование отрицательной формы команды (no) отключает PPP-пользователя.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

PPP-пользователь отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPP-USER

Пример:

```
wlc-30(config-ppp-user)# enable
```

ip tcp header-compression

Данной командой включается протокол сжатия tcp-заголовком. Протокол используется для улучшения производительности низкоскоростных каналов связи.

Использование отрицательной формы команды (no) отключает протокол сжатия tcp-заголовков.

Синтаксис

```
[no] ip tcp header-compression
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
(config-e1)# ip tcp header-compression
```

ip tcp compression-connections

Данной командой указывается количество одновременных tcp-соединений, для которых будет использоваться протокол компрессии tcp-заголовков.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию для количества одновременных tcp-соединений, для которых будет использоваться протокол компрессии tcp-заголовков.

Синтаксис

`ip tcp compression-connections <NUMBER>`

`no ip tcp compression-connections`

Параметры

<NUMBER> – количество одновременных tcp-соединений, для которых будет использоваться протокол компрессии tcp-заголовков. Может принимать значения [2..16].

Значение по умолчанию

16

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ip tcp compression-connections 32
```

mrru

Данная команда определяет максимальный размер принимаемого пакета для MLPPP-интерфейса.

Использование отрицательной формы команды (no) устанавливает значение mrru по умолчанию.

Синтаксис

```
mrru { <MRRU> }
no mrru
```

Параметры

<MRRU> – максимальный размер принимаемого пакета для MLPPP интерфейса, принимает значения в диапазоне [1500..10000].

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-MULTILINK

Пример:

```
wlc-30(config-multilink)# mrru 1700
```

password

Команда для установки пароля в открытой или зашифрованной форме определенному пользователю для аутентификации удаленной стороны. Пароль пользователя хранится в конфигурации в зашифрованной форме. При конфигурировании можно задать пароль в открытой форме либо скопировать пароль в зашифрованной форме с другого устройства.

Использование отрицательной формы команды (no) удаляет пароль пользователя.

Синтаксис

```
password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no password
```

Параметры

<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F];

<ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов.

⚠ Пароли хранятся в конфигурации в зашифрованной форме независимо от формата, использованного при вводе команды.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPP-USER

Пример:

```
wlc-30(config-ppp-user)# password ascii-text 01234567
```

ppp authentication chap

Данной командой включается CHAP-аутентификация.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
[no] ppp authentication chap
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp authentication chap
```

ppp chap hostname

Данной командой указывается имя контроллера, которое отправляется удаленной стороне для прохождения CHAP-аутентификации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ppp chap hostname <NAME>
no ppp chap hostname
```

Параметры

<NAME> – имя контроллера, задаётся строкой до 31 символа.

Значение по умолчанию

Системное имя устройства (hosthame).

Необходимый уровень привилегий

15

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp chap hostname wlc-30_1
```

ppp chap password

Данной командой указывается пароль, который отправляется удаленной стороне вместе с именем контроллера для прохождения CHAP-аутентификации.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
ppp chap password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no ppp chap password
```

Параметры

<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F];

<ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов.

⚠ Пароль хранится в конфигурации в зашифрованной форме независимо от формата, использованного при вводе команды.

Необходимый уровень привилегий

15

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp chap password ascii-text 01234567
```

ppp chap refuse

Данной командой включается игнорирование аутентификации.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`[no] ppp chap refuse`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Игнорирование аутентификации выключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp chap refuse
```

ppp chap username

Данной командой указывается пользователь для аутентификации удаленной стороны и осуществляется переход в режим конфигурирования пользователя.

Использование отрицательной формы команды (no) удаляет указанного пользователя.

Синтаксис

```
[no] ppp chap username <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp chap username xap
```

ppp ipcp accept-address

Данной командой разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ppp ipcp accept-address
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Прием IP-адреса запрещен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp ipcp accept-address
```

ppp ipcp remote-address

Данной командой устанавливается IP-адрес, который отправляется удаленной стороне для последующего его присвоения.

Использование отрицательной формы команды (no) удаляет IP-адрес удаленной стороны.

Синтаксис

`ppp ipcp remote-address <ADDR>`

`no ppp ipcp remote-address`

Параметры

<ADDR> – IP-адрес удаленного шлюза.

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp ipcp remote-address 192.168.1.2
```

ppp max-configure

Данной командой устанавливается количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ppp max-configure <VALUE>`

`no ppp max-configure`

Параметры

<VALUE> – время в секундах, принимает значения [1..255].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)#i ppp max-configure 4
```

ppp max-failure

Данной командой устанавливается количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ppp max-failure <VALUE>`

`no ppp max-failure`

Параметры

<VALUE> – время в секундах, принимает значения [1..255].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-multilink)# ppp max-failure 4
```

ppp max-terminate

Данной командой устанавливается количество попыток выслать Terminate-Request пакеты, прежде чем сессия будет прервана.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ppp max-terminate <VALUE>
no ppp max-terminate
```

Параметры

<VALUE> – время в секундах, принимает значения [1..255].

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-multilink)# ppp max-terminate 4
```

ppp mru

Данной командой указывается размер MRU (Maximum Receive Unit) для интерфейса.

Использование отрицательной формы команды (no) устанавливает значение MRU по умолчанию.

Синтаксис

```
ppp mru <MRU>
no ppp mru
```

Параметры

<MRU> – значение MRU, принимает значения в диапазоне [552..1500].

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp mru 1400
```

ppp multilink

Данной командой включается режим MLPPP на E1-интерфейсе.

Использование отрицательной формы команды (no) отключает режим MLPPP.

Синтаксис

`[no] ppp multilink`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

Пример:

```
wlc-30(config-e1)# ppp multilink
```

ppp multilink-group

Данной командой E1-интерфейс включается в группу агрегации.

Использование отрицательной формы команды (no) исключает интерфейс из группы агрегации.

Синтаксис

`ppp multilink-group <GROUP-ID>`

Параметры

<GROUP-ID> – идентификатор группы, принимает значение [1..4].

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

Пример:

```
wlc-30(config-e1)# ppp multilink-group 1
```

ppp timeout keepalive

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер отправляет keepalive-сообщение.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ppp timeout keepalive [ <TIME >]`

`no ppp timeout keepalive`

Параметры

<TIME> – время в секундах, принимает значения [1..32767].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp timeout keepalive 200
```

ppp timeout retry

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер повторяет запрос на установление сессии.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ppp timeout retry <TIME>
no ppp timeout retry
```

Параметры

<TIME> – время в секундах, принимает значения [1..255].

Значение по умолчанию

3

Необходимый уровень привилегий

10

Командный режим

CONFIG-E1

CONFIG-MULTILINK

Пример:

```
wlc-30(config-e1)# ppp timeout retry 3
```

show controllers e1

Данной командой выводится информация о E1-контролерах.

Синтаксис

```
show controllers e1 [<IF>]
```

Параметры

<IF> – имя физического интерфейса контроллера, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show controllers e1
Interface 'te1/0/1':
 SFP present:     Yes
 SFP Vendor name: NSC-COM
 SFP Vendor PN:   611.900
 Line code:       HDB3
 Clock source:    Internal
 Timeslot:        24
 Invert Data:     No
 Framing CRC4:    No
 Loopback:        --
 CRC algorithm:   FCS16
 E1 Link:         Down
 E1 Synced:       No
 E1 RX AIS:       No
 E1 RX RAI:       No
```

switchport e1 slot

Данной командой порт e1 привязывается к физическому интерфейсу. Использование отрицательной формы команды (no) переходит в стандартный режим.

Синтаксис

```
[no] switchport e1 slot <SLOT>
```

Параметры

<SLOT> – идентификатор слота, принимает значение в диапазоне [0..12].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 0
```

switchport e1 clock source

Данной командой определяется источник синхронизации e1-интерфейса.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport e1 clock source { internal | line }
no switchport e1 clock source
```

Параметры

internal – используется внутренний источник синхронизации;

line – в качестве источника синхронизации используется сигнал с линии.

Значение по умолчанию

internal

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 clock source line
```

switchport e1 crc

Данной командой определяется режим проверки целостности передаваемых данных.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport e1 crc { 16 | 32 }
no switchport e1 crc
```

Параметры

16 – используется 16-битный алгоритм проверки отсутствия ошибок (CRC);

32 – используется 32-битный алгоритм проверки отсутствия ошибок (CRC).

Значение по умолчанию

16

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 crc 16
```

switchport e1 framing

Данной командой включается проверка целостности по алгоритму CRC4.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport e1 framing { crc4 | no-crc4 }
no switchport e1 framing
```

Параметры

crc4 – включение проверки целостности по CRC4;

no-crc4 – выключение проверки целостности по CRC4.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 framing crc4
```

switchport e1 invert data

Данной командой включается реверсивная отправка данных.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] switchport e1 invert data
```

Параметры

Отсутствуют.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 invert data
```

switchport e1 linecode

Данной командой определяется алгоритм кодирования данных, осуществляемое для их передачи по физическому каналу.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport e1 linecode { ami | hdb3 }
```

Параметры

ami – использовать алгоритм ami;

hdb3 – использовать алгоритм hdb3.

Значение по умолчанию

hdb3

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 linecode ami
```

switchport e1 timeslots

Данной командой определяется количество используемых 64 Кбит/с каналов в потоке E1.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
switchport e1 timeslots < RANGE >
no switchport e1 timeslots
```

Параметры

< RANGE > – количество 64 Кбит/с каналов, принимает значение [1..31].

Значение по умолчанию

31

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 timeslots 16
```

switchport e1 unframed

Данной командой включается режим использования потока E1 как единого без разделения на каналы по 64 Кбит/с.

Использование отрицательной формы командой (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] switchport e1 unframed
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport e1 unframed
```

switchport mode e1

Данной командой физический порт переводится в режим работы с SFP e1 модулем.

Использование отрицательной формы команды (no) переводит порт в стандартный режим.

Синтаксис

```
[no] switchport mode e1
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример:

```
wlc-30(config-if-gi)# switchport mode e1
```

Беспроводные модемы

allowed-auth

Данной командой задается метод аутентификации пользователя в мобильной сети.

Использование отрицательной формы команды (no) устанавливает метод аутентификации по умолчанию.

Синтаксис

```
allowed-auth <TYPE>
no allowed-auth
```

Параметры

<TYPE> – метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP].

Значение по умолчанию

PAP

Необходимый уровень привилегий

15

Командный режим

CONFIG-CELLULAR-PROFILE

Пример:

```
wlc-30(config-cellular-profile)# allowed-auth MSCHAP
```

allowed-mode

Данной командой разрешается использование режима при работе USB-модема.

Использование отрицательной формы команды (no) удаляет разрешение на использование режима.

Синтаксис

```
[no] allowed-mode <MODE>
```

Параметры

<MODE> – допустимый режим работы USB-модема [2g, 3g, 4g]

Значение по умолчанию

Разрешены режимы, которые отображаются как "Allowed modes:" в выводе команды show cellular status modem <ID>.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# allowed-mode 4g
```

apn

Данной командой задается точка доступа мобильной сети.

Синтаксис

`apn <NAME>`

Параметры

<NAME> – точка доступа мобильной сети, задаётся строкой до 253 символов.

Значение по умолчанию

Не сконфигурирована.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-PROFILE

Пример:

```
wlc-30(config-cellular-profile)# apn internet
```

cellular modem

Данной командой создается USB-модем с определенным идентификатором и осуществляется переход в режим конфигурирования USB-модема.

Использование отрицательной формы команды (no) удаляет сконфигурированный USB-модем.

Синтаксис

`[no] cellular modem <ID>`

Параметры

<ID> – идентификатор USB-модема в системе [1..10].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# cellular modem 1
```

cellular profile

Данной командой создается профиль настроек для USB-модема с определенным идентификатором и осуществляется переход в режим конфигурирования профиля.

Использование отрицательной формы команды (no) удаляет сконфигурированный профиль настроек USB-модема.

Синтаксис

```
[no] cellular profile <ID>
```

Параметры

<ID> – идентификатор профиля настроек для USB-модема в системе [1..10].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример:

```
wlc-30(config)# cellular profile 1
```

device

Данной командой задается идентификатор USB-порта подключенного модема.

Использование отрицательной формы команды (no) удаляет установленный идентификатор.

Синтаксис

```
device <WORD>
no device
```

Параметры

<WORD> – идентификатор USB-порта подключенного модема [1..12].

Данный идентификатор должен совпадать с идентификатором в поле "USB port device" в выводе команды show cellular status modem.

Значение по умолчанию

Не указан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# device 1-1
```

enable

Данной командой активируется USB-модем.

Использование отрицательной формы команды (no) деактивирует USB-модем.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

USB-модем не активирован.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)#
```

ip-version

Данной командой ограничивается возможность использования семейств IP-адресов в мобильной сети.

Использование отрицательной формы команды (no) разрешает использование адресаций обоих семейств IPv4 и IPv6.

Синтаксис

```
ip-version { ipv4 | ipv6 }
no ip-version
```

Параметры

ipv4 – семейство IPv4;

ipv6 – семейство IPv6;

Значение по умолчанию

Разрешена адресация обоих семейств IPv4 и IPv6.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-PROFILE

Пример:

```
wlc-30(config-cellular-profile)# ip-version ipv4
```

mru

Данной командой задается размер максимального принимаемого пакета.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
mru { <MRU> }
no mru
```

Параметры

<MRU> – значение MRU, принимает значения в диапазоне [128..16383].

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# mru 1476
```

number

Данной командой устанавливается номер дозвона для подключения к мобильной сети.

Использование отрицательной формы команды (no) удаляет номер дозвона для подключения к мобильной сети.

Синтаксис

`number <WORD>`

`no number`

Параметры

<WORD> – номер дозвона для подключения к мобильной сети, задаётся строкой от 1 до 15 символов.

Значение по умолчанию

Номер не задан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-PROFILE

Пример:

```
wlc-30(config-cellular-profile)# number *99#
```

password

Команда для установки пароля пользователя мобильной сети в открытой или зашифрованной форме. Пароль пользователя хранится в конфигурации в зашифрованной форме. При конфигурировании можно задать пароль в открытой форме либо скопировать пароль в зашифрованной форме с другого устройства.

Использование отрицательной формы команды (no) удаляет пароль пользователя.

Синтаксис

```
password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no password
```

Параметры

<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1..64] символов, может включать символы [0-9a-fA-F];

<ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов.

⚠ Пароли хранятся в конфигурации в зашифрованной форме независимо от формата, использованного при вводе команды.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPP-USER

Пример:

```
wlc-30(config-ppp-user)# password ascii-text 01234567
```

pin

Данной командой задается код разблокировки SIM-карты.

Использование отрицательной формы команды (no) удаляет код разблокировки SIM-карты.

Синтаксис

```
pin <WORD>
no pin
```

Параметры

<WORD> – код разблокировки SIM-карты [4..8] символов. Возможно использование только цифр.

Значение по умолчанию

PIN не задан.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# pin 4856
```

preferred-mode

Данной командой задается предпочтительный режим работы USB-модема в мобильной сети.

Использование отрицательной формы команды (no) удаляет предпочтительный режим работы USB-модема в мобильной сети.

Синтаксис

```
preferred-mode { <MODE> }
no preferred-mode
```

Параметры

<MODE> – предпочтительный режим работы USB-модема [2g, 3g, 4g].

Значение по умолчанию

Определяется USB-модемом.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# preferred-mode 4g
```

profile

Данной командой на USB-модем назначается созданный профиль настроек для USB-модема.

Использование отрицательной формы команды (no) удаляет назначенный профиль настроек для USB-модема.

Синтаксис

```
profile <ID>
no profile
```

Параметры

<ID> – идентификатор профиля настроек для USB-модема в системе [1..10].

Значение по умолчанию

ID профиля настроек не задан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CELLULAR-MODEM

Пример:

```
wlc-30(config-cellular-modem)# profile 1
```

show cellular configuration modem

Данной командой отображается информация о сконфигурированных USB-модемах.

Синтаксис

```
show cellular configuration modem [ <ID> ]
```

Параметры

<ID> – идентификатор USB-модема в системе [1..10].

Без указания номера USB-модема выводится таблица с краткой информацией о всех сконфигурированных USB-модемах.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show cellular configuration modem
Number   State      Description                      USB port device   Profile
modem
------   --------   ------------------------------   ---------------   --------
1        Enabled    megafon                          1-1               1
2        Enabled    mts                              1-2               2

wlc-30# show cellular configuration modem 2
State:              Enabled
Description:        mts
USB port device:    1-2
Pin:                --
MRU:                --
MTU:                1500
Preferred mode:     none
Allowed modes:      all
Profile:            2
Description:           MTS
  User name:             mts
  Number:                *99#
  APN:                   internet.mts.ru
  Password (encrypted): 91A010
  IP version:            both
  Allowed auth:          EAP
Security zone:      --
```

show cellular configuration profile

Данной командой отображается информация о сконфигурированных профилях USB-модемов.

Синтаксис

```
show cellular configuration profile [ <ID> ]
```

Параметры

<ID> – идентификатор USB-модема в системе [1..10].

Без указания номера USB-модема выводится таблица с краткой информацией о всех сконфигурированных профилях USB-модемов.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример:

```
wlc-30# show cellular configuration profile
Number    User name          APN                Number             Description
profile
-------   ------------       ---------         -------             -------------
1         gdata              internet           *99#               MEGAFON
2         mts                internet.mts.ru    *99#               MTS

wlc-30# show cellular configuration profile 1
Description:          MEGAFON
User name:            gdata
Number:               *99#
APN:                  internet
Password (encrypted): 9BB00279B1
IP version:           both
Allowed auth:         EAP
```

show cellulas status modem

Данной командой отображается информация о статусе подключенных USB-модемов.

Синтаксис

`show cellular status modem [ <ID> ]`

Параметры

<ID> – идентификатор USB-модема в системе [1..10].

Без указания номера USB-модема выводится таблица с краткой информацией о всех обнаруженных USB-модемах.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример:

```
wlc-30# show cellular status modem
Number   USB port   Manufacturer   Model        Current state   Inteface          Link
device                                                                            state
------   --------   ------------   ----------   -------------   ---------------   -----
1        1-1        huawei         E3372        disabled        --                Down

wlc-30# show cellulars status modem 1
Interface 'modem 1' status information:
```

```
    USB port device:         1-1
    Manufacturer:            huawei
    Model:                   E3372
    Revision:                21.180.01.00.00
    IMEI:                    861821036192893
    Status SIM lock:         --
    Status unlock retries:   sim-pin (3) sim-pin2 (3) sim-puk (10) sim-puk2 (10)
    Current state:           disabled
    Access tech:             unknown
    Signal level:            0
    Support modes:
        allowed 2G; preferred none;
        allowed 3G; preferred none;
        allowed 4G; preferred none;
        allowed 2G 3G 4G; preferred none;
    Allowed modes:           2G 3G 4G
    Preferred modes:         none
    Type IP:                 IPv4
    Operator name:
    Registration:            unknown
```

user

Данной командой задается имя пользователя мобильной сети. После выполнения данной команды контроллер переходит в режим конфигурирования параметров пользователя.

Использование отрицательной формы команды (no) удаляет имя пользователя мобильной сети.

Синтаксис

`[no] user <NAME>`

Параметры

<NAME> – имя пользователя, задаётся строкой до от 1 до 31 символа.

Значение по умолчанию

Пользователь не создан.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CELLULAR-PROFILE

Пример:

```
wlc-30(config-cellular-profile)# user gdata
```

14 Конфигурирование и мониторинг туннелей

- auth-nocache
- authentication algorithm
- authentication method
- authentication required disable
- certificate
- clear ip nhrp
- clear tunnels counters
- clear tunnels softgre
- compression
- default-profile
- description
- dscp
- enable
- encryption algorithm
- history statistics
- ignore-default-route
- interface
- ip nhrp authentication
- ip nhrp enable
- ip nhrp holding-time
- ip nhrp ipsec
- ip nhrp map
- ip nhrp multicast
- ip nhrp nhs
- ip nhrp redirect
- ip nhrp shortcut
- ip tcp adjust-mss
- ipsec authentication method
- ipsec authentication pre-shared-key
- ipsec ike proposal
- ipsec proposal
- keepalive dhcp dependent-interface
- keepalive dhcp link-timeout
- keepalive dst-address
- keepalive enable
- keepalive retries
- keepalive timeout
- keepalive timeout ipsec
- key
- load-average
- local address
- local address xauth
- local checksum
- local cookie
- local interface
- local port
- local session-id
- mode
- mode
- mtu
- multipoint
- password
- peer lt
- port
- ppp failure-count

- ppp timeout keepalive
- protocol
- protocol
- remote address
- remote address
- remote address xauth
- remote checksum
- remote cookie
- remote port
- remote session-id
- route-metric
- route-nopull
- snmp init-trap
- show ip nhrp
- show tunnels configuration
- show tunnels counters
- show tunnels history
- show tunnels status
- show tunnels utilization
- ttl
- tunnel
- tunnel
- tunnel-source
- username
- username

auth-nocache

Данной командой отключается кэширование пароля пользователя OPENVPN-клиента.

Использование отрицательной формы команды (no) активирует кэширование пароля пользователя OPENVPN-клиента.

Синтаксис

```
[no] auth-nocache
```

Параметры

Отсутствуют.

Значение по умолчанию

Кэширование разрешено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config)# auth-nocache
```

authentication algorithm

Данной командой устанавливается алгоритм аутентификации, который используется для аутентификации при подключении к OPENVPN-серверу.

Использование отрицательной формы команды (no) удаляет алгоритм аутентификации.

Синтаксис

`authentication algorithm <ALGORITHM>`

`no authentication algorithm`

Параметры

<ALGORITHM> – алгоритм аутентификации, принимает значения: md4, rsa-md4, md5, rsa-md5, mdc2, rsa-mdc2, sha, sha1, rsa-sha, rsa-sha1, rsa-sha1-2, dsa, dsa-sha, dsa-sha1, dsa-sha1-old, ripemd160, rsa-ripemd160, ecdsa-with-sha1, sha-224, rsa-sha-224, sha-256, rsa-sha-256, sha-384, rsa-sha-384, sha-512, rsa-sha-512, whirlpool.

Значение по умолчанию

Не задан.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# authentication algorithm md5
```

authentication method

Данной командой определяется метод аутентификации, который будет использоваться при установлении удаленного подключения клиентами PPPoE, PPTP и L2TP.

Использование отрицательной формы команды (no) удаляет указанный метод аутентификации.

Синтаксис

`authentication method <METHOD>`

`no authentication method <METHOD>`

Параметры

<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap.

Значение по умолчанию

chap

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

Пример

```
wlc-30(config-pppoe)# authentication method mschap-v2
```

authentication required disable

Данной командой отключается обязательная аутентификация PPP на сервере PPTP и L2TP.

Использование отрицательной формы команды (no) включается аутентификация PPP на сервере PPTP и L2TP.

Синтаксис

```
[no] authentication required disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Не задан.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

Пример

```
wlc-30(config-pppoe)# authentication required disable
```

certificate

Данной командой указываются необходимые сертификаты для подключения к OPENVPN-серверу.

Использование отрицательной формы команды (no) удаляет название сертификата из конфигурации.

Синтаксис

```
certificate <CERTIFICATE-TYPE> <NAME>
no certificate <CERTIFICATE-TYPE>
```

Параметры

<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения:

- ca – сертификат центра сертификации;
- client-crt – сертификат клиента;
- client-key – клиентский ключ;
- crl – список отозванных сертификатов;
- dh – ключ Диффи-Хеллмана;
- ta – HMAC-ключ.

<NAME> – имя сертификата или ключа, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# certificate ca KEY
```

clear ip nhrp

Данная команда служит для очистки NHRP-записей с контроллера.

Синтаксис

```
clear ip nhrp [ { dynamic | static | incomplete | nhs} ] [ { nbma-address <ADDR> | tunnel gre <ID> | tunnel-address <ADDR> } ] [ vrf <VRF> ]
```

Параметры

<ID> – идентификатор туннеля;

<ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будут удалены NHRP-записи, указанные в данном VRF;

dynamic – очистить динамически приобретённую информацию;

incomplete – очистить незаполненные записи;

nbma-address – очистить записи, касающиеся определённого NBMA-адреса;

nhs – очистить записи, касающиеся определённого NHS;

static – очистить записи, заданные статически;

tunnel – очистить записи, касающиеся определённого туннеля;

tunnel-address – очистить записи, касающиеся определённого туннеля;

vrf – очистить записи, находящиесяся в определённом VRF.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip nhrp vrf vrf_test tunnel gre 9 static
```

clear tunnels counters

Данной командой осуществляется сброс счетчиков заданного туннеля или группы туннелей.

Синтаксис

```
clear tunnels counters [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire
pseudowire [ <ID> <NEIGBOR-ADDR> ] } ]
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Можно указать несколько туннелей перечислением через запятую «,» либо указать диапазон туннелей через дефис «-». Если не указывать индексы туннелей, то будут очищены счетчики всех туннелей заданной группы.

<ID> – идентификатор псевдопровода/динамического псевдопровода.

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear tunnels counters dypseudowire 2 192.0.2.10
```

clear tunnels softgre

Данная команда разрушает softgre-туннели/туннель.

Синтаксис

```
clear tunnels softgre [ remote-address <REMOTE-IP> ]
```

Параметры

<REMOTE-IP> – удаленный IP-адрес, с которого поднят softgre-туннель.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# clear tunnels softgre wlc-30#clear tunnels softgre remote-address10.10.42.10
```

compression

Данной командой включается механизм сжатия передаваемых данных между клиентами и сервером OPENVPN.

Использование отрицательной формы команды (no) отключает механизм сжатия передаваемых данных.

Синтаксис

```
[no] compression
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# compression
```

default-profile

Данная команда позволяет использовать конфигурацию данного SoftGRE-туннеля для автоматического создания туннелей с такими же mode и local address.

Использование отрицательной формы команды (no) запрещает использования конфигурации туннеля для автоматического создания туннелей.

Синтаксис

```
[no] default-profile
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SOFTGRE

Пример

```
wlc-30(config-softgre)# default-profile
```

description

Данная команда используется для изменения описания конфигурируемого туннеля.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4
CONFIG-SUBTUNNEL
CONFIG-GRE
CONFIG-L2TP
CONFIG-L2TPV3
CONFIG-VTI
CONFIG-LT
CONFIG-PPTP
CONFIG-PPPOE
CONFIG-OPENVPN

Пример

```
wlc-30(config-gre)# description "tunnel to branch"
```

dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке инкапсулирующего пакета.
Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
dscp <DSCP>
no dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

Наследуется от инкапсулируемого пакета.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

Пример

```
wlc-30(config-ip4ip4)# dscp 40
```

enable

Данной командой включается туннель.

Использование отрицательной формы команды (no) отключает туннель.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Туннель выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-L2TP

CONFIG-L2TPV3

CONFIG-VTI

CONFIG-LT

CONFIG-PPTP

CONFIG-PPPOE

CONFIG-OPENVPN

Пример

```
wlc-30(config-gre)# enable
```

encryption algorithm

Данной командой выбирается алгоритм шифрования, используемый при передачи данных.

Использование отрицательной формы команды (no) отключает шифрование.

Синтаксис

```
encryption algorithm <ALGORITHM>
no encryption algorithm
```

Параметры

<ALGORITHM> – идентификатор протокола шифрования, принимает значения: des, blowfish128, aes128, des-ede, aes192, 3des, desx, aes256.

Значение по умолчанию

Шифрование отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# encryption algorithm aes128
```

history statistics

Данной командой включается запись статистики использования текущего туннеля.

Использование отрицательной формы команды (no) отключает запись статистики использования текущего туннеля.

Синтаксис

```
[no] history statistics
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

CONFIG-SOFTGRE

CONFIG-SUBTUNNEL

CONFIG-IP4IP4

CONFIG-L2TPV3

CONFIG-LT

CONFIG-VTI

CONFIG-PPTP

CONFIG-PPPOE

CONFIG-OPENVPN

CONFIG-L2TP

Пример

```
wlc-30(config-ip4ip4)# history statistics
```

ignore-default-route

Данная команда включает режим, в котором маршрут по умолчанию, полученный от сервера, не устанавливается в таблицу маршрутизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ignore-default-route
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Маршрут по умолчанию, полученный от сервера, устанавливается в таблицу маршрутизации.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP

CONFIG-PPTP

CONFIG-PPPOE

Пример

```
wlc-30(config-pptp)# ignore-default-route
```

interface

Данной командой определяется интерфейс, через который будет устанавливаться PPPoE-соединение.

Использование отрицательной формы команды (no) удаляет указанный интерфейс.

Синтаксис

`interface <IF>`

`no interface`

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPPOE

Пример

```
wlc-30(config-pppoe)# interface gigabitethernet 1/0/5.100
```

ip nhrp authentication

Данная команда включает аутентификацию для протокола NHRP. У всех участников NHRP-процесса должен быть одинаковый пароль.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

`ip nhrp authentication { <WORD> | encrypted <ENCRYPTED-TEXT> }`

`[no] ip nhrp authentication`

Параметры

<WORD> – пароль в открытой форме, задается строкой [1..8] символов, может включать символы [0-9a-fA-F].

<ENCRYPTED-TEXT> – зашифрованный пароль, размером [1..8] байт, задаётся строкой [2..16] символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp authentication pass
```

ip nhrp enable

Данной командой включается работа протокола NHRP в туннеле контроллера.

Использование отрицательной формы команды (no) отключает работу протокола NHRP на контроллере.

Синтаксис

```
[no] ip nhrp enable
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp enable
```

ip nhrp holding-time

Данная команда служит для установки времени, в течении которого на NHRP-сервере будет существовать запись о клиенте. Также этой командой задаётся периодичность отправки клиентом запросов о регистрации на NHRP-сервер, она равна 1/3 NHRP holding time.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip nhrp holding-time <TIME>
[no] ip nhrp holding-time
```

Параметры

<TIME> – время в секундах, в течении которого на сервере будет существовать запись о данном клиенте, принимает значения [1..65535].

Значение по умолчанию

7200 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp holding-time
```

ip nhrp ipsec

Данной командой указывается использование ранее созданного IPsec-VPN на mGRE туннеле.

Использование отрицательной формы команды (no) отключает использование IPsec-VPN с mGRE туннелем.

Синтаксис

```
ip nhrp ipsec <WORD> { static | dynamic }
no ip nhrp ipsec <WORD> { static | dynamic }
```

Параметры

<WORD> – имя VPN, задаётся строкой до 31 символа;

static – статическое соединение, применяются для связи с NHRP-сервером, задаётся на клиенте, неограниченно по времени;

dynamic – динамически устанавливающееся соединение, конфигурируется для связи с NHRP-клиентом.

Необходимый уровень привилегий

15

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp ipsec VPN static
```

ip nhrp map

Данная команда задаёт соответствие «внутреннего» туннельного адреса с «внешним» NBMA-адресом.

Использование отрицательной формы команды (no) удаляет соответствие.

Синтаксис

```
[no] ip nhrp map <ADDR-IN> <ADDR-OUT>
```

Параметры

<ADDR-IN> – IP-адрес туннельного интерфейса задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<ADDR-OUT> – IP-адрес внешнего интерфейса задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp map 192.168.1.2 67.86.141.231
```

ip nhrp multicast

Данная команда определяет адресата мультикастного трафика.

Использование отрицательной формы команды (no) удаляет адресата.

Синтаксис

```
[no] ip nhrp multicast { dynamic | nhs | <ADDR> }
```

Параметры

dynamic — отправляет трафик на все пиры, с которыми установлено соединение;

nhs — отправляет на все статические сконфигурированные NHRP-сервера;

<ADDR> — отправляет на специфически сконфигурированный IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp multicast nhs
```

ip nhrp nhs

Данная команда служит для задания «логического (туннельного)» адреса NHRP-сервера.

Использование отрицательной формы команды (no) удаляет запись о сервере.

Синтаксис

`ip nhrp nhs <ADDR/LEN> [ no-registration ]`

`no ip nhrp nhs <ADDR/LEN>`

Параметры

<ADDR/LEN> – адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

no-registration — не регистрироваться на NHRP-сервере.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp nhs 192.168.1.2
```

ip nhrp redirect

Данной командой включается режим, в котором NHRP-сервер может отправлять сообщения NHRP Traffic Indication.

Использование отрицательной формы команды (no) отключает режим.

Синтаксис

`[no] ip nhrp redirect`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp redirect
```

ip nhrp shortcut

Данной командой включается режим, позволяющий использование кратчайших маршрутов для связи с другими клиентами.

Использование отрицательной формы команды (no) отключает режим.

Синтаксис

```
[no] ip nhrp shortcut
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# ip nhrp shortcut
```

ip tcp adjust-mss

Данной командой переопределяется значение поля MSS (Maximum segment size) во входящих TCP-пакетах.

Использование отрицательной формы команды (no) отключает корректировку значение поля MSS.

Синтаксис

```
ip tcp adjust-mss <MSS>
no ip tcp adjust-mss
```

Параметры

<MSS> – значение MSS, принимает значения в диапазоне [500..1460].

Значение по умолчанию

1460

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-L2TP

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-VTI

CONFIG-LT

Пример

```
wlc-30(config-gre)# ip tcp adjust-mss 1400
```

ipsec authentication method

Данной командой выбирается метод аутентификации по ключу для IKE-соединения. Аутентификация сообщений по ключу используется при установлении IKE-соединения, ключ задаётся командой «ipsec authentication pre-shared-key» (см. раздел ipsec authentication pre-shared-key).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ipsec authentication method pre-shared-key`

`no ipsec authentication method`

Параметры

pre-shared-key – метод аутентификации, использующий предварительно полученные ключи шифрования.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP

Пример

```
wlc-30(config-l2tp-server)# ipsec authentication method psk
```

ipsec authentication pre-shared-key

Данной командой устанавливается общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.

Использование отрицательной формы команды (no) удаляет установленный ключ.

Синтаксис

```
ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }|
hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }
```

```
no ipsec authentication pre-shared-key
```

Параметры

<TEXT> – строка [1..64] ASCII символов;

<HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...);

<ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;

<ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.

Значение по умолчанию

none

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP

Пример

```
wlc-30(config-l2tp-server)# ipsec authentication pre-shared-key ascii-text password
```

ipsec ike proposal

Данной командой для L2TP-клиента назначается шаблон, ограничивающий используемые методы аутентификации и шифрования протокола IKE.

Использование отрицательной формы команды (no) удаляет ограничения на использование методов аутентификации и шифрования протокола IKE.

Синтаксис

```
[no] ipsec ike proposal <NAME>
```

Параметры

<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP

Пример

```
wlc-30(config-l2tp)# ipsec ike proposal IKE_PROPOSAL
```

ipsec proposal

Данной командой для L2TP-клиента назначается шаблон, ограничивающий используемые методы аутентификации и шифрования протокола IPsec.

Использование отрицательной формы команды (no) удаляет ограничения на использование методов аутентификации и шифрования протокола IPsec.

Синтаксис

```
[no] ipsec ike proposal <NAME>
```

Параметры

<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP

Пример

```
wlc-30(config-l2tp)# ipsec  proposal IPSEC_PROPOSAL
```

keepalive dhcp dependent-interface

Данной командой включается механизм перезапроса IP-адресов по протоколу DHCP на указанных интерфейсах при отключении GRE-туннеля по keepalive. Возможно указать до 8-ми интерфейсов для каждого GRE-туннеля.

Использование отрицательной формы команды (no) отключает механизм перезапроса IP-адресов по протоколу DHCP.

Синтаксис

```
keepalive dhcp dependent-interface <IF>
```

```
no keepalive dst-address
```

Параметры

<IF> – физический или агрегированный интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive dhcp dependent-interface gi 1/0/1
```

keepalive dhcp link-timeout

Данной командой указывается интервал времени между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах указанных командой keepalive dhcp dependent-interface (см. раздел keepalive dhcp dependent-interface)

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
keepalive dhcp link-timeout <SEC>
```

```
no keepalive dhcp link-timeout
```

Параметры

<SEC> – интервал в секундах между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах указанных командой keepalive dhcp dependent-interface, принимает значения [1..32767] секунд.

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive dhcp link-timeout 90
```

keepalive dst-address

Данной командой настраивается IP-адрес для отправки keepalive пакетов для проверки работоспособности туннеля. Если указанный IP-адрес недоступен, то туннель меняет оперативное состояние на DOWN. Данный параметр имеет значение только при включенном механизме keepalive (см. раздел keepalive enable).

Использование отрицательной формы команды (no) отключает данную проверку.

Синтаксис

```
keepalive dst-address <ADDR>
no keepalive dst-address
```

Параметры

<ADDR> – IP-адрес для проверки работоспособности GRE-туннеля.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive dst-address 192.168.1.57
```

keepalive enable

Данной командой включается проверка доступности удаленного шлюза туннеля. Если удаленный шлюз туннеля недоступен, то туннель меняет оперативное состояние на DOWN.

Использование отрицательной формы команды (no) отключает данную проверку.

Синтаксис

```
[no] keepalive enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию.

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive enable
```

keepalive retries

Данная команда определяет количество попыток проверки доступности удаленного шлюза туннеля. По достижению указанного количества неудачных попыток, туннель будет считаться неактивным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
keepalive retries <VALUE>
no keepalive retries
```

Параметры

<VALUE> – количество попыток, принимает значения в диапазоне [1..255].

Значение по умолчанию

6

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive retries 8
```

keepalive timeout

Данной командой регулируется период отправки keepalive пакетов встречной стороне.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`keepalive timeout <TIME>`

`no keepalive timeout`

Параметры

<TIME> – время в секундах, принимает значения в диапазоне [1..32767].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive timeout 18
```

keepalive timeout ipsec

Данной командой задается время, которое отводится на восстановление соединения IPsec VPN, по истечении которого контроллер будет перезагружен. Данный функционал работает только когда контроллер работает в режиме OTT. Режим работы OTT включается при производстве устройства.

При использовании отрицательной формы команды (no) значение приводится к значению по умолчанию.

Синтаксис

```
keepalive timeout ipsec <TIME>
no keepalive timeout ipsec
```

Параметры

<TIME> – время в секундах, принимает значения в диапазоне [30-32767].

Значение по умолчанию

180

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# keepalive timeout ipsec 1000
```

key

Данная команда разрешает передачу ключа (Key) в туннельном заголовке GRE (в соответствии с RFC 2890) и устанавливает значение ключа. Ключ может быть использован для идентификации потоков трафика в GRE-туннеле.

Использование отрицательной формы команды (no) запрещает передачу ключа.

Синтаксис

```
key <KEY>
no key
```

Параметры

<KEY> – значение KEY, принимает значения в диапазоне [1..2000000].

Значение по умолчанию

Ключ не передаётся.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# key 40
```

load-average

Данной командой устанавливается интервал времени, за который усредняется статистика о нагрузке на туннеле.

Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

`load-average <TIME>`

`no load-average`

Параметры

<TIME> – интервал в секундах, принимает значения [5..150].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

CONFIG-SUBTUNNEL

CONFIG-L2TPv3

CONFIG-VTI

CONFIG-PPTP

CONFIG-PPPOE

CONFIG-OPENVPN

CONFIG-L2TP

Пример

```
wlc-30(config-gre)# load-average
```

local address

Данной командой устанавливается IP-адрес локального шлюза туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес локального шлюза.

Синтаксис

`local address <ADDR>`

`no local address`

Параметры

<ADDR> – IP-адрес локального шлюза.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-L2TPV3

CONFIG-VTI

Пример

```
wlc-30(config-ip4ip4)# local address 192.168.1.1
```

local address xauth

Данной командой задается использование адреса, выдаваемого по mode config, при использовании ранее настроенного IPsec VPN в режиме XAUTH-клиента.

При использовании отрицательной формы команды (no) удаляет настройку.

Синтаксис

`local address xauth <NAME>`

`no local address`

Параметры

<NAME> – имя ранее созданного IPsec VPN, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-)# local address xauth IPsecVPN
```

local checksum

Данная команда включает вычисление контрольной суммы и занесение её в GRE-заголовок отправляемых пакетов.

Использование отрицательной формы команды (no) отключает процесс вычисления и отправки контрольной суммы.

Синтаксис

```
[no] local checksum
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# local checksum
```

local cookie

Данная команда определяет значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией.

Использование отрицательной формы команды (no) удаляет локальный cookie.

Синтаксис

```
local cookie <COOKIE>
no local cookie
```

Параметры

<COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде [8 или 16].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# local cookie 8FB51B8FB
```

local interface

Данной командой устанавливается использование IP-адреса, назначенного на интерфейс в качестве локального шлюза GRE-туннеля.

При использовании отрицательной формы команды (no) прекращается использование IP-адреса, назначенного на интерфейс в качестве локального шлюза.

Синтаксис

```
local interface { <IF> | <TUN> }
no local interface
```

Параметры

<IF> – тип и идентификатор интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# local interface gigabitethernet 1/0/1
```

local port

Команда определяет локальный UDP-порт, если в качестве метода инкапсуляции был выбран UDP-протокол.

Использование отрицательной формы команды (no) удаляет локальный номер UDP-порта.

Синтаксис

`local port <UDP>`

`no local port`

Параметры

<UDP> – номер UDP-порта в диапазоне [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# local port 1501
```

local session-id

Установить локальный идентификатор сессии.

Использование отрицательной формы команды (no) удаляет локальный идентификатор сессии.

Синтаксис

`local session-id <SESSION-ID>`

`no local session-id`

Параметры

<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# local session-id 200
```

mode

Данной командой задается режим работы SoftGRE-туннеля.

Использование отрицательной формы команды (no) снимает установленный режим.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – режим работы туннеля, возможные значения:

- data – режим данных;
- management – режим управления.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SOFTGRE

Пример

```
wlc-30(config-softgre)# mode data
```

mode

Данной командой указывается режим инкапсуляции для GRE-туннеля.

Использование отрицательной формы команды (no) устанавливает инкапсуляцию по умолчанию.

Синтаксис

```
mode <MODE>
```

Параметры

<MODE> – режим инкапсуляции для GRE-туннеля:

- ip – инкапсуляция IP-пакетов в GRE;
- ethernet – инкапсуляция Ethernet-фреймов в GRE.

Значение по умолчанию

ip

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# mode ethernet
```

mtu

Данной командой указывается размер MTU (Maximum Transmition Unit) для туннелей.

Использование отрицательной формы команды (no) устанавливает значение MTU по умолчанию.

Синтаксис

`mtu <MTU>`

`no mtu`

Параметры

<MTU> – значение MTU, принимает значения в диапазоне [552..10000].

- Для PPPoE-туннелей, принимает значения в диапазоне [552..1500]

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-L2TP

CONFIG-L2TPV3

CONFIG-VTI

CONFIG-LT

CONFIG-PPTP

CONFIG-PPPOE

CONFIG-OPENVPN

Пример

```
wlc-30(config-l2tpv3)# mtu 1400
```

multipoint

Данная команда служит для перевода туннеля в режим multipoint. В этом режиме возможно установление нескольких соединений с одного туннельного интерфейса.

Использование отрицательной формы команды (no) переводит в обычный, point-to-point режим.

Синтаксис

```
[no] multipoint
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# multipoint
```

password

Команда для установки пароля пользователя OPENVPN-сервера.

Использование отрицательной формы команды (no) удаляет пароль пользователя.

Синтаксис

```
password { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no password
```

Параметры

<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8..32] символов, может включать символы [0-9a-fA-F];

<ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [8..32] символов.

Пароли хранятся в конфигурации в зашифрованной форме независимо от формата, использованного при вводе команды.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# password 01234567
```

peer lt

Данная команда используется для задания удаленной стороны (в другом VRF) логического туннеля.

Использование отрицательной формы команды (no) удаляет привязку удаленной стороны туннеля.

Синтаксис

```
[no] peer lt <ID>
```

Параметры

<ID> – идентификатор удаленной стороны логического туннеля.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LT

Пример

```
wlc-30(config-lt)# peer lt 2
```

port

Данной командой определяется номер UDP-порта, по которому устанавливается соединение с L2TP-сервером.

Использование отрицательной формы команды (no) удаляет указанный метод аутентификации.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер UDP-порта, задаётся в диапазоне [1024..65535].

Значение по умолчанию

1701

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP

Пример

```
wlc-30(config-l2tp)# port 1048
```

ppp failure-count

Данной командой устанавливается количество неудачных data-link тестов перед разрывом сессии.
При использовании отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ppp failure-count <NUM>
no ppp failure-count
```

Параметры

<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP
CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-l2tp)# ppp failure-count 20
```

ppp timeout keepalive

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер отправляет keepalive-сообщение.

При использовании отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`ppp timeout keepalive <TIME >`

`no ppp timeout keepalive`

Параметры

<TIME> – время в секундах, задается в диапазоне [1..32767].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TP

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-l2tp)# ppp timeout keepalive 5000
```

protocol

Выбор метода инкапсуляции для туннеля L2TPv3.

Синтаксис

`protocol <TYPE>`

`no protocol`

Параметры

<TYPE> – тип инкапсуляции, возможные значения:

- IP-инкапсуляция в IP-пакет;
- UDP-инкапсуляция в UDP-дейтаграммы.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# protocol ip
```

protocol

Выбор метода инкапсуляции для туннеля OPENVPN.

Синтаксис

```
protocol <TYPE>
no protocol
```

Параметры

<TYPE> – тип инкапсуляции, возможные значения:

- TCP – инкапсуляция в TCP-сегмент;
- UDP – инкапсуляция в UDP-дейтаграммы.

Значение по умолчанию

TCP

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# protocol tcp
```

remote address

Данной командой устанавливается IP-адрес удаленного шлюза туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес удаленного шлюза.

Синтаксис

```
remote address <ADDR>
no remote address
```

Параметры

<ADDR> – IP-адрес удаленного шлюза.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-SOFTGRE

CONFIG-L2TP

CONFIG-L2TPV3

CONFIG-VTI

CONFIG-PPTP

Пример

```
wlc-30(config-ip4ip4)# remote address 192.168.1.2
```

remote address

Данной командой устанавливается IP-адрес и TCP/UDP-порт удаленного шлюза туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес удаленного шлюза.

Синтаксис

```
[no] remote address <ADDR> [ port <PORT>]
```

Параметры

<ADDR> – IP-адрес удаленного шлюза;

<PORT> – номер TCP/UDP порта удаленного шлюза в диапазоне [1..65535].

Значение по умолчанию

<PORT> – 1194.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# remote address 192.168.1.2 port 1233
```

remote address xauth

Данной командой задается использование адреса management-ip или data-ip, выдаваемого по mode config, при использовании ранее настроенного IPsec VPN в режиме XAUTH-клиента. Требует наличия соответствующих настроек на IPsec-VPN-сервере.

При использовании отрицательной формы команды (no) удаляет настройку.

Синтаксис

```
remote address xauth <NAME> {management-ip|data-ip}
no remote address
```

Параметры

<NAME> – имя ранее созданного IPsec VPN, задаётся строкой до 31 символа;

management-ip – адрес, получаемый по mode config при установке IPsec VPN в режиме XAUTH-клиента. Требует наличия в настройках IPsec-VPN-сервера роутера ELTEX_MANAGEMENT_IP (28683).

data-ip – адрес, получаемый по mode config при установке IPsec VPN в режиме XAUTH-клиента. Требует наличия в настройках IPsec-VPN-сервера ELTEX_DATA_IP (28684).

Значение по умолчанию

Не задано.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# remote address xauth IPsecVPN
```

remote checksum

Команда включает проверку наличия и соответствия значений контрольной суммы в заголовках принимаемых GRE-пакетов.

Использование отрицательной формы команды (no) отключает проверку контрольной суммы.

Синтаксис

```
[no] remote checksum
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

По умолчанию проверка контрольной суммы выключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# remote checksum
```

remote cookie

Данная команда определяет значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией.

Использование отрицательной формы команды (no) удаляет удаленный cookie.

Синтаксис

```
remote cookie <COOKIE>
no remote cookie
```

Параметры

<COOKIE> – значение COOKIE, принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде [8 или 16].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# remote cookie 8FB51B8FB
```

remote port

Данная команд определяет удаленный UDP-порт, если в качестве метода инкапсуляции был выбран UDP.

Использование отрицательной формы команды (no) удаляет удаленный номер UDP-порта.

Синтаксис

```
remote port <UDP>
no remote port
```

Параметры

<UDP> – номер UDP порта в диапазоне [1..65535].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# remote port 65000
```

remote session-id

Данной командой устанавливается удаленный идентификатор сессии.

Использование отрицательной формы команды (no) удаляет удаленный идентификатор сессии.

Синтаксис

```
remote session-id <SESSION-ID>
no remote session-id
```

Параметры

<SESSION-ID> – идентификатор сессии, принимает значение в диапазоне [1..200000].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2TPV3

Пример

```
wlc-30(config-l2tpv3)# remote session-id 2
```

route-metric

Данной командой назначается метрика маршрутов получаемых клиентом от OPENVPN-сервера.
Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
route-metric <METRIC>
no route-metric
```

Параметры

<METRIC> – метрика маршрута, принимает значение в диапазоне [0..255].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config)# route-metric 100
```

route-nopull

Данной командой отключается применение маршрутов, передаваемых OPENVPN-сервером.
Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] route-nopull
```

Параметры

Отсутствуют.

Значение по умолчанию

Игнорирование маршрутов отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config)# route-nopull
```

snmp init-trap

Данная команда используется для включения отправки snmp-trap о включении/отключении туннеля.

Использование отрицательной формы команды (no) отключает отправку snmp-trap о включении/отключении туннеля.

Синтаксис

```
[no] snmp init-trap
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-GRE

CONFIG-SUBTUNNEL

Пример

```
wlc-30(config-gre)# snmp init-trap
```

show ip nhrp

Данная команда служит для просмотра NHRP-записей.

Синтаксис

```
show ip nhrp [ { dynamic | static | incomplete | nhs } ] [ { nbma-address <ADDR> | tunnel gre <ID> | tunnel-address <ADDR> } ] [ vrf <VRF> ]
```

Параметры

<ID> – идентификатор туннеля;

<ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<VRF> – имя экземпляра VRF, задается строкой от 1 до 31 символа. При указании данного параметра будут отображены NHRP-записи, указанные в данном VRF;

dynamic – показать информацию, приобретённую динамически;

incomplete – показать незаполненные записи;

nbma-address – показать записи с определённым NBMA-адресом;

nhs – показать записи определённого NHS;

static – показать записи, заданные статически;

tunnel – показать записи определённого туннеля;

tunnel-address – показать записи с определённым туннельным адресом;

vrf – показать записи, находящиеся в определённом VRF.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# hub-12# sh ip nhrp
Tunnel address   NBMA address   Interface   Peer type     Expire      Created     Flags
--------------   ------------   ---------   -----------   ---------   ---------   ---------
12.1.1.3         192.168.3.4      gre 1       dynamic      0:04:38     00:23:18    lower-up,
                                                                                      up

12.1.1.9         192.168.9.4      gre 1       dynamic      0:04:45     00:23:49    lower-up,
                                                                                      up

12.1.1.99        120.12.120.12    gre 1       dynamic      0:01:14     00:24:11    lower-up,
                                                                                      up
```

show tunnels configuration

Командой выполняется просмотр конфигурации туннеля.

Синтаксис

```
show tunnels configuration [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire pseudowire [ <ID> <NEIGBOR-ADDR> ] } ]
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<ID> – идентификатор псевдопровода/динамического псевдопровода;

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show tunnels configuration gre 25
State:                                              enabled
Description:
Local address:                                      14.0.0.2
Remote address:                                     14.0.0.1
Calculates checksums for outgoing GRE packets:      no
Requires that all input GRE packets were checksum: no
key:                                                -
TTL:                                                Inherit
DSCP:                                               0
MTU:                                                1500
Security zone:                                      remote
```

show tunnels counters

Командой выполняется просмотр счетчиков на туннелях.

Синтаксис

```
show tunnels counters [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire pseudowire [ <ID> <NEIGBOR-ADDR> ] } ]
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Можно указать несколько туннелей. Если не указывать индексы туннелей, то будут отображены счетчики всех туннелей заданной группы. Если задан определённый туннель, то будет отображена детальная информация по данному туннелей.

<ID> – идентификатор псевдопровода/динамического псевдопровода.

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show tunnels counters  dypseudowire 2 192.0.2.10
Tunnel 'dypseudowire 2_192.0.2.10' counters:
 Packets received:               1006
 Bytes received:                 84200
 Dropped on receive:             0
 Receive errors:                 0
 Multicasts received:            0
 Receive length errors:          0
 Receive buffer overflow errors: 0
 Receive CRC errors:             0
 Receive frame errors:           0
 Receive FIFO errors:            0
 Receive missed errors:          0
 Receive compressed:             0
 Packets transmitted:            1006
 Bytes transmitted:              102308
 Dropped on transmit:            0
 Transmit errors:                0
 Transmit aborted errors:        0
 Transmit carrier errors:        0
 Transmit FIFO errors:           0
 Transmit heartbeat errors:      0
 Transmit window errors:         0
 Transmit comressed:             0
 Collisions:                     0
```

show tunnels history

Команда используется для просмотра статистики использования туннеля.

Синтаксис

```
show tunnels history [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire
pseudowire [ <ID> <NEIGBOR-ADDR> ] } ] [ timer <TIMER}> ]
```

Параметры

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<ID> – идентификатор псевдопровода/динамического псевдопровода;

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<TIMER> – не обязательный ключ timer. В качестве параметров для данного ключа могут выступать:

- hours отображает историю за последние 72 часа;
- minutes отображает историю за последние 60 минут;
- seconds отображает историю за последние 60 секунд;
- При отсутствии ключа timer, выводятся 3 таблицы истории использования туннеля (туннелей).

Необходимый уровень привилегий

5

Командный режим

ROOT

Пример

```
wlc-30# show tunnel history gre 1 timer minutes
gre 1
Last 60 minutes:
Timer  Recv utilization, Kbps    Sent utilization, Kbps   Recv errors  Sent errors   Output
drops
------ -------                   ----------               ---------    -------       -------
0-1    240                       16                       0            0             0
1-2    961                       64                       0            0             0
2-3    962                       64                       0            0             0
3-4    962                       64                       0            0             0
4-5    960                       64                       0            0             0
5-6    961                       64                       0            0             0
6-7    719                       64                       0            0             0
7-8    960                       64                       0            0             0
8-9    800                       65                       0            0             0
9-10   962                       64                       0            0             0
10-11  865                       64                       0            0             0
11-12  962                       64                       0            0             0
12-13  817                       65                       0            0             0
13-14  962                       65                       0            0             0
14-15  961                       65                       0            0             0
15-16  880                       60                       0            0             0
16-17  960                       63                       0            0             0
17-18   0                        0                        0            0             0
18-19   0                        0                        0            0             0
19-20   0                        0                        0            0             0
20-21   0                        0                        0            0             0
21-22   0                        0                        0            0             0
```

show tunnels status

Команда используется для просмотра состояния системных интерфейсов.

Синтаксис

```
show tunnels status [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire
pseudowire [ <ID> <NEIGBOR-ADDR> ] } ]
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

В команде можно указать несколько туннелей. Если не указывать индексы туннелей, то будут отображены статусы всех туннелей заданной группы. Если задан конкретный туннель, то будет отображена детальная информация по данному туннелю.

<ID> – идентификатор псевдопровода/динамического псевдопровода.

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show tunnels status
Tunnel    Admin state    MTU      Local IP       Remote IP      Uptime
------     ----------    -----    ------------   -----------    ---------------
ip4ip4 4       Up        1500     115.0.0.100    115.0.0.30     1 minute and 4 seconds
```

show tunnels utilization

Команда используется для просмотра средней нагрузки в туннелях за указанный период.

Синтаксис

```
show tunnels utilization [{ <TUN> | pseudowire [ <ID> <NEIGBOR-ADDR> ] | dypseudowire
pseudowire [ <ID> <NEIGBOR-ADDR> ] } ]
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Можно указать несколько туннелей перечислением через «,» либо указать диапазон интерфейсов через «-». Если не указывать индексы туннелей, то будут очищены счетчики всех туннелей заданной группы.

<ID> – идентификатор псевдопровода/динамического псевдопровода.

<NEIGBOR-ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show tunnels utilization gre 2
Tunnel      Period, s     Sent,         Recv,        Frames Sent   Frames Recv
                          Kbit/s        Kbit/s
---------   -----------   -----------   -----------   -----------   -----------
gre 2       15            0             0             0             0
```

ttl

Команда задаёт значение времени жизни TTL для туннельных пакетов.

Использование отрицательной формы команды (no) устанавливает значение TTL по умолчанию.

Синтаксис

`ttl <TTL>`

`no ttl`

Параметры

<TTL> – значение TTL, принимает значения в диапазоне [1..255].

Значение по умолчанию

Наследуется от инкапсулируемого пакета.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IP4IP4

CONFIG-GRE

Пример

```
wlc-30(config-ip4ip4)# ttl 10
```

tunnel

Данная команда позволяет перейти в режим конфигурирования туннеля.

Использование отрицательной формы команды (no) удаляет туннель.

Синтаксис

```
[no] tunnel <TUN>
```

Параметры

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример 1

Переход в режим конфигурирования туннеля l2tp 10:

```
wlc-30(config)# tunnel l2tp 10
wlc-30(config-l2tp)#
```

Пример 2

Переход в режим конфигурирования туннеля l2tpv3 10:

```
wlc-30(config)# tunnel l2tpv3 10
wlc-30(config-l2tpv3)#
```

Пример 3

Переход в режим конфигурирования туннеля ip4ip4 200:

```
wlc-30(config)# tunnel ip4ip4 200
wlc-30(config-ip4ip4)#
```

Пример 4

Переход в режим конфигурирования туннеля gre 25:

```
wlc-30(config)# tunnel gre 25
wlc-30(config-gre)#
```

Пример 5

Переход в режим конфигурирования туннеля vti 125:

```
wlc-30(config)# tunnel vti 125
wlc-30(config-vti)#
```

Пример 6

Переход в режим конфигурирования туннеля pptp 10:

```
wlc-30(config)# tunnel pptp 10
wlc-30(config-pptp)#
```

Пример 7

Переход в режим конфигурирования туннеля pppoe 8:

```
wlc-30(config)# tunnel pppoe 8
wlc-30(config-pppoe)#
```

tunnel

Данной командой указывается режим инкапсуляции для OPENVPN-клиента.

Использование отрицательной формы команды (no) устанавливает инкапсуляцию по умолчанию.

Синтаксис

`tunnel <MODE>`

Параметры

<MODE> – режим инкапсуляции для OPENVPN-клиента:

- ip – инкапсуляция IP-пакетов в OPENVPN;
- ethernet – инкапсуляция Ethernet-фреймов в OPENVPN.

Значение по умолчанию

ip

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# mode ethernet
```

tunnel-source

Данной командой указывается имя VRF от IP-интерфейса которого будет строиться данный GRE-туннель. Данная команда актуальна в случае, если GRE-туннель строится через VRF отличный от VRF самого туннеля.

Использование отрицательной формы команды (no) устанавливает режим, когда GRE-туннель и IP-интерфейс, от которого строится GRE-туннель, находятся в одном VRF.

Синтаксис

```
tunnel-source [ vrf <VRF> ]
[no] tunnel-source
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Без указания ключа "vrf" и имени экземпляра VRF, будет использоваться IP-интерфейс глобальной конфигурации.

Значение по умолчанию

Отключено (GRE-туннель и IP-интерфейс относятся к одному VRF).

Необходимый уровень привилегий

10

Командный режим

CONFIG-GRE

Пример

```
wlc-30(config-gre)# tunnel-source vrf magistral
```

username

Данной командой задается пользователь и пароль для подключения к L2TP-, PPPoE- или PPTP-серверу.

Использование отрицательной формы команды (no) удаляет указанного пользователя.

Синтаксис

```
username <NAME> password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no username <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа;

<CLEAR-TEXT> – пароль, задаётся строкой [1 .. 64] символов;

<ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [2..128] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-pptp)# username fedor password ascii-text password
```

username

Данной командой создается пользователь для подключения к OPENVPN-серверу.

Использование отрицательной формы команды (no) удаляет указанного пользователя.

Синтаксис

```
username <NAME>
no username <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN

Пример

```
wlc-30(config-openvpn)# username fedor
```

15 Управление L2-функциями

- Управление L2-функциями
  - bridge
  - bridge-group
  - description
  - enable
  - mac-address
  - ports vrrp filtering
  - protected-ports
  - protected-ports exclude vlan
  - show interfaces bridge
  - thresholds wifi-tunnels-number high
  - thresholds wifi-tunnels-number low
  - unknown-unicast-forwarding disable
  - vlan
- Управление Spanning Tree
  - show spanning-tree
  - show spanning-tree active
  - show spanning-tree bpdu
  - spanning-tree
  - spanning-tree
  - spanning-tree bpdu
  - spanning-tree cost
  - spanning-tree disable
  - spanning-tree guard root
  - spanning-tree forward-time
  - spanning-tree hello-time
  - spanning-tree link-type
  - spanning-tree max-age
  - spanning-tree mode
  - spanning-tree pathcost method
  - spanning-tree portfast
  - spanning-tree port-priority
  - spanning-tree priority
- Настройка и мониторинг VLAN
  - force-up
  - name
  - show vlans
  - switchport default-vlan tagged
  - switchport forbidden default-vlan
  - switchport macs-group
  - switchport trunk allowed vlan
  - switchport trunk allowed vlan auto-all
  - switchport trunk native-vlan
  - vlan

Управление L2-функциями

bridge

Данной командой добавляется сетевой мост в систему и осуществляется переход в режим настройки его параметров.

Использование отрицательной формы команды (no) удаляет мост.

Синтаксис

```
[no] bridge <BRIDGE-ID>
```

Параметры

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

Переход в режим конфигурирования сетевого моста *bridge 10*:

```
wlc-30(config)# bridge 10
wlc-30(config-bridge)#
```

bridge-group

Данная команда используется для добавления в текущего сетевого интерфейса в L2-домен.

Использование отрицательной формы команды (no) удаляет интерфейс из L2-домена.

Синтаксис

```
bridge-group <BRIDGE-ID> [tagged]
no bridge-group
```

Параметры

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

tagged – ключ для направления тегированных кадров физического интерфейса в bridge.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-L2TPV3

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-OPENVPN

Пример

```
wlc-30(config-subif)# bridge-group 15
```

description

Данная команда используется для назначения описания конфигурируемому сетевому мосту.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

`description <DESCRIPTION>`

`no description`

Параметры

<DESCRIPTION> – описание сетевого моста, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# description "broadway"
```

enable

Данной командой разрешается работа сетевого моста. Без указания данной команды, сетевой мост не работает.

Использование отрицательной формы команды (no) выключает маршрутизацию данных.

Синтаксис

`[no] enable`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# enable
```

mac-address

Данная команда позволяет задать MAC-адрес сетевого моста, физического или агрегированного интерфейса, отличного от системного.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
mac-address <ADDR>
no mac-address
```

Параметры

<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Значение по умолчанию

Системный MAC-адрес.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# mac-address A8:F9:B0:00:00:04
```

ports vrrp filtering

Данной командой включается запрет на отправку VRRP-сообщений в интерфейсах, включенных в L2-домен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ports vrrp filtering {enable | exclude vlan}
```

Параметры

enable – включение запрета на отправку VRRP-сообщений в интерфейсах, включенных в L2-домен;

exclude vlan – при указании данного параметра VLAN исключается из списка фильтруемых.

Значение по умолчанию

Фильтрация VRRP-сообщений отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# ports vrrp filtering enable
```

protected-ports

Данной командой осуществляется управление режимом изоляции интерфейсов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
protected-ports <MODE>
```

Параметры

<MODE> – режим изоляции интерфейсов, принимает следующие значения:

- none – изоляция интерфейсов отключена. В данном режиме коммутация кадров между членами сетевого моста разрешена.
- local – изоляция интерфейсов включена. В данном режиме коммутация кадров между членами сетевого моста запрещена.
- radius – изоляция интерфейсов включена. Для использования данного режима требуется настройка Wi-Fi контроллера туннелей в режиме "radius". В данном режиме коммутация кадров между членами сетевого моста запрещена, за исключением SoftGRE DATA туннелей.
  Для SoftGRE DATA туннелей параметры изоляции запрашиваются у RADIUS-сервера.

Значение по умолчанию

none

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# protected-ports local
```

protected-ports exclude vlan

Данной командой VLAN, назначенный сетевому мосту, исключается из списка изолируемых на входящих в bridge интерфейсов. Данная опция актуальна при настройке режима protected-ports отличного от значения по умолчанию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] protected-ports exclude vlan
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# protected-ports exclude vlan
```

show interfaces bridge

Данная команда используется для просмотра информации о VLAN, интерфейсах, туннелях объединенных мостом.

Синтаксис

```
show interfaces bridge [<BRIDGE-ID>]
```

Параметры

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces bridge 1
Bridges      Interfaces
----------   ----------------------------------------
bridge 1     vlan 1,gi1/0/1.10
```

thresholds wifi-tunnels-number high

⚠ Данный функционал поддерживается только при наличии лицензии на Wi-Fi controller.

Данной командой устанавливается верхний порог аварии превышения числа включенных сабтуннелей softgre в bridge.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
thresholds wifi-tunnels-number high<NUM>
no thresholds wifi-tunnels-number high
```

Параметры

<NUM> – верхний порог аварии превышения числа включенных сабтуннелей softgre в bridge, принимает значение в диапазоне [1..1000].

Значение по умолчанию

950

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config)# thresholds wifi-tunnels-number high 200
```

thresholds wifi-tunnels-number low

⚠ Данный функционал поддерживается только при наличии лицензии на Wi-Fi controller.

Данной командой устанавливается нижний порог аварии превышения числа включенных сабтуннелей softgre в bridge.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
thresholds wifi-tunnels-number low <NUM>
no thresholds wifi-tunnels-number low
```

Параметры

<NUM> – нижний порог аварии превышения числа включенных сабтуннелей softgre в bridge, принимает значение в диапазоне [1..1000].

Значение по умолчанию

925

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config)# thresholds wifi-tunnels-number low 20
```

unknown-unicast-forwarding disable

Данной командой запрещается коммутация юникастового трафика с отсутствующими MAC-адресами в таблице MAC-адресов сетевого моста.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] unknown-unicast-forwarding disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Коммутация юникастового трафика с неизвестными MAC-адресами разрешена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# unknown-unicast-forwarding disable
```

vlan

Данная команда используется для связывания текущего сетевого моста с VLAN. Все порты, являющиеся членами назначаемого VLAN, автоматически включаются в сетевой мост и становятся участниками общего L2-домена. Для управления членством сетевых интерфейсов в VLAN используются команды, описанные в разделе Настройка и мониторинг VLAN.

Использование отрицательной формы команды (no) удаляет привязку VLAN и отключает соответствующие интерфейсы от сетевого моста.

Синтаксис

```
vlan <VID>
no vlan
```

Параметры

<VID> – идентификатор VLAN, задаётся в диапазоне [1..4095].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-vlan)# vlan 40
```

Управление Spanning Tree

show spanning-tree

Данная команда отображает подробную информацию о настройке протокола STP для выбранного интерфейса или устройства в целом.

Синтаксис

```
show spanning-tree { <IF> | tunnel <TUN> | bridge [<BRIDGE>] }
```

Параметры

<IF> – физический или агрегированный интерфейс или группа интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<BRIDGE> – номер сконфигурированного bridge;

bridge – команда для отображения общей информации об устройстве.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show spanning-tree gigabitethernet 1/0/10
Port gi1/0/10 disabled
State: BLK
Port id: ---
Type: ---
Designated bridge Priority: ---
Designated port id: ---
Role: ---
Port cost: ---
Designated path cost: ---
Address: ---
Port Fast: ---
wlc-30# show spanning-tree bridge
Protocol version: STP
     Root ID: [32768] 02:01:02:03:04:55
               Root port: [128] gigabitethernet 1/0/14
               Pathcost 4
               Message Age 1
               Hello time: 2 Max age time: 20 Forward delay: 15
   Bridge ID: [32768] 02:20:03:A0:04:90
               Hello time: 2 Max age time: 20 Forward delay: 15
               Transmit hold count: 6 Topology change: 0
               Time since topology change: 13736 Topology change count: 2 show
```

show spanning-tree active

Показывает информацию о настройке протокола STP, информацию об активных интерфейсах.

Синтаксис

`show spanning-tree active`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show spanning-tree active
Protocol version: RSTP
          Root ID: [32768] A8:F9:4B:83:52:C0
                    Root port: [128] gigabitethernet 1/0/20
                    Pathcost 20000
                    Message Age 1
                    Hello time: 2 Max age time: 20 Forward delay: 15
        Bridge ID: [32768] A8:F9:4B:AA:03:00
                    Hello time: 2 Max age time: 20 Forward delay: 15
                    Transmit hold count: 6 Topology change: 0
                    Time since topology change: 2318 Topology change count: 1
Name           State   Prio.Num   Cost        Status     Role       Type
------------   -----   --------   ---------   --------   --------   --------------
gi1/0/20       en      128.2318   20000       FRW        Root       RSTP
```

show spanning-tree bpdu

Данной командой выполняется просмотр режима обработки BPDU-пакетов интерфейсами контроллера.

Синтаксис

```
show spanning-tree bpdu
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show spanning-tree bpdu
Global: filtering
```

spanning-tree

Команда активирует протоколы семейства Spanning Tree (STP, RSTP) на физических интерфейсах контроллера в режиме switchport.

Использование отрицательной формы команды (no) выключает поддержку протоколов семейства Spanning Tree на физических интерфейсах контроллера в режиме switchport.

Синтаксис

```
[no] spanning-tree
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# spanning-tree
```

spanning-tree

Команда активирует протоколы семейства Spanning Tree (STP, RSTP) для широковещательного домена, организованного с помощью bridge.

Использование отрицательной формы команды (no) выключает поддержку протоколов семейства Spanning Tree для широковещательного домена, организованного с помощью bridge.

Синтаксис

```
[no] spanning-tree
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# spanning-tree
```

spanning-tree bpdu

Данной командой определяется режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree bpdu <MODE>
no spanning-tree bpdu
```

Параметры

<MODE> – режим работы:

- filtering – на интерфейсе с выключенным протоколом STP BPDU-пакеты фильтруются;
- flooding – на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные – фильтруются.

Значение по умолчанию

flooding

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-L2TPV3

CONFIG-OPENVPN

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree bpdu filtering
```

spanning-tree cost

Данной командой устанавливается размер, на который увеличивается поле cost при коммутации DPDU-пакета.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree cost <COST>
no spanning-tree cost
```

Параметры

<COST> – стоимость пути, устанавливается в диапазоне [1..20000000].

Значение по умолчанию

4

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-PORT-CHANNEL
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-GRE
CONFIG-SUBTUNNEL
CONFIG-L2TPV3
CONFIG-OPENVPN
CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree cost 115
```

spanning-tree disable

Данной командой запрещается работа протокола STP на конфигурируемом интерфейсе.
Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] spanning-tree disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

STP на интерфейсе включен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-PORT-CHANNEL
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-GRE
CONFIG-SUBTUNNEL
CONFIG-L2TPV3
CONFIG-OPENVPN
CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree disable
```

spanning-tree guard root

Данной командой включается блокировка получения BPDU с более высоким STP-приоритетом.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] spanning-tree guard root
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-L2TPV3

CONFIG-OPENVPN

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree guard root
```

spanning-tree forward-time

Данной командой устанавливается интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree forward-time <TIME>
no spanning-tree forward-time
```

Параметры

<TIME> – время в секундах, принимает значения [4..30].

Значение по умолчанию

15

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-BRIDGE

Пример

```
wlc-30(config)# spanning-tree forward-time 20
```

spanning-tree hello-time

Данной командой устанавливается интервал времени между отправкой BPDU-пакетов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree hello-time <TIME>
no spanning-tree hello-time
```

Параметры

<TIME> – время в секундах, принимает значения [1..10].

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-BRIDGE

Пример

```
wlc-30(config)# spanning-tree hello-time 20
```

spanning-tree link-type

Данной командой устанавливается протокол RSTP в передающее состояние и определяет тип связи для выбранного порта – «точка-точка», «разветвлённый».

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree link-type { point-to-point | shared }
no spanning-tree link-type
```

Параметры

point-to-point – команда определяет интерфейс как «точка-точка»;

shared – команда определяет интерфейс как «разветвленный».

Значение по умолчанию

point-to-point

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-L2TPV3

CONFIG-OPENVPN

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree link-type point-to-point
```

spanning-tree max-age

Данной командой устанавливается время жизни связующего дерева STP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree max-age <TIME>
no spanning-tree max-age
```

Параметры

<TIME> – время в секундах, принимает значения [6..40].

Значение по умолчанию

20

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-BRIDGE

Пример

```
wlc-30(config)# spanning-tree max-age 35
```

spanning-tree mode

Данной командой выбирается поддерживаемый протокол из семейства STP для широковещательного домена, организованного с помощью bridge или физических интерфейсов контроллера в режиме switchport.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree mode <MODE>
no spanning-tree mode
```

Параметры

<MODE> – протокол семейства STP:

- STP – IEEE 802.1D Spanning Tree Protocol;
- RSTP – IEEE 802.1W Rapid Spanning Tree Protocol.

Значение по умолчанию

RSTP

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-BRIDGE

Пример

```
wlc-30(config)# spanning-tree mode STP
```

spanning-tree pathcost method

Данной командой устанавливается метод определения ценности пути.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree pathcost method { short | long }
no spanning-tree pathcost method
```

Параметры

long – значение ценности в диапазоне [1..200000000];

short – значение ценности в диапазоне [1..65535].

Значение по умолчанию

short

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# spanning-tree pathcost method short
```

spanning-tree portfast

Данной командой включается режим, в котором L2-интерфейс при поднятии на нем линка сразу переходит в состояние передачи, не дожидаясь истечения таймера.

Использование отрицательной формы команды (no) выключает режим моментального перехода в состояние передачи по поднятию линка.

Синтаксис

```
[no] spanning-tree portfast
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

CONFIG-SUBIF

CONFIG-QINQ-IF
CONFIG-GRE
CONFIG-SUBTUNNEL
CONFIG-L2TPV3
CONFIG-OPENVPN
CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree portfast
```

spanning-tree port-priority

Данной командой устанавливается приоритет интерфейса в связующем дереве STP.
Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree port-priority <PRIORITY>
no spanning-tree port-priority
```

Параметры

<PRIORITY> – приоритет, указывается в диапазоне с шагом 16 [0..240].

Значение по умолчанию

128

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-PORT-CHANNEL
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-GRE
CONFIG-SUBTUNNEL
CONFIG-L2TPV3
CONFIG-OPENVPN
CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-if-gi)# spanning-tree port-priority 160
```

spanning-tree priority

Данной командой настраивается приоритет связующего дерева STP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
spanning-tree priority <PRIORITY>
no spanning-tree priority
```

Параметры

<PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440].

Значение по умолчанию

32768

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-BRIDGE

Пример

```
wlc-30(config)# spanning-tree priority 4096
```

Настройка и мониторинг VLAN

force-up

Данная команда используется для включения режима активности VLAN вне зависимости от состояния интерфейсов, на которых разрешена обработка фреймов данного VLAN.

Использование отрицательной формы команды (no) отменяет режим активности VLAN.

Синтаксис

```
[no] force-up
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-VLAN

Пример

```
wlc-30(config-vlan)# force-up
```

name

Данная команда используется для добавления описания VLAN.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
name <NAME>
no name
```

Параметры

<NAME> – описание VLAN, задаётся строкой до 255 символов.

Значение по умолчанию

Описание не задано.

Необходимый уровень привилегий

10

Командный режим

CONFIG-VLAN

Пример

```
wlc-30(config)# name L2-ACCESS
```

show vlans

Данная команда используется для просмотра информации об определенной VLAN.

Синтаксис

```
show vlans [<VID>]
```

Параметры

<VID> – идентификационный номер VLAN, диапазон допустимых значений [1 .. 4094].

Можно указать несколько VLAN перечислением через запятую «,» либо указать диапазон VLAN через дефис «-». При выполнении команды без параметра будут показаны все созданные VLAN.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show vlans
VID    Name                   Tagged                 Untagged
----   --------------------   --------------------   ----------------------
1      default                                       gi1/0/3-4, gi1/0/6-24,
                                                     po1
2      --                                            gi1/0/1, te1/0/1-2
```

switchport default-vlan tagged

Данная команда используется для изменения членства интерфейса во VLAN по умолчанию на тегированное.

Использование отрицательной формы команды (no) изменяет членство интерфейса во VLAN по умолчанию на нетегированное.

Синтаксис

```
[no] switchport default-vlan tagged
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# switchport default-vlan tagged
```

switchport forbidden default-vlan

Данная команда используется для удаления интерфейса из VLAN по умолчанию.

Использование отрицательной формы команды (no) разрешает добавление vlan на порту.

Синтаксис

```
[no] switchport forbidden default-vlan
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# no switchport forbidden default-vlan
```

switchport macs-group

Данной командой назначается профиль MAC-адресов и сопоставляется VLAN-ID, в который будут попадать пакеты с MAC-адресом источника, являющегося частью профиля MAC-адресов. Информация о конфигурировании профилей находится в разделе Управление профилями.

Использование отрицательной формы команды (no) удаляет сопоставление профиля MAC-адресов и VLAN-ID.

Синтаксис

```
switchport macs-group <NAME> vlan <VID>
```

```
no switchport macs-group <NAME>
```

Параметры

<NAME> – имя профиля MAC-адресов, задается строкой до 31 символа.

<VID> – идентификационный номер VLAN, задаётся в диапазоне [2..4094].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# switchport macs-group OGM1 vlan 999
```

switchport trunk allowed vlan

Данная команда используется для включения/исключения интерфейса в/из VLAN в режиме работы trunk.

Синтаксис

```
switchport trunk allowed vlan <ACT> <VID>
```

Параметры

<ACT> – назначаемое действие:

- add – включение интерфейса во VLAN;
- remove – исключение интерфейса из VLAN.

<VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно задать диапазоном через «-» или перечислением через «,».

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# switchport trunk allowed vlan add 10-50
```

switchport trunk allowed vlan auto-all

Данная команда включает автоматическое добавление порта во все созданные на контроллере VLAN.

Использование отрицательной формы команды (no) отключает автоматическое добавление порта во все созданные на контроллере VLAN.

Синтаксис

```
[no] switchport trunk allowed vlan auto-all
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# switchport trunk allowed vlan auto-all
```

switchport trunk native-vlan

Данная команда используется для настройки VLAN по умолчанию для интерфейса в режиме работы trunk. Весь нетегированный трафик, поступающий на данный интерфейс, направляется в данную VLAN.

Синтаксис

```
switchport trunk native-vlan <VID>
no switchport trunk native-vlan
```

Параметры

<VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# switchport trunk native-vlan 55
```

vlan

Данной командой добавляется VLAN в систему и осуществляется переход в режим настройки параметров VLAN. На контроллере всегда существует VLAN с идентификатором 1, все интерфейсы по умолчанию включены в данный VLAN.

Использование отрицательной формы команды (no) удаляет VLAN.

Синтаксис

```
[no] vlan <VID>
```

Параметры

<VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# vlan 40
```

16 Работа с адресными таблицами

- clear arp-cache
- clear ipv6 neighbors
- clear mac address-table
- ip arp
- ip arp reachable-time
- ipv6 nd
- ipv6 nd reachable-time
- mac address-table aging-time
- show arp
- show arp configuration
- show ipv6 neighbors
- show ipv6 neighbors configuration
- show mac address-table

clear arp-cache

Команда используется для очистки содержимого ARP-таблицы.

Синтаксис

```
clear arp-cache [ <OPTIONS> ]
```

Параметры

<OPTIONS> – параметры команды для детализации запрашиваемой информации, опциональный параметр:

- vrf <VRF> – имя экземпляра VRF, задается строкой до 31 символа. Опциональный параметр, при указании которого будет очищена ARP-таблица в указанном VRF;
- <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;
- ip-address <ADDR> – IP-адрес, по которому ведется поиск, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- mac-address <ADDR> – MAC-адрес, по которому ведется поиск, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear arp-cache ip-address 10.0.0.8
```

clear ipv6 neighbors

Команда используется для очистки содержимого IPv6 Neighbor Discovery таблицы.

Синтаксис

```
clear ipv6 neighbors [<OPTIONS> ]
```

Параметры

<OPTIONS> – параметры команды для детализации запрашиваемой информации, опциональный параметр:

- vrf <VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будет очищена IPv6 Neighbor Discovery таблица в указанном VRF;
- <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;
- ipv6-address <IPV6-ADDR> – указывается IPv6-адрес, по которому ведется поиск, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
- mac-address <ADDR> – MAC-адрес, по которому ведется поиск, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ipv6 neighbors
```

clear mac address-table

Команда используется для удаления информации об изученных MAC-адресах.

Синтаксис

```
clear mac address-table [ { dynamic | static } ] [ { interface { <IF> | host-port <U/S/
P> } | bridge <BRIDGE-ID> | tunnel { gre | softgre } <ID> | vlan <VLAN-ID> }
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<U/S/P> – юнит (1), слот (0) и номер интерфейса пакетного процессора;

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<ID> – идентификатор туннеля;

<VLAN-ID> – номер vlan. Возможно задание списка vlan через символ "," без пробелов, диапазона vlan через символ "-" и/или комбинации списков и диапазонов.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear mac address-table
```

ip arp

Данной командой добавляется статическая запись в ARP-таблицу.

Использование отрицательной формы команды (no) удаляет статическую запись из ARP-таблицы.

Синтаксис

```
ip arp [ vrf <VRF> ] <IP> <MAC> { <IF> | <TUN> }
no ip arp [ vrf <VRF> ] <IP>
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<IP> – IP-адрес статической записи, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config-if-gi)# ip arp 192.168.54.22 a8:f9:4b:ab:2e:d0 bridge 3
```

ip arp reachable-time

Данной командой устанавливается время жизни записи в ARP-таблице.

Использование отрицательной формы команды (no) устанавливает значение параметра arp reachable-time по умолчанию.

Синтаксис

```
ip arp reachable-time <TIME>
no ip arp reachable-time
```

Параметры

< TIME > – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*< TIME >.

Необходимый уровень привилегий

10

Значение по умолчанию

160000

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-LOOPBACK

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip arp reachable-time 6000
```

ipv6 nd

Данной командой добавляется статическая запись в ND-таблицу.

Использование отрицательной формы команды (no) удаляет статическую запись из ND-таблицы.

Синтаксис

```
ipv6 nd [ vrf <VRF> ] <IPV6> <MAC> {<IF> | <TUN>}
no ipv6 nd [ vrf <VRF> ] <IP>
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<IPV6-ADDR> – указывается IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config-if-gi)# ip arp 192.168.54.22 a8:f9:4b:ab:2e:d0 bridge 3
```

ipv6 nd reachable-time

Данной командой устанавливается время, в течение которого удаленный узел IPv6 считается доступным при отсутствии активности узла.

Использование отрицательной формы команды (no) устанавливает значение параметра nd reachable-time по умолчанию.

Синтаксис

```
ipv6 nd reachable-time <TIME>
no ipv6 nd arp reachable-time
```

Параметры

<TIME> – время жизни записи об удаленном узле IPv6 в таблице ND протокола, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*< TIME >.

Значение по умолчанию

30000

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd reachable-time 27000
```

mac address-table aging-time

Командой устанавливается время жизни динамических MAC-адресов в forwarding-таблице.

Использование отрицательной формы команды (no) устанавливает значение «aging time» по умолчанию.

Синтаксис

```
mac address-table aging-time <AGING TIME>
[no] mac address-table aging time
```

Параметры

<AGING TIME> – время жизни динамических MAC-адресов, в секундах. Допустимые значения – от 20 до 630 секунд.

Значение по умолчанию

300

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# mac address-table aging-time 30
```

show arp

Команда используется для просмотра ARP-таблицы.

Синтаксис

```
show arp [<OPTIONS>]
```

Параметры

<options> – параметры команды для детализации запрашиваемой информации, опциональный параметр:

- vrf <VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будет отображена ARP-таблица в указанном VRF;
- <IF> – наименование системного интерфейса или списка интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера. Отображается только информация по указанным интерфейсам;
- <TUN> – наименования туннелей, задаются в виде, описанном в разделе Типы и порядок именования туннелей контроллера;
- mac-address <MAC> – MAC-адрес, по которому ведется поиск, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];
- ip-address <ADDR> – IP-адрес, по которому ведется поиск, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show arp
Interface         IP address        MAC address         State             Age(min)
---------------   ---------------   -----------------   ---------------   ----------
bridge 1          192.168.1.1       a8:f9:4b:aa:00:40   --                --
gi1/0/5           10.255.100.1      d8:50:e6:d2:f0:46   reachable         2
gi1/0/5           10.255.100.5      a8:f9:4b:aa:00:45   --                --
```

show arp configuration

Команда используется для просмотра значений времени жизни записей в ARP-таблице.

Синтаксис

```
show arp configuration <IF>
```

Параметры

<IF> – наименования системных интерфейсов, задаются в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh arp configuration gigabitethernet 1/0/1-5
Globally configured ARP reachable time is 6000 msec
Interface         ARP reachable time, msec
---------------   -------------------------
gi1/0/1           6000
gi1/0/2           6000
gi1/0/3           6000
gi1/0/4           6000
gi1/0/4           6000
```

show ipv6 neighbors

Команда используется для просмотра IPv6 Neighbor Discovery таблицы.

Синтаксис

```
show ipv6 neighbors [<OPTIONS>]
```

Параметры

<OPTIONS> – параметры команды для детализации запрашиваемой информации, опциональный параметр:

- vrf <VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будет отображена IPv6 Neighbor Discovery таблица в указанном VRF;
- <IF> – наименование системного интерфейса или списка интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера. Отображается только информация по указанным интерфейсам;
- mac-address <MAC> – указывается MAC-адрес, по которому ведется поиск, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];
- ipv6-address <IPV6-ADDR> – указывается IPv6-адрес, по которому ведется поиск, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 neighbors
Interface         IPv6 address                MAC address         State             Age(min)
---------------   -------------------------   -----------------   ---------------   ----------
gi1/0/5           fc00::1                     d8:50:e6:d2:f0:46   reachable         1
gi1/0/5           fc00::2                     a8:f9:4b:aa:00:45   --                --
bridge 1          fe80::aaf9:4bff:feaa:40     a8:f9:4b:aa:00:40   --                --
bridge 2          fe80::aaf9:4bff:feaa:40     a8:f9:4b:aa:00:40   --                --
gi1/0/5           fe80::aaf9:4bff:feaa:45     a8:f9:4b:aa:00:45   --                --
gi1/0/5           ff02::16                    33:33:00:00:00:16   norarp            --
gi1/0/5           ff02::fb                    33:33:00:00:00:fb   norarp            --
gi1/0/5           ff02::1:ff00:1              33:33:ff:00:00:01   norarp            --
gi1/0/5           ff02::1:ff00:2              33:33:ff:00:00:02   norarp            --
```

show ipv6 neighbors configuration

Команда используется для просмотра значений времени жизни записи об удаленном узле в таблице ND протокола.

Синтаксис

```
show ipv6 neighbors configuration <IF>
```

Параметры

<IF> – наименования системных интерфейсов, задаются в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh ipv6 neighbors configuration tengigabitethernet 1/0/1-2
Globally configured NDP reachable time is 30000 msec
Interface         ND reachable time, msec
---------------   -------------------------
te1/0/1           30000
te1/0/2           30000
```

show mac address-table

Команда используется для просмотра информации, находящейся в таблице MAC-адресов.

Синтаксис

```
show mac address-table [ { count { bridge <BRIDGE-ID> | l2vpn p2p <P2P-NAME> } | { static
| dynamic} { bridge <BRIDGE-ID> | l2vpn p2p <P2P-NAME> | interface { <IF> | host-port <U/
S/P> } | tunnel { gre | softgre } <ID> | vlan <VLAN-ID> | mac <MAC-ADDR> <MAC-MASK> } } ]
```

Параметры

- count – просмотр количества записей в таблице MAC-адресов. Список MAC-адресов не отображается;
- static – просмотр записей в таблице MAC-адресов внесенных из конфигурации контроллера;
- dynamic – просмотр записей в таблице MAC-адресов внесенных в процессе изучения MAC-адресов;
- <BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;
- <P2P-NAME> – имя существующего p2p сервиса, задается строкой до 31 символа;
- <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;
- <HOST-U/S/P> – интерфейс пакетного процессора. Указывается в виде Юнит (1), слот (0) и номер интерфейса пакетного процессора;
- <ID> – идентификатор туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;
- <VLAN-ID> – номер vlan. Возможно задание списка vlan через символ "," без пробелов, диапазона vlan через символ "-" и/или комбинации списков и диапазонов;
- <MAC-ADDR> – MAC-адрес, по которому ведется поиск, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];
- [MAC-MASK] – маска MAC-адреса, опциональный параметр, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске. Значение маски по умолчанию FF:FF:FF:FF:FF:FF.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show mac address-table
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
102     a8:f9:4b:aa:44:bb    host-port 1/0/2                 Dynamic
101     a8:f9:4b:aa:44:bb    host-port 1/0/2                 Dynamic
100     a8:f9:4b:aa:44:bb    host-port 1/0/2                 Dynamic
3 valid mac entries
```

17 Настройка VRF

- description
- ip source-vrf
- ip vrf
- ip vrf forwarding
- show ip vrf

description

Данная команда используется для назначения описания конфигурируемому экземпляру VRF.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание экземпляра VRF, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-VRF

Пример

```
wlc-30(config-vrf)# description "VRF1"
```

ip source-vrf

Данной командой осуществляется перевод системы копирования по TFTP, SCP, FTP, SFTP в VRF.

Использование отрицательной формы команды (no) системы копирования в стандартный режим.

Синтаксис

```
ip { tftp | ftp | ssh | sftp | http } source-vrf <VRF>
no ip { tftp | ftp | ssh | sftp | http } source-vrf
```

Параметры

<VRF> – имя VRF, задается строкой до 31 символа;

tftp – копирование по протоколу TFTP;

ftp – копирование по протоколу FTP;

ssh – копирование по протоколу SCP;

sftp – копирование по протоколу SFTP;

http – копирование по протоколу HTTP.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip tftp source-vrf vrf1
```

ip vrf

Данной командой в системе создается экземпляр VRF и осуществляется переход в режим настройки параметров экземпляра VRF.

Использование отрицательной формы команды (no) удаляет экземпляр VRF из системы.

Синтаксис

```
[no] ip vrf <VRF>
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip vrf VRF1
wlc-30(config-vrf)#
```

ip vrf forwarding

Данной командой задаётся имя экземпляра VRF, в котором будут использоваться указанные сетевой интерфейс, мост, зона безопасности, сервер динамической авторизации (DAS) или группа правил NAT.

Использование отрицательной формы команды (no) удаляет привязку сетевого интерфейса, моста, зоны безопасности или группы правил NAT к экземпляру VRF.

Синтаксис

```
ip vrf forwarding <VRF>
no ip vrf forwarding
```

Параметры

<VRF> – имя VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-CELLULAR-MODEM
CONFIG-BRIDGE
CONFIG-LOOPBACK
CONFIG-GRE
CONFIG-LT
CONFIG-SUBTUNNEL
CONFIG-ZONE
CONFIG-DNAT-RULESET
CONFIG-SNAT-RULESET
CONFIG-DAS-SERVER
CONFIG-SNMP-USER
CONFIG-SNMP-VIEW
CONFIG-L2TP
CONFIG-PPPOE
CONFIG-PPTP
CONFIG-OPENVPN
CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-snat-ruleset)# ip vrf forwarding VRF1
```

show ip vrf

Команда используется для просмотра информации о существующих в системе экземплярах VRF.

Синтаксис

show ip vrf [<VRF>]

Параметры

<VRF> – имя VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip vrf
Name                              Interfaces
--------------------------------  ------------------------------------------
VRF1                              gi1/0/8
VRF2                              gi1/0/10.22
test                              gi1/0/2
```

18 Настройка IP-адресации

- ip address
- ip redirects
- ip route source-route
- ip unnumbered
- ip unreachables
- show ip interfaces

ip address

Данной командой создаётся IP-интерфейс и добавляются IP-адрес и маска подсети для конфигурируемого интерфейса (физического интерфейса, группы агрегации каналов, туннеля или сетевого моста).

Использование отрицательной формы команды (no) удаляет IP-адрес с интерфейса. При удалении последнего адреса IP-интерфейс уничтожается.

> ⚠ При создании IP-интерфейса система резервирует наибольший незанятый VLAN ID, который будет использоваться внутри системы. Для каждого IP-интерфейса на Ethernet-порту резервируется VLAN. Если VLAN уже был зарезервирован для IPv6-интерфейса, то для IP-интерфейса VLAN резервироваться не будет.
> Можно зарезервировать VLAN ID для внутреннего использования явно с помощью команды ip internal-usage vlan <VLAN_ID>.

Синтаксис

```
ip address <ADDR/LEN>
no ip address { <ADDR/LEN> | all }
```

Параметры

<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов (включая IPv6-адреса) на интерфейс. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IP-адреса;

all – команда удаляет все IP-адреса на интерфейсе.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-E1

CONFIG-MULTILINK

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip address 192.168.25.25/24
```

ip redirects

Данной командой включается механизм отправки ICMP сообщений о существовании более приоритетного контроллера в данной IP-сети для конкретного IP-назначения.

Использование отрицательной формы команды (no) отключает механизм отправки ICMP-сообщений о существовании более приоритетного контроллера в данной IP-сети для конкретного IP-назначения.

Синтаксис

```
[no] ip redirects
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Значение по умолчанию

Отправки ICMP-сообщений о существовании более приоритетного контроллера в данной IP-сети для конкретного IP-назначения включена.

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-MULTILINK

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# no ip redirects
```

ip route source-route

Данной командой на контроллере включается поддержка опции ip source-route.

Использование отрицательной формы команды (no) поддержка опции ip source-route отключается.

Синтаксис

```
[no] ip route source-route
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip route source-route
```

ip unnumbered

Данной командой включается режим работы интерфейса с использованием ip-адреса назначенного на другой интерфейс.

Использование отрицательной формы команды (no) отключает режим ip unnumbered.

Синтаксис

```
ip unnumbered { <IF> | <TUN> }
no ip unnumbere
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – наименования туннелей, задаются в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-MULTILINK

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config-e1)# ip unnumbered gigabitethernet 1/0/1
wlc-30(config-e1)#
```

ip unreachables

Данной командой включается отправка ICMP-пакетов о недоступности конечного адреса.

Использование отрицательной формы команды (no) отключает возможность отправки ICMP-пакетов о недоступности конечного адреса.

Синтаксис

```
[no] ip unreachables
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Значение по умолчанию

Отправка ICMP-пакетов о недоступности конечного адреса включена.

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-MULTILINK

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# no ip unreachables
```

show ip interfaces

Команда используется для просмотра информации о существующих в системе IP-интерфейсах.

Синтаксис

```
show ip interfaces [ { <IF> | <TUN> | vrf <VRF> [ ip-address <ADDR> ] } ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будут отображены IP-интерфейсы в указанном VRF;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть принимает значения [0..255]. При указании данного параметра будет отображен IP-интерфейс с указанным IP-адресом;

<IF> – наименования системных интерфейсов, задаются в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – наименования туннелей, задаются в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

В команде можно указать несколько системных интерфейсов. Если не указывать индексы интерфейсов, то будут отображены все IP-интерфейсы, относящиеся к системным интерфейсам указанного типа.

Если в команде указан определенный системный интерфейс, получающий IP-параметры по протоколу DHCP, то будут отображены настройки DHCP-клиента и состояние текущей аренды IP-параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip interfaces
IP address            Interface       Type
-------------------   -------------   -------
155.0.0.60/24         br10            static
16.0.0.2/24           gi1/0/16        DHCP
10.0.0.1/8            gi1/0/18        static
180.0.0.1/24          gi1/0/18        static
192.168.1.1/24        gi1/0/2         static
25.0.0.2/30           gre 25          static
10.1.0.2/24           ip4ip4 10       static
wlc-30# show ip interfaces gigabitethernet 1/0/16
IP address            Interface       Type
-------------------   -------------   -------
16.0.0.2/24           gi1/0/16        DHCP
 DHCP Client settings:
 DHCP Server:          N/A
 Lease time(dd:hh:mm): 00:02:00
 Reboot time:          10 seconds
 Retry time:           300 seconds
 Timeout:              60 seconds
 Select timeout:       0 seconds
 Vendor class ID:      N/A
 Ignore options:
    router

 Latest lease contents:
 Lease time(dd:hh:mm): 00:02:00
 DHCP message type:    DHCPACK
 Renew at:             Wednesday2015/02/25 12:22:24 2015/02/25 12:22:24
 Rebind at:            Wednesday2015/02/25 13:14:09 2015/02/25 13:14:09
 Expires at:           Wednesday2015/02/25 13:29:09 2015/02/25 13:29:09
```

19 Настройка IPv6-адресации

- ipv6 address
- ipv6 enable
- ipv6 nd managed-config-flag
- ipv6 nd ns-interval
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra hop-limit
- ipv6 nd ra lifetime
- ipv6 nd ra max-interval
- ipv6 nd ra min-interval
- ipv6 nd router-preference
- ipv6 redirects
- ipv6 route source-route
- ipv6 unreachables
- show ipv6 interfaces

ipv6 address

Данной командой создаётся IPv6-интерфейс и добавляется IPv6-адрес и маска подсети для конфигурируемого интерфейса: физического интерфейса, группы агрегации каналов, туннеля или сетевого моста.

Использование отрицательной формы команды (no) удаляет IPv6-адрес с интерфейса. При удалении последнего адреса IPv6-интерфейс уничтожается.

> ⚠ При создании IPv6-интерфейса система резервирует наибольший незанятый VLAN ID, который будет использоваться внутри системы. Для каждого IPv6-интерфейса на Ethernet-порту резервируется VLAN. Если VLAN уже был зарезервирован для IP-интерфейса, то для IPv6-интерфейса VLAN резервироваться не будет.
> Можно зарезервировать VLAN ID для внутреннего использования явно с помощью команды ip internal-usage vlan <VLAN_ID>.

Синтаксис

```
ipv6 address <IPV6-ADDR/LEN>
no ipv6 address {<IPV6-ADDR/LEN>|all}
```

Параметры

<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. Можно указать несколько IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv6-адресов (включая IP-адреса) на интерфейс. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IPv6-адреса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 address fc00::1/120
```

ipv6 enable

Данной командой включается поддержка IPv6 на интерфейсе.

Использование отрицательной формы команды (no) отключает поддержку IPv6 на интерфейсе.

Синтаксис

```
[no] ipv6 enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Поддержка IPv6 отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 enable
```

ipv6 nd managed-config-flag

Данной командой устанавливается managed-config-flag в SLAAC-сообщениях. Использование данного флага определяет получение всех IPv6-настроек от DHCPv6-сервера.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
[no] ipv6 nd managed-config-flag
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

Данной командой устанавливается интервал отправки IPv6-сообщений поиска соседа (neighbor solicitation) для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd ns-interval <TIME>
no ipv6 nd ns-interval
```

Параметры

<TIME> – интервал отправки, определяется в миллисекундах [1..172800000].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd ns-interval 2000
```

ipv6 nd other-config-flag

Данной командой устанавливается other-config-flag в SLAAC-сообщениях. Использование данного флага подразумевает предоставление IPv6-префикса по протоколу SLAAC, а остальных параметров по протоколу DHCPv6.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
[no] ipv6 nd other-config-flag
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd other-config-flag
```

ipv6 nd prefix

Данной командой устанавливается IPv6-префикс для рассылаемых SLAAC-сообщений для широковещательного домена.

Использование отрицательной формы команды (no).

Синтаксис

```
ipv6 nd prefix <IPV6-ADDR/LEN> <VLAID-TIME> <PREFER-TIME> [no-autoconfig] [no-onlink]
no ipv6 nd prefix
```

Параметры

<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];

<VLAID-TIME> – допустимое время жизни анонса, определяется в секундах [1..2147483647];

<PREFER-TIME> – предпочтительное время жизни анонса, определяется в секундах [1..2147483647];

[no-autoconfig] – не использовать Neighbor Discovery для установки всех действительных префиксов на канале из объявлений контроллера (RA), полученных на интерфейсе;

[no-onlink] – конфигурирует указанный префикс как не on-link. Префикс будет объявлен с установленным L-битом.

Значение по умолчанию

Префикс не установлен;

valid time – 0;

preffered time – 0;

no-onlink – не установлен;

no-autoconfig – не установлен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd prefix
```

ipv6 nd ra hop-limit

Данной командой устанавливается параметр hop-limit для рассылаемых SLAAC-сообщений для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd ra hop-limit <HOP-LIMIT>
no ipv6 nd ra hop-limit
```

Параметры

<HOP-LIMIT> – задается в диапазоне [0..255].

Значение по умолчанию

64

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd ra hop-limit 128
```

ipv6 nd ra lifetime

Данной командой устанавливается параметр lifetime для рассылаемых SLAAC-сообщений для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd ra lifetime <TIME>
no ipv6 nd ra lifetime
```

Параметры

<TIME> – время жизни рассылаемых объявлений контроллера, определяется в секундах [0..9000].

Значение по умолчанию

Не ограничено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd ra lifetime 120
```

ipv6 nd ra max-interval

Данной командой устанавливается максимальный интервал для рассылаемых SLAAC-сообщений для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd ra max-interval <TIME>
no ipv6 nd ra max-interval
```

Параметры

<TIME> – максимальный интервал рассылки SLAAC-сообщений, определяется в секундах [4..1800].

Значение по умолчанию

600

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd ra max-interval 1200
```

ipv6 nd ra min-interval

Данной командой устанавливается минимальный интервал для рассылаемых SLAAC-сообщений для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd ra min-interval <TIME>
no ipv6 nd ra min-interval
```

Параметры

<TIME> – минимальный интервал рассылки SLAAC-сообщений, определяется в секундах [3..1350].

Значение по умолчанию

200

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd ra min-interval 30
```

ipv6 nd router-preference

Данной командой устанавливается приоритетность контроллера в процессе выбора маршрута по умолчанию для широковещательного домена.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ipv6 nd router-preference <ACTION>
no ipv6 nd router-preference
```

Параметры

<ACTION> – принимает значения:

- low;
- medium;
- high.

Значение по умолчанию

medium

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-LOOPBACK

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 nd router-preference low
```

ipv6 redirects

Данной командой включается механизм отправки ICMP-сообщений о существовании более приоритетного контроллера в данной IPv6-сети для конкретного IPv6-назначения.

Использование отрицательной формы команды (no) отключает механизм отправки ICMP-сообщений о существовании более приоритетного контроллера в данной IPv6-сети для конкретного IPv6-назначения.

Синтаксис

```
[no] ipv6 redirects
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Значение по умолчанию

Отправки ICMP-сообщений о существовании более приоритетного контроллера в данной IP-сети для конкретного IP-назначения включена.

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# no ipv6 redirects
```

ipv6 route source-route

Данной командой на контроллере включается поддержка опции ipv6 source-route.

Использование отрицательной формы команды (no) поддержка опции ipv6 source-route отключается.

Синтаксис

```
[no] ipv6 route source-route
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 route source-route
```

ipv6 unreachables

Данной командой включается отправка IPv6 ICMP-пакетов о недоступности конечного адреса.

Использование отрицательной формы команды (no) отключает возможность отправки IPv6 ICMP-пакетов о недоступности конечного адреса.

Синтаксис

```
[no] ipv6 unreachables
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отправка IPv6 ICMP-пакетов о недоступности конечного адреса включена.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# no ipv6 unreachables
```

show ipv6 interfaces

Команда используется для просмотра информации о существующих в системе IPv6-интерфейсах.

Синтаксис

```
show ipv6 interfaces { { <IF> | <TUN> | ipv6-address <IPV6-ADDR> } | vrf <VRF> [ ipv6-address <IPV6-ADDR> ] }
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа. При указании данного параметра будут отображены IPv6-интерфейсы в указанном VRF;

<IF> – наименования системных интерфейсов, задаются в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – наименования туннелей, задаются в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. При указании данного параметра будут отображен IPv6-интерфейс с указанным IPv6-адресом.

В команде можно указать несколько системных интерфейсов. Если не указывать индексы интерфейсов, то будут отображены все IPv6-интерфейсы, относящиеся к системным интерфейсам указанного типа.

Если в команде указан определенный системный интерфейс, получающий IPv6 параметры по протоколу DHCP, то будут отображены настройки DHCP-клиента и состояние текущей аренды IPv6-параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 interfaces
IPv6 address                                          Interface       Type
----------------------------------------------------  -------------   -------
fc00::2/120                                           gi1/0/5         static
fe80::aaf9:4bff:feaa:45/64                            gi1/0/5         static
wlc-30# show ip interfaces gigabitethernet 1/0/16
IP address            Interface       Type
-------------------   -------------   -------
16.0.0.2/24           gi1/0/16        DHCP
 DHCP Client settings:
 DHCP Server:          N/A
 Lease time(dd:hh:mm): 00:02:00
 Reboot time:          10 seconds
 Retry time:           300 seconds
 Timeout:              60 seconds
 Select timeout:       0 seconds
 Vendor class ID:      N/A
 Ignore options:
    router
 Latest lease contents:
 Lease time(dd:hh:mm): 00:02:00
 DHCP message type:    DHCPACK
 Renew at:             Wednesday2015/02/25 12:22:24 2015/02/25 12:22:24
 Rebind at:            Wednesday2015/02/25 13:14:09 2015/02/25 13:14:09
 Expires at:           Wednesday2015/02/25 13:29:09 2015/02/25 13:29:09
```

20 Управление профилями

- address-port pair
- application
- category
- description
- email
- ip address-range
- ip prefix
- ipv6 address-range
- ipv6 prefix
- mac address
- object-group address-port
- object-group application
- object-group content-filter
- object-group email
- object-group mac
- object-group network
- object-group service
- object-group url
- port-range
- regexp
- show object-group
- url
- vendor

address-port pair

Команда используется для задания связки IP-адресов и TCP/UDP-порта.

Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
[no] address-port pair < ADRR >:< PORT >
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – номер порта, принимает значение [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-ADDRESS-PORT

Пример

```
wlc-30(config-object-group-address-port)# address-port pair 192.168.1.1:23
```

application

Данная команда используется для указания приложений, попадающих под действие данного профиля.

Использование отрицательной формы команды (no) удаляет приложение из текущего профиля.

Синтаксис

```
[no] application < APPLICATION >
```

Параметры

< APPLICATION > – указывает приложение, подпадающее под действие данного профиля, может принимать значения:

- afp – Apple Filing Protocol;
- amazon – Amazon Data Services;
- amqp – Advanced Message Queuing Protocol;
- apple – Apple Inc.;
- apple-icloud – Apple iCloud;
- apple-itunes – Apple iTunes;
- apple-push – Apple PUSH notifications;
- apple-store – Apple Store;
- applejuice – Applejuice P2P;
- ajp – Apache JServ Protocol;
- signal – Signal Protocol;
- ayiya – Anything In Anything;
- battlefield – Battlefield;
- bgp – Border Gateway Protocol;
- bittorrent – BitTorrent;
- bjnp – Canon BJNP protocol;
- cisco-skinny – Cisco Skinny;
- cisco-vpn – Cisco VPN;
- citrix – Citrix;
- cloudflare – Cloudflare Inc.;
- coap – Constrained Application Protocol;
- collectd – Collectd;
- corba – Common Object Request Broker Architecture;
- dce-rpc – Distributed Computing Environment / Remote Procedure Calls;
- deezer – Deezer (music streaming service).;
- dhcp – Dynamic Host Configuration Protocol;
- dhcpv6 – IPv6 Dynamic Host Configuration Protocol;
- directconnect – Direct Connect;
- dns – Domain Name System;
- dnscrypt – DNSCrypt;
- drda – Distributed Relational Database Architecture;
- dropbox – Dropbox;
- ebay – eBay;
- edonkey – eDonkey;
- egp – Exterior Gateway Protocol;
- facebook – Facebook;
- facebook-zero – Facebook Zero;
- fasttrack – FastTrack P2P;
- ftp-control – File Transfer Protocol (control connections);
- ftp-data – File Transfer Protocol (data connections);
- git – Git (version control system);
- github – GitHub, Inc.;

- gmail – Gmail;
- gnutella – Gnutella P2P;
- google – Google Inc.;
- google-maps – Google Maps;
- google-drive – Google Drive;
- google-docs – Google Docs;
- google-plus – Google Plus;
- google-services – Google Services;
- gre – Generic Routing Encapsulation;
- gtp – GPRS Tunneling Protocol;
- h323 – H323 Protocol;
- half-life2 – Half-Life 2;
- imo – IMO Messenger;
- hangout-duo – Google Hangout and Duo Messengers;
- hotmail – Hotmail;
- hotspotshield – Hotspot Shield;
- http – HTTP;
- http-connect – HTTP tunnel;
- http-download – HTTP download data;
- http-proxy – HTTP proxy;
- https – HTTPS;
- iax – IAX;
- icecast – Icecast;
- icmp – ICMP;
- icmpv6 – ICMP IPv6;
- iflix – iflix services;
- igmp – IGMP;
- imap – IMAP;
- imaps – IMAP over TLS/SSL;
- instagram – Instagram;
- ip-in-ip – IP in IP;
- ipp – Internet Printing Protocol;
- ipsec – IPsec;
- irc – Internet Relay Chat;
- kakaotalk – KakaoTalk;
- kaspersky-lab – Kaspersky Laboratory;
- kaspersky-update – Kaspersky Anti-Virus Update;
- kerberos – Kerberos;
- lastfm – LastFM;
- ldap – Lightweight Directory Access Protocol;
- llmnr – Link-local Multicast Name Resolution;
- linkedin – Linkedin;
- lotusnotes – Lotus Notes;
- mdns – Multicast DNS;
- messenger – Messenger;
- megaco – Megaco;
- mgcp – Media Gateway Control Protocol;
- microsoft – Microsoft services;
- mining – Mining protocols;
- mpeg-ts – MPEG-TS;
- mqtt – Message Queue Telemetry Transport;
- msn – MSN;
- ms-netlogon – Microsoft Netlogon;
- ms-onedrive – Microsoft OneDrive;
- ms-sms – Microsoft System Management Server;
- mssql-tds – Tabular Data Stream;
- mysql – MySQL;

- netbios – NetBIOS;
- netflix – Netflix;
- netflow – Netflow;
- nest-log-sink – Nest Log Sink Protocol;
- nfs – Network File System;
- noe – New Office Environment protocol;
- ntp – Network Time Protocol;
- office365 – Office365;
- ookla – Ookla services;
- opendns – OpenDNS;
- openft – OpenFT P2P;
- openvpn – OpenVPN;
- oracle – Oracle Database;
- oscar – OSCAR;
- ospf – Open Shortest Path First;
- pando-media-booster – Pando Media Booster;
- pandora – Pandora Radio;
- pcanywhere – PcAnywhere;
- playstore – Google Playstore;
- pop – Post Office Protocol;
- pops – Post Office Protocol over TLS/SSL;
- postgresql – PostgreSQL;
- pptp – Point-to-Point Tunneling Protocol;
- quic – QUIC;
- quicktime – QuickTime content in HTTP payload;
- radius – Remote Authentication in Dial-In User Service;
- rdp – Remote Desktop Protocol;
- redis – Remote dictionary server;
- rsync – Remote Synchronization;
- rtcp – Real-Time Transport Control Protocol;
- rtmp – Real Time Messaging Protocol;
- rtp – Real-time Transport Protocol;
- rtp-audio – Real-time Transport Protocol audio content;
- rtp-dynamic – Real-time Transport Protocol dynamic content;
- rtp-video – Real-time Transport Protocol video content;
- rtsp – Real time streaming protocol;
- sctp – Stream Control Transmission Protocol;
- sflow – sFlow;
- shoutcast – SHOUTcast;
- sip – Session Initiation Protocol;
- skype – Skype;
- smb – Server Message Block;
- smbv23 – Server Message Block Version 23;
- smpp – Short Message Peer-to-Peer;
- smtp – Simple Mail Transfer Protocol;
- smtps – Simple Mail Transfer Protocol over TLS/SSL;
- snmp – Simple Network Management Protocol;
- socks – SOCKS Protocol;
- soulseek – Soulseek P2P;
- soundcloud – Soundcloud;
- ssdp – Simple Service Discovery Protocol;
- ssh – Secured Shell;
- starcraft – StarCraft;
- stealthnet – StealthNet P2P;
- steam – Steam;
- stun – Session Traversal Utilities for NAT;
- syslog – System Logging Utility;category

- teamspeak – TeamSpeak;
- teamviewer – TeamViewer;
- telegram – Telegram;
- telnet – Teletype network;
- teredo – Teredo tunneling;
- tftp – Trivial File Transfer Protocol;
- tor – The Onion Router;
- tls – Transport Layer Security Protocol;
- twitch – Twitch;
- twitter – Twitter;
- unencrypted-jabber – Unencrypted Jabber;
- viber – Viber;
- vmware-vsphere – VMWare vSphere;
- vnc – Virtual Network Computing;
- vrrp – Virtual Router Redundancy Protocol;
- warcraft3 – Warcraft 3;
- wechat – WeChat;
- whatsapp – WhatsApp;
- whatsapp-call – WhatsApp call;
- whatsapp-files – WhatsApp file;
- whois-das – Whois/DAS;
- wikipedia – Wikipedia;
- windows-update – Windows update services;
- world-of-warcraft – World of Warcraft;
- xbox – Xbox services;
- xdmcp – X Display Manager control protocol);
- yahoo – Yahoo services;
- youtube – YouTube;
- zabbix – Zabbix;
- zeromq – ZeroMQ;
- zoom – Zoom call.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-APPLICATION

Пример

```
wlc-30(config-object-group-application)# application egp
```

category

Команда используется для задания категорий контентной фильтрации.

Использование отрицательной формы команды (no) удаляет заданную категорию.

Синтаксис

```
[no] category <CATEGORY>
```

Параметры

<CATEGORY> – имя категории. Принимает значения:

- 436-fz – контент, запрещенный Федеральным законом Российской Федерации № 436-ФЗ.
- abortions – контент, связанный с абортами.
- ads – тизерные сетевые сайты, рекламные сервисы, услуги контекстной рекламы, рекламные агентства.
- adult-dating – сайты знакомств для взрослых.
- adware – контент, связанный с программным обеспечением, которое загружает или отображает нежелательную рекламу, собирает маркетинговые данные.
- alcohol – продажа алкоголя, обсуждение, статьи по теме.
- animals – контент, связанный с домашними животными и животными. Статьи и дискуссии.
- anonymizers – веб-анонимайзеры и прокси-серверы.
- anorexia – контент, связанный с анорексией и пропагандой анорексии.
- banks – сайты банков.
- blogs – блоги и блог-хостинги.
- books – интернет-библиотеки, книжные магазины, книжные обзоры.
- business – веб-страницы коммерческих фирм, бизнес-ассоциаций, отраслевых групп и корпоративных сайтов в целом.
- casino – контент, связанный с казино и карточными играми.
- chats – веб-чаты, форумы, мгновенные сообщения.
- cryptocurrency – веб-страницы о криптовалюте и программном обеспечении для криптомайнинга.
- cultural-heritage – веб-страницы, содержащие информацию об изобразительном искусстве, исполнительском искусстве, культурном наследии и пропагандирующие их.
- dating – услуги знакомств. Не включает в себя услуги знакомств для взрослых.
- dyn-dns – ресурс предоставляет сервис динамического DNS.
- educational-institutions – сайты школ и университетов.
- electronics – веб-страницы с контентом, связанным с бытовой электроникой.
- email – веб-сервисы электронной почты.
- encyclopedias – образовательные порталы, базы знаний, энциклопедии.
- extremist-materials – содержание из Федерального списка экстремистских материалов Российской Федерации.
- family – содержание, связанное с домом и семьей. Сопутствующие магазины.
- fashion – контент, связанный с модой и стилем.
- file-sharing – сайты и сервисы для обмена файлами.
- finance – веб-страницы, содержащие информацию о финансах и национальной экономике.
- food – контент, связанный с пищей.
- games – контент, связанный с играми.
- government – правительственные сайты, политические партии, законы и юридические компании.
- health – контент, связанный со здоровьем, медициной, здоровым образом жизни, диетами, вегетарианцами.
- hosting – услуги хостинга и регистрации доменов, услуги whois, продавцы доменов.
- humour – юмористический контент.
- hunting – контент, связанный с охотой и рыбалкой.
- internet-services – сайты глобальных и локальных интернет-провайдеров.
- it-security – веб-страницы, содержащие информацию об ИТ-безопасности, включая веб-сайты, предоставляющие продукты и услуги безопасности для корпоративных и домашних пользователей.
- kids-internet – контент для детей.
- lgbt – контент для лесбиянок, геев, бисексуалов и трансгендеров (ЛГБТ).
- lingerie – контент, изображающий нижнее белье.
- magic – содержание, связанное с эзотерикой, астрологией, гороскопами, гаданием, хиромантией, уфологией, магией.
- malware – вредоносные ресурсы или URL-адреса загрузки вредоносного программного обеспечения.
- military – контент, связанный с вооружением или военной техникой.

- motor-vehicles – веб-страницы с контентом об автомобильном транспорте.
- music – контент, связанный с музыкой.
- narcotics – наркотики. Продажа, производство, обсуждение.
- news – новостные и медийные сайты.
- nudism – нудизм и эксгибиционизм, родственные сообщества.
- online-betting – сервисы онлайн-ставок. Ставки на скачки и спорт.
- online-lotteries – онлайн-лотереи.
- online-payments – услуги онлайн-платежей и онлайн-банкинга.
- pharmacy – контент, связанный с аптекой, легальными лекарствами, медицинскими добавками.
- phishing – фишинговые сайты.
- porno – порнографическое и эротическое содержание, нагота.
- profane-language – контент с ненормативной лексикой.
- racism – экстремистский и расистский контент.
- rat-node – ресурсы с программным обеспечением для удалённого администрирования.
- recruitment – сайты по подбору персонала, найму и трудоустройству.
- religion – содержание, связанное с религиозными объединениями, организациями, культами и сектами.
- rental-services – услуги по аренде недвижимости.
- riskware – контент, связанный с законными программами, которые могут нанести ущерб, если их используют злонамеренные пользователи.
- roskomnadzor – контент, занесенный в Черный список Роскомнадзора.
- searchers – поисковые системы и сервисы.
- self-damage - содержания направленное на самоповреждение.
- sex-education – содержание, связанное с половым воспитанием.
- sex-shops – секс-шопы и секс-игрушки.
- shops – интернет-магазины и аукционы.
- social-networks – социальные сети.
- spam – сайты, специально созданные для спам-целей и/или найденные в спам-письмах.
- sport – контент, связанный со спортом и бодибилдингом.
- streams – видео и аудио хостинг, загрузки, потоковое вещание.
- tobacco – продажа табака, обсуждение.
- tor – узлы Tor-сети.
- torrent – торрент-трекеры и форумы, включая спецификации протоколов и программное обеспечение.
- traveling – контент, связанный с путешествиями.
- tv-radio – контент, связанный с телевидением и радио.
- uncategorized – контент, который не отнесен ни к одной категории.
- violence – физическое или психологическое насилие, жестокое обращение с животными.
- weapons – содержание, относящееся к оружию, взрывчатым веществам и пиротехническим изделиям.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-CF-KASPERSKY

Пример

```
wlc-30(config-object-group-cf-kaspersky)# category books
```

description

Команда используется для изменения описания профиля.

Использование отрицательной формы команды (no) удаляет описание профиля.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-NETWORK

CONFIG-OBJECT-GROUP-SERVICE

CONFIG-OBJECT-GROUP-MAC

CONFIG-OBJECT-GROUP-APPLICATION

CONFIG-OBJECT-GROUP-URL

CONFIG-OBJECT-GROUP-ADDRESS-PORT

CONFIG-OBJECT-GROUP-CONTENT-FILTER

CONFIG-OBJECT-GROUP-MAIL

Пример

Установить описание для профиля IP-адресов:

```
wlc-30(config-object-group-network)# description "Internal addresses"
```

email

Команда используется для задания почтового домена или адреса почтового ящика.

Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
[no] email <NAME>
```

Параметры

<NAME> – почтовый домен или адреса почтового ящика, задаётся строкой от 1 до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-MAIL

Пример

```
wlc-30(config-object-group-email)# email eltex@eltex-co.ru
wlc-30(config-object-group-email)# email eltex-co.ru
```

ip address-range

Команда используется для задания диапазона IP-адресов.

Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
[no] ip address-range <FROM-ADDR>[-<TO-ADDR>]
```

Параметры

<FROM-ADDR> – начальный IP-адрес диапазона адресов;

<TO-ADDR> – конечный IP-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IP-адрес;

Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

Возможно указать до 6 отдельных IP-диапазонов в рамках одной группы адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-NETWORK

Пример

```
wlc-30(config-object-group-network)# ip address-range 192.168.1.1 192.168.1.25
```

ip prefix

Команда используется для задания подсети.

Использование отрицательной формы команды (no) удаляет заданную подсеть.

Синтаксис

```
[no] ip prefix <ADDR/LEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [8..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-NETWORK

Пример

```
wlc-30(config-object-group-network)# ip prefix 10.10.10.0/24
```

ipv6 address-range

Команда используется для задания диапазона IPv6-адресов. Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
[no] ipv6 address-range <FROM-ADDR>[-<TO-ADDR>]
```

Параметры

<FROM-ADDR> – начальный IPv6-адрес диапазона адресов.

<TO-ADDR> – конечный IPv6-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IPv6-адрес.

Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Возможно указать до 6 отдельных IP-диапазонов в рамках одной группы адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-NETWORK

Пример

```
wlc-30(config-object-group-network)# ipv6 address-range fc00::1:1-fc00:1::32
```

ipv6 prefix

Команда используется для задания IPv6-подсети.

Использование отрицательной формы команды (no) удаляет заданную подсеть.

Синтаксис

```
[no] ipv6 prefix <IPV6-ADDR/LEN>
```

Параметры

<IPV6-ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-NETWORK

Пример

```
wlc-30(config-object-group-network)# ipv6 prefix fc00::/126
```

mac address

Данная команда используется для задания диапазона MAC-адресов.

Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
[no] mac address <MAC-ADDR> <MAC-MASK>
```

Параметры

<MAC-ADDR> – MAC-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<MAC-MASK> – маска MAC-адреса, опциональный параметр, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске. Значение маски по умолчанию FF:FF:FF:FF:FF:FF.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-MAC

Пример

```
wlc-30(config-object-group-mac)# mac address a8:f9:4b:80:e7:00 FF:FF:FF:FF:FF:00
```

object-group address-port

Команда предназначена для создания профиля связок IP-адресов и TCP/UDP-портов. Профили используются при настройке сервисов, работающих с пулами IP-адресов и TCP/UDP-портами – NAT, Firewall.

Использование отрицательной формы команды (no) удаляет профиль IP-адресов.

Синтаксис

```
[no] object-group address-port <NAME>
```

Параметры

<NAME> – имя конфигурируемого профиля связок IP-адресов и TCP/UDP-портов., задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра "all" будут удалены все профили IP-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

Создание профиля IP-адресов с именем *remote* и переход в режим конфигурирования профиля:

```
wlc-30(config)# object-group address-port WEB
```

object-group application

Данная команда используется для создания профиля приложений. Данный профиль используется для фильтрации по приложениям (DPI).

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group application <NAME>
```

Параметры

<NAME> – имя профиля приложений, задается строкой до 31 символа. При удалении вместо имени возможно использовать ключ all. При использовании ключа "all" будут удалены все профили приложений.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group application OGA045
```

object-group content-filter

Данная команда используется для создания профиля категорий контентной фильтрации. Данный профиль используется в наборе пользовательских правил.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group content-filter <NAME>
```

Параметры

<NAME> – имя профиля контентной фильтрации, задается строкой до 31 символа. При удалении вместо имени возможно использовать ключ all. При использовании ключа "all" будут удалены все профили контентной фильтрации.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group content-filter OGC042
```

object-group email

Данная команда используется для создания профиля почтовых доменов и адресов почтовых ящиков. Данный профиль используется в правилах профиля сервиса «Антиспам».

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group email <NAME>
```

Параметры

<NAME> – имя профиля почтовых доменов и адресов почтовых ящиков, задается строкой до 31 символа. При удалении вместо имени возможно использовать ключ all. При использовании ключа "all" будут удалены все профили почтовых доменов и адресов почтовых ящиков.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group email chinese_spammers
```

object-group mac

Данная команда используется для создания профиля MAC-адресов. Данный профиль используется в MAC-based VLAN.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group mac <NAME>
```

Параметры

<NAME> – имя профиля MAC-адресов, задается строкой до 31 символа. При удалении вместо имени возможно использовать ключ all. При использовании ключа "all" будут удалены все профили MAC-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group mac OGM007
```

object-group network

Команда предназначена для создания профиля IP-адресов. Профили используются при настройке сервисов, работающих с пулами IP-адресов – например, NAT, Firewall, Remote-Access, также для создания списка префиксов.

Использование отрицательной формы команды (no) удаляет профиль IP-адресов.

Синтаксис

```
[no] object-group network <NAME>
```

Параметры

<NAME> – имя конфигурируемого профиля IP-адресов, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все профили IP-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

Создание профиля IP-адресов с именем *remote* и переход в режим конфигурирования профиля:

```
wlc-30(config)# object-group network remote
```

object-group service

Команда предназначена для создания профиля TCP/UDP-портов. Данный профиль используется в правилах сервисов NAT и Firewall.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group service <NAME>
```

Параметры

<NAME> – наименование профиля портов, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все профили TCP/UDP-портов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group service ssh
```

object-group url

Команда предназначена для создания профиля URL-ссылок.

Использование отрицательной формы команды (no) удаляет профиль.

Синтаксис

```
[no] object-group url <NAME>
```

Параметры

<NAME> – наименование профиля портов, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все профили URL-ссылок.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# object-group url vk
```

port-range

Командой задаётся диапазон TCP/UDP-портов, относящихся к профилю.

Использование отрицательной формы команды (no) удаляет запись из конфигурируемого профиля.

Синтаксис

```
port-range <PORT>
no port-range [<PORT> | all]
```

Параметры

<PORT> – номер порта, принимает значение [1..65535].

Можно указать несколько портов перечислением через запятую «,» либо указать диапазон портов через «-». Пример записи: <PORT>, <PORT> или <PORT>-<PORT> или <PORT>-<PORT>, <PORT>-<PORT>.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-SERVICE

Пример

```
wlc-30(config-object-group-service)# port-range 22
```

regexp

Данной командой описывается шаблон URL-ссылок.

Использование отрицательной формы команды (no) удаляет шаблон URL-ссылок.

Синтаксис

```
regexp <REGEXP>
no regexp {<REGEXP>|all}
```

Параметры

<REGEXP> – регулярное выражение. Описывается строкой до 255 символов. Символ "\" должен быть экранирован.

all – ключ, используемый для удаления всех созданный правил.

Значение по умолчанию

Шаблон не создан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-URL

Пример

```
wlc-30(config-object-group-url)# '^http:\/\/site\.ru'
```

show object-group

Данная команда используется для просмотра информации о профилях IP-адресов и TCP/UDP-портов.

Синтаксис

```
show object-group <PROFILE_TYPE> [<NAME>]
```

Параметры

<PROFILE_TYPE> – тип профиля:

- address-port – профиль связок IP-адресов и TCP/UDP-портов;
- application – профиль приложений;
- content-filter – профиль контентной фильтрации;
- email – профиль почтовых доменов и адресов почтовых ящиков;
- mac – профиль профиля MAC-адресов;
- network – профиль IP-адресов;
- service – профиль TCP/UDP-портов;
- url – профиль URL-ссылок.

<NAME> – имя профиля, задаётся строкой до 31 символа, опциональный параметр. Если имя профиля не задано, то будет выведена информация по всем профилям IP-адресов и TCP/UDP-портов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show object-group network
Network                          Description
-------------------------------   --------------------------------
remote                           --
local                            --
tunnel                           --
wlc-30# show object-group network remote
IP Addresses
--------------------------------
10.102.0.0/16
wlc-30# show object-group service
Service                          Description
-------------------------------   --------------------------------
telnet                           --
ssh                              --
dhcp_server                      --
dhcp_client                      --
ntp                              --
wlc-30# show object-group service ssh
Port ranges
--------------------------------
22
```

url

Команда используется для задания URL-ссылки.

Использование отрицательной формы команды (no) удаляет ссылку из конфигурируемого профиля.

Синтаксис

`url <URL>`

`no url [ <URL> | all ]`

Параметры

<URL> – текстовое поле, содержащее URL-ссылку длинной от 8 до 255 символов.

При удалении с использованием ключа "all" будут удалены все внесенные ранее URL-ссылки.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-URL

Пример

```
wlc-30(config-object-group-url)# url https://vk.com
```

vendor

Команда используется для задания поставщика категорий контентной фильтрации.

Использование отрицательной формы команды (no) удаляет категории контентной фильтрации данного поставщика.

Синтаксис

```
[no] vendor <CONTENT-FILTER-VENDOR>
```

Параметры

<CONTENT-FILTER-VENDOR> – название поставщика категорий контентной фильтрации. Принимает значения:

Kaspersky-Lab – в текущей версии ПО в качестве поставщика категорий контентной фильтрации может выступать только Лаборатория Касперского.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OBJECT-GROUP-CONTENT-FILTER

Пример

```
wlc-30(config-object-group-content-filter)# vendor kaspersky-lab
```

21 Управление NAT

- action destination-nat
- action source-nat
- description
- enable
- from
- ip address
- ip address-range
- ip nat proxy-arp
- ip port
- ip port-range
- match destination-address
- match destination-address-port
- match destination-port
- match icmp
- match protocol
- match source-address
- match source-address-port
- match source-port
- nat alg
- nat destination
- nat source
- persistent
- pool
- rearrange
- renumber rule
- rule
- ruleset
- show ip nat alg
- show ip nat pool
- show ip nat ruleset
- show ip nat translations
- show ip nat proxy-arp
- to

action destination-nat

Данной командой выполняется трансляция адреса и порта получателя для трафика, удовлетворяющего заданным критериям.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
action destination-nat { off | pool <NAME> | netmap <ADDR/LEN> }
```

```
no action destination-nat
```

Параметры

off – трансляция отключена. Трафик, попадающий под заданные критерии, не будет изменен;

pool <NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP-портов. У трафика, попадающего под заданные критерии, будет изменен IP-адрес и TCP/UDP-порт получателя на значения, выбранные из пула;

netmap <ADDR/LEN> – IP-подсеть, используемая при трансляции. У трафика, попадающего под заданные критерии, будет изменен IP-адрес получателя на IP-адрес из указанной подсети. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

Пример

```
wlc-30(config-dnat-rule)# action destination-nat netmap 10.10.10.0/24
```

action source-nat

Данной командой назначается тип действия «трансляция адреса и порта отправителя» и параметры трансляции для трафика, удовлетворяющего критериям, заданным командами «match».

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
action source-nat { off | pool <NAME> | netmap <ADDR/LEN> [static] | interface
[FIRST_PORT - LAST_PORT] }
```

```
no action source-nat
```

Параметры

off – трансляция отключена. Трафик, попадающий под заданные критерии, не будет изменен;

pool <NAME> – задаёт пул IP-адресов и/или TCP/UDP-портов. У трафика, попадающего под заданные критерии, будет изменен IP-адрес и/или TCP/UDP-порт отправителя на значения, выбранные из пула;

netmap <ADDR/LEN> – задаёт IP-подсеть для трансляции. У трафика, попадающего под заданные критерии, будет изменен IP-адрес отправителя на IP-адрес из указанной подсети. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

static – включение статического NAT, доступно при использовании netmap;

interface [FIRST_PORT – LAST_PORT] – задаёт трансляцию в IP-адрес интерфейса. У трафика, попадающего под заданные критерии, будет изменён IP-адрес отправителя на IP-адрес интерфейса, в который трафик будет отправлен. Если дополнительно задан диапазон TCP/UDP-портов, то трансляция будет происходить ещё и для TCP/UDP-портов отправителя, они будут заменены на указанный диапазон портов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# action source-nat netmap 10.10.10.0/24
```

description

Данной командой задаётся описание.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание, задаётся стройкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULESET

CONFIG-SNAT-RULESET

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

CONFIG-DNAT-POOL

CONFIG-SNAT-POOL

Пример

```
wlc-30(config-snat-ruleset)# description "test ruleset"
```

enable

Данной командой активируется конфигурируемое правило.

Отрицательная форма команды (no) деактивирует использование правила.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# enable
```

from

Данной командой ограничивается область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса.

Использование отрицательной формы команды (no) удаляет ограничение области применения группы правил.

Синтаксис

```
from { zone <NAME> | interface <IF> | tunnel <TUN> | default }
no from
```

Параметры

<NAME> – имя зоны изоляции;

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил.

⚠ Группа правил со значением «default» параметра «from» может быть только одна.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULESET

Пример

```
wlc-30(config-dnat-ruleset)# from zone untrusted
```

ip address

Данной командой устанавливается внутренний IP-адрес, на который будет заменяться IP-адрес получателя.

Использование отрицательной формы команды (no) удаляет заданный IP-адрес.

Синтаксис

```
ip address <ADDR>
no ip address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-POOL

Пример

```
wlc-30(config-dnat-pool)# ip address 10.10.10.10
```

ip address-range

Данной командой задаётся диапазон внешних IP-адресов, на которые будет заменяться IP-адрес отправителя.

Использование отрицательной формы команды (no) удаляет заданный диапазон адресов.

Синтаксис

```
ip address-range <IP>[-<ENDIP>]
no ip address-range
```

Параметры

<IP> – IP-адрес начала диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<ENDIP> – IP-адрес конца диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для трансляции используется только IP-адрес начала диапазона.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-POOL

Пример

```
wlc-30(config-snat-pool)# ip address-range 10.10.10.1-10.10.10.20
```

ip nat proxy-arp

Данная команда позволяет контроллеру отвечать на ARP-запросы IP-адресов из указанного пула. Функция необходима для того, чтобы не назначать все IP-адреса из пула трансляции на интерфейсе.

Синтаксис

```
ip nat proxy-arp <OBJ-GROUP-NETWORK-NAME>
no ip nat proxy-arp
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Функция NAT Proxy ARP отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip nat proxy-arp nat-pool
```

ip port

Данной командой устанавливается внутренний TCP/UDP-порт, на который будет заменяться TCP/UDP-порт получателя.

Использование отрицательной формы команды (no) удаляет заданный TCP/UDP-порт.

Синтаксис

```
ip port <PORT>
no ip port
```

Параметры

<PORT> – TCP/UDP-порт, принимает значения [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-POOL

Пример

```
wlc-30(config-dnat-pool)# ip port 5000
```

ip port-range

Данной командой задаётся диапазон внешних TCP/UDP-портов, на которые будет заменяться TCP/UDP-порт отправителя.

Использование отрицательной формы команды (no) удаляет заданный диапазон портов.

Синтаксис

```
ip port-range <PORT>[-<ENDPORT>]
no ip port-range
```

Параметры

<PORT> – TCP/UDP-порт начала диапазона, принимает значения [1..65535];

<ENDPORT> – TCP/UDP-порт конца диапазона, принимает значения [1..65535]. Если не указывать TCP/UDP-порт конца диапазона, то в качестве TCP/UDP-порта для трансляции используется только TCP/UDP-порт начала диапазона.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-POOL

Пример

```
wlc-30(config-snat-pool)# ip port-range 20-100
```

match destination-address

Данной командой устанавливается профиль IP-адресов получателя, для которых должно срабатывать правило.

При использовании команды «not» правило будет срабатывать для IP-адресов получателя, которые не входят в указанный профиль. Использование отрицательной формы команды (no) отменяет установленное действие.

Синтаксис

```
match [not] destination-address <OBJ-GROUP-NETWORK-NAME>
no match destination-address
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адреса, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match destination-address remote
```

match destination-address-port

Данной командой устанавливается профиль связок IP-адресов и TCP/UDP-портов получателя, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для связок IP-адресов и TCP/UDP-портов получателя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] destination-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
no match destination-address
```

Параметры

<OBJ-GROUP-ADDRESS-PORT-NAME> – имя профиля связок IP-адресов и TCP/UDP-портов, задаётся строкой до 31 символа. При указании значения «any» правило не будет учитывать данный способ фильтрации.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match destination-address local
```

match destination-port

Данной командой устанавливается профиль TCP/UDP-портов получателя, для которых должно срабатывать правило.

При использовании команды «not» правило будет срабатывать для TCP/UDP-портов получателя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет установленное действие.

Синтаксис

```
match [not] destination-port <PORT-SET-NAME>
no match destination-port
```

Параметры

<PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match destination-port ssh
```

match icmp

Данная команда используется для настройки параметров протокола ICMP, если он выбран командой «match protocol». Командой устанавливается тип и код сообщений протокола ICMP, для которых должно срабатывать правило.

При использовании команды «not» правило будет срабатывать для всех типов и кодов сообщений протокола ICMP, кроме указанных.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
match [not] icmp { <ICMP_TYPE> <ICMP_CODE> | <OPTION> }
no match icmp
```

Параметры

<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0 ..255];

<ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0 ..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP;

<OPTION> – стандартные типы ICMP-сообщений, может принимать значения:

- administratively-prohibited;
- alternate-address;
- conversion-error;
- dod-host-prohibited;
- dod-network-prohibited;
- echo;
- echo-reply;
- host-isolated;
- host-precedence;
- host-redirect;
- host-tos-redirect;
- host-tos-unreachable;
- host-unknown;
- host-unreachable;
- information-reply;
- information-request;
- mask-reply;
- mask-request;
- network-redirect;
- network-tos-redirect;
- network-tos-unreachable;
- network-unknown;
- network-unreachable;
- option-missing;
- packet-too-big;
- parameter-problem;
- port-unreachable;
- precedence;
- protocol-unreachable;
- reassembly-timeout;
- router-advertisement;
- router-solicitation;
- source-quench;
- source-route-failed;
- time-exceeded;
- timestamp-reply;
- timestamp-request;
- traceroute;

Значение по умолчанию

any any

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match icmp 2 any
```

match protocol

Данной командой устанавливается имя или номер IP-протокола, для которого должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для всех протоколов, кроме указанного.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] protocol <TYPE>
no match protocol
match [not] protocol-id <ID>
no match protocol-id
```

Параметры

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre.

При указании значения «any» правило будет срабатывать для любых протоколов;

<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match protocol udp
```

match source-address

Данной командой устанавливается профиль IP-адресов отправителя, для которых должно срабатывать правило.

При использовании команды «not» правило будет срабатывать для IP-адресов отправителя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет установленное действие.

Синтаксис

```
match [not] source-address <OBJ-GROUP-NETWORK-NAME>
no match source-address
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match source-address local
```

match source-address-port

Данной командой устанавливается профиль связок IP-адресов и TCP/UDP-портов отправителя, для которых должно срабатывать правило.

При использовании параметра «not» (match not) правило будет срабатывать для связок IP-адресов и TCP/UDP-портов отправителя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
no match source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
```

Параметры

<OBJ-GROUP-ADDRESS-PORT-NAME> – имя профиля связок IP-адресов и TCP/UDP-портов, задаётся строкой до 31 символа. При указании значения «any» правило не будет учитывать данный способ фильтрации.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match source-address-port admin
```

match source-port

Данной командой устанавливается профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило.

При использовании команды «not» правило будет срабатывать для TCP/UDP портов отправителя, которые не входят в указанный профиль. Использование отрицательной формы команды (no) отменяет установленное действие.

Синтаксис

```
match [not] source-port <PORT-SET-NAME>
no match source-port
```

Параметры

<PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULE

CONFIG-SNAT-RULE

Пример

```
wlc-30(config-snat-rule)# match source-port telnet
```

nat alg

Данная команда включает функцию трансляции IP-адресов в заголовках уровня приложений.

Использование отрицательной формы команды (no) отключает функцию трансляции IP-адресов в заголовках уровня приложений.

Синтаксис

```
[no] nat alg { <PROTOCOL> }
```

Параметры

<PROTOCOL> – протокол уровня приложений, в заголовках которого должна работать трансляция адресов, принимает значения [ftp, h323, pptp, netbios-ns, gre, sip, tftp].

Вместо имени отдельного протокола можно использовать ключ "all", который включает трансляцию IP-адресов в заголовках всех доступных протоколов.

Значение по умолчанию

Функцию трансляции IP-адресов в заголовках уровня приложений отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# nat alg ftp
```

nat destination

Данная команда позволяет войти в режим настройки сервиса трансляции адресов получателя (DNAT, Destination NAT).

Использование отрицательной формы команды (no) удаляет настройки сервиса трансляции адресов получателя (DNAT, Destination NAT).

Синтаксис

```
[no] nat destination
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# nat destination
wlc-30(config-dnat)#
```

nat source

Данная команда позволяет войти в режим настройки сервиса трансляции адресов отправителя (SNAT, Source NAT).

Использование отрицательной формы команды (no) удаляет настройки сервиса трансляции адресов отправителя (SNAT, Source NAT).

Синтаксис

```
[no] nat source
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# nat source
wlc-30(config-snat)#
```

persistent

Командой выполняется включение функции NAT persistent.

NAT persist ent позволяет приложениям использовать STUN (session traversal utilities for NAT – утилиты проброса сессий для NAT) для установления соединения с устройствами, находящимися за шлюзом NAT. При этом гарантируется, что запросы от одного и того же внутреннего адреса транслируются в один и тот же внешний адрес.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] persistent
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Функция NAT persistent отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-POOL

Пример

```
wlc-30(config-snat-pool)# persistent
```

pool

Команда создаёт и назначает пул IP-адресов и TCP/UDP-портов с определённым именем для сервиса NAT и меняет командный режим на SNAT POOL или DNAT POOL.

⚠ Если пул используется в какой-либо группе правил, то его удалять нельзя.

Использование отрицательной формы команды (no) удаляет заданный пул NAT-адресов.

Синтаксис

```
[no] pool <NAME>
```

Параметры

<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа. Если использовать команду для удаления, то при указании значения «all» будут удалены все пулы IP-адресов и TCP/UDP-портов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT

CONFIG-SNAT

Пример

```
wlc-30(config-snat)# pool nat
wlc-30(config-snat-pool)#
```

rearrange

Данная команда меняет шаг между созданными правилами.

Синтаксис

```
rearrange <VALUE>
```

Параметры

<VALUE> – шаг между правилами, принимает значения [1..50].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULESET

CONFIG-SNAT-RULESET

Пример

```
wlc-30(config-dnat-ruleset)# rearrange 10
```

renumber rule

Данная команда меняет номер правила.

Синтаксис

```
renumber rule <CUR_ORDER> <NEW_ORDER>
```

Параметры

<CUR_ORDER> – текущий номер правила, принимает значения [1..10000];

<NEW_ORDER> – новый номер правила, принимает значения [1..10000].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULESET

CONFIG-SNAT-RULESET

Пример

```
wlc-30(config-dnat-ruleset)# renumber rule 13 100
```

rule

Данной командой создается правило с определённым номером и устанавливается режим командного интерфейса SNAT RULE или DNAT RULE. Правила обрабатываются устройством в порядке возрастания номеров правил.

Использование отрицательной формы команды (no) удаляет правило по номеру либо все правила.

Синтаксис

```
[no] rule <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1 .. 10000]. Если использовать команду для удаления, то при указании значения «all» будут удалены все правила.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT-RULESET

CONFIG-SNAT-RULESET

Пример

```
wlc-30(config-snat-ruleset)# rule 10
wlc-30(config-snat-rule)#
```

ruleset

Данная команда используется для создания группы правил с определённым именем и перехода в командный режим SNAT RULESET или DNAT RULESET.

Использование отрицательной формы команды (no) удаляет заданную группу правил.

Синтаксис

```
[no] ruleset <NAME>
```

Параметры

<NAME> – имя группы правил, задаётся строкой до 31 символа. Если использовать команду для удаления, то при указании значения «all» будут удалены все группы правил.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DNAT

CONFIG-SNAT

Пример

```
wlc-30(config-snat)# ruleset wan
wlc-30(config-snat-ruleset)#
```

show ip nat alg

Данная команда используется для просмотра информации о функционале трансляции IP-адресов в заголовках уровня приложений.

Синтаксис

```
show ip nat alg
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip nat alg
ALG Status:
    FTP:   Enabled
    H.323: Disabled
    GRE:   Disabled
    PPTP:  Disabled
    SIP:   Disabled
    SNMP:  Disabled
    TFTP:  Disabled
```

show ip nat pool

Данная команда используется для просмотра пулов внутренних и внешних IP-адресов и TCP/UDP-портов.

Синтаксис

```
show ip nat <TYPE> pools
```

Параметры

<TYPE> – тип пулов, для просмотра:

- source – внешние IP-адреса и TCP/UDP-порты;

- destination – внутренние IP-адреса и TCP/UDP-порты.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show nat source pools
   Pools
   ~~~~~
ID     Name                    Ip address          Port      Description   Persi
                                                   range                   stent
----   ---------------------   -----------------   -------   -----------   -----
0      outside                 25.56.48.11         2000 -    outside-poo   false
                                                   3000       l
```

show ip nat ruleset

Данной командой выполняется просмотр всех или выбранных групп правил, используемых функцией NAT.

Синтаксис

```
show ip nat <TYPE> ruleset [<NAME>]
```

Параметры

<TYPE> – тип группы правил:

- source – группа правил для трансляции IP-адреса и TCP/UDP-порта отправителя;
- destination – группа правил для трансляции IP-адреса и TCP/UDP-порта получателя;

[NAME] – имя группы правил, опциональный параметр. Если имя не задано – будет выведен список всех групп правил.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip nat source rulesets
   Rulesets
   ~~~~~~~~
ID     Name                              To                   Description
----   -------------------------------   ------------------   -----------------
0      factory                           zone 'untrusted'
1      test                              gigabitethernet      test
                                           1/0/1
```

```
wlc-30# show ip nat source rulesets factory
Ruleset:           factory
Description:
To:                none
Rules:
------
Order:             10
Description:       replace 'source ip' by outgoing interface ip address
Matching pattern:
    Protocol:      any(0)
    Src-addr:      any
    Dest-addr:     any
Action:          interface port any
Status:            Enabled
-------------------------------------------------------------------------------
```

show ip nat translations

Данная команда используется для просмотра сессий трансляции. Для просмотра информации о статистике необходимо включить счетчики (раздел ip firewall mode).

Синтаксис

```
show ip nat translations [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address
<ADDR> ] [ outiside-source-address <ADDR> ] [ inside-destination-address <ADDR> ]
[ outside-destination-address <ADDR> ] [ inside-source-port <PORT> ] [ outside-source-
port <PORT> ] [ inside-destination-port <PORT> ] [ outside-destination-port <PORT> ]
[ summary ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены сессии трансляций в указанном VRF;

summary – выводит суммарную статистику по сессиям трансляции;

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – TCP/UDP-порт, принимает значения [1..65535].

Для Source NAT:

- inside-source-address – ключ для указания IP-адреса источника до трансляции;
- inside-destination-address – ключ для указания IP-адреса назначения на входе в контроллер;
- outiside-source-address – ключ для указания IP-адреса источника после трансляции;

- outside-destination-address – ключ для указания IP-адреса назначения на выходе из контроллера.
- inside-source-port – ключ для указания TCP/UDP-порта отправителя до трансляции;
- outside-source-port – ключ для указания TCP/UDP-порта отправителя после трансляции;
- inside-destination-port – ключ для указания TCP/UDP-порта назначения до трансляции;
- outside-destination-port – ключ для указания TCP/UDP-порта назначения после трансляции.

Для Destination NAT:

- inside-source-address – ключ для указания IP-адреса источника на выходе из контроллера;
- inside-destination-address – ключ для указания IP-адреса назначения после трансляции;
- outiside-source-address – ключ для указания IP-адреса источника на входе в контроллер;
- outside-destination-address – ключ для указания IP-адреса назначения до трансляции;
- inside-source-port – ключ для указания TCP/UDP-порта отправителя до трансляции;
- outside-source-port – ключ для указания TCP/UDP-порта отправителя после трансляции;
- inside-destination-port – ключ для указания TCP/UDP-порта назначения до трансляции;
- outside-destination-port – ключ для указания TCP/UDP-порта назначения после трансляции.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

Source NAT

```
wlc-30# show ip nat translations
Prot   Inside source  Inside destination Outside source Outside destination Pkts Bytes
----   ------------  ------------------   ------------   --------------     -----  -----
icmp   115.0.0.10         1.1.0.2         1.1.0.24          1.1.0.2          3    252
```

Пример 2

Destination NAT

```
wlc-30#  show ip nat translations
Prot   Inside source  Inside destination Outside source Outside destination Pkts Bytes
----   ------------  ------------------   ------------   --------------     -----  -----
 icmp     1.1.0.2        115.0.0.10         1.1.0.2         1.1.0.16          --    --
```

show ip nat proxy-arp

Данная команда используется для просмотра настроек NAT Proxy ARP.

Синтаксис

```
show ip nat proxy-arp
```

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show nat proxy-arp
Interface     IP address range
-----------   ------------------------------------------
gi1/0/15      115.0.0.15-115.0.0.100
```

to

Данной командой ограничивается область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс.

Использование отрицательной формы команды (no) удаляет ограничение области применения группы правил.

Синтаксис

`to { zone <NAME> | interface <IF> | tunnel <TUN> | default }`

`no to`

Параметры

<NAME> – имя зоны изоляции;

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

default – обозначает группу правил для всего трафика, место назначение которого не попало под критерии других групп правил.

⚠ Группа правил со значением «default» параметра «to» может быть только одна.

Значение по умолчанию

None

Необходимый уровень привилегий

10

Командный режим

CONFIG-SNAT-RULESET

Пример

```
wlc-30(config-snat)# ruleset test
wlc-30(config-snat-ruleset)# to interface gigabitethernet 1/0/1
```

22 Настройки IPsec VPN

- Управление VPN. Настройки IKE
  - access profile
  - address-assignment pool
  - assign-interface
  - authentication algorithm
  - authentication mode
  - authentication method
  - bind-interface vti
  - certificate
  - data-tunnel address
  - dead-peer-detection action
  - dead-peer-detection interval
  - dead-peer-detection timeout
  - description
  - dh-group
  - encryption algorithm
  - ike-policy
  - ip prefix
  - lifetime seconds
  - local address
  - local interface
  - local network
  - management-tunnel address
  - mobike disable
  - mode
  - mode
  - password
  - password local-crt-key
  - pfs dh-group
  - pre-shared-key
  - proposal
  - remote address
  - remote network
  - remote network dynamic client
  - security ike gateway
  - security ike policy
  - security ike proposal
  - security ike session uniqueids
  - show security ike
  - user
  - version
  - xauth access-profile
- Управление VPN. Настройки IPsec
  - authentication algorithm
  - description
  - enable
  - encryption algorithm
  - ike dscp
  - ike establish-tunnel
  - ike gateway
  - ike idle-time
  - ike rekey disable
  - ike rekey margin
  - ike rekey randomization

- ike ipsec-policy
- lifetime
- manual authentication algorithm
- manual authentication key
- manual bind-interface vti
- manual encryption algorithm
- manual encryption key
- manual mode
- manual protocol
- manual spi
- mode
- proposal
- protocol
- security ipsec policy
- security ipsec proposal
- security ipsec vpn
- show security ipsec
- show security ipsec vpn authentication
- show security ipsec vpn status
- type

Управление VPN. Настройки IKE

access profile

Данной командой создается профиль настроек пользователя для IKE-GATEWAY с определенным именем и осуществляется переход в режим конфигурирования профиля.

Использование отрицательной формы команды (no) удаляет сконфигурированный профиль настроек пользователя для IKE-GATEWAY.

Синтаксис

```
[no] access profile <NAME>
```

Параметры

<NAME> – имя профиля пользователя для IKE-GATEWAY, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# access profile OFFICE
```

address-assignment pool

Команда используется для создания пула адресов и настройки передаваемых параметров для динамической конфигурации IPsec-клиентов.

Использование отрицательной формы команды (no) удаляет пула адресов.

Синтаксис

```
[no] address-assignment pool <NAME>
```

Параметры

<NAME> – имя пула адресов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# address-assignment pool CENTER
wlc-30(config-pool)#
```

assign-interface

Данной командой указывается loopback-интерфейс для назначения динамического адреса получаемого от IPsec-VPN-сервера.

При использовании отрицательной формы команды (no) удаляется loopback-интерфейс для назначения динамического адреса получаемого от IPsec-VPN-сервера.

Синтаксис

```
assign-interface loopback <LOOPBACK>[-<LOOPBACK>
no assign-interface
```

Параметры

<LOOPBACK> – номер созданного ранее loopback-интерфейса, принимает значение в диапазоне [1..8].

Значение по умолчанию

Отсутствует

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GW

Пример

```
wlc-30(config-ike-gw)# assign-interface loopback 3
```

authentication algorithm

Данной командой устанавливается алгоритм аутентификации, который используется для аутентификации сообщений установленного IKE-соединения. При установлении IKE-соединения используется аутентификация сообщений по ключу (authentication, см. password).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512.

Значение по умолчанию

sha1

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-PROPOSAL

Пример

```
wlc-30(config-ike-proposal)# authentication algorithm md5
```

authentication mode

Данной командой устанавливается режим XAUTH аутентификации удаленных пользователей, подключающихся по протоколу IPsec.

Использование отрицательной формы команды (no) удаляет установленный режим.

Синтаксис

```
authentication mode { local | radius | client }
```

```
no authentication mode
```

Параметры

local – режим аутентификации, использующий локальную базу пользователей конфигурируемого профиля;

radius – режим, при котором аутентификация пользователей проходит через RADIUS-сервер;

client – режим используемый xauth-клиентом.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# authentication mode local
```

authentication method

Данной командой выбирается метод аутентификации по ключу для IKE-соединения. Аутентификация сообщений по ключу используется при установлении IKE-соединения, ключ задаётся в IKE-политике (см. раздел pre-shared-key). После установления IKE-соединения аутентификация сообщений осуществляется при помощи алгоритма хеширования.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
authentication method <METHOD>
no authentication method
```

Параметры

<METHOD> – метод аутентификации ключа. Может принимать значения:

- pre-shared-key – метод аутентификации, использующий предварительно полученные ключи шифрования;
- rsa-public-key – метод аутентификации, использующий RSA-сертификат;
- xauth-psk-key – метод расширенной аутентификации, использующий локальные или удаленные базы пользователей.

Значение по умолчанию

pre-shared-key

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-proposal)# authentication method pre-shared-key
```

bind-interface vti

Данной командой указывается туннельный интерфейс, через который будет проходить трафик в режиме туннеля «route-based».

Использование отрицательной формы команды (no) удаляет привязку к туннельному интерфейсу.

Синтаксис

```
bind-interface vti <VTI>
no bind-interface vti
```

Параметры

<VTI> – идентификационный номер интерфейса VTI.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# bind-interface vti 1
```

certificate

Данной командой указываются необходимые сертификаты.

Использование отрицательной формы команды (no) удаляет название сертификата из конфигурации.

Синтаксис

```
certificate <CERTIFICATE-TYPE> <NAME>
no certificate <CERTIFICATE-TYPE>
```

Параметры

<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения:

- ca – сертификат центра сертификации;
- crl – список отозванных сертификатов;

- local-crt – сертификат локальной стороны;
- local-crt-key – RSA-ключ сертификата локальной стороны;
- local-id – идентификатор локальной стороны. Для отключения проверки полей атрибута Subject локального сертификата используется ключ "any";
- remote-crt – сертификат удаленной стороны. Вместо имени файла возможно использование ключа "any" для установления режима приема открытого ключа удаленной стороны по сети;
- remote-id – идентификатор удаленной стороны. Для отключения проверки полей атрибута Subject сертификата удаленной стороны используется ключ "any".

<NAME> – имя сертификата или ключа, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# certificate ca KEY
```

data-tunnel address

Данной командой указывается IP-адрес для постройки GRE data туннеля, передаваемого клиенту, подключаемому через IPsec с использованием динамического конфигурирования параметров. GRE data туннель должен быть поддержан на стороне клиента. (Требует ELTEX_DATA_IP(28684).

Использование отрицательной формы команды (no) удаляет IP-адрес для постройки GRE data туннеля.

Синтаксис

```
data-tunnel address <ADDR>
no data-tunnel address
```

Параметры

<ADDR> – IP-адрес, для постройки GRE data туннеля задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POOL

Пример

```
wlc-30(config-pool)# data-tunnel address 192.168.2.66
```

dead-peer-detection action

Данной командой устанавливается действие, которое должно предпринять устройство, в случае обнаружения недоступности IPsec соседа, механизмом Dead Peer Detection.

Dead Peer Detection (DPD) – это механизм проверки состояния и доступности соседних устройств. Механизм периодически отправляет R-U-THERE сообщения (для IKE версии 1) или пустые INFORMATIONAL сообщения (для IKE версии 2) для проверки доступности IPsec-соседа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dead-peer-detection action <MODE>
no dead-peer-detection action
```

Параметры

<MODE> – режим работы DPD:

- restart – соединение переустанавливается;
- clear – соединение останавливается;
- hold – соединение поддерживается;
- none – механизм выключен, никаких действий не предпринимается.

Значение по умолчанию

none

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# dead-peer-detection action clear
```

dead-peer-detection interval

Данной командой устанавливается интервал между отправкой сообщений механизмом DPD.

Механизм DPD описан в разделе certificate.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dead-peer-detection interval <SEC>
no dead-peer-detection interval
```

Параметры

<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.

Значение по умолчанию

2 секунды

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# dead-peer-detection interval 15
```

dead-peer-detection timeout

Данной командой задаётся таймаут ответа на сообщения, отправленные механизмом DPD.

Механизм DPD описан в разделе certificate.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
dead-peer-detection timeout <SEC>
no dead-peer-detection timeout
```

Параметры

<SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд.

Значение по умолчанию

30 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# dead-peer-detection timeout 60
```

description

Команда используется для изменения описания профиля, политики или шлюза протокола IKE.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

`description <DESCRIPTION>`

`no description`

Параметры

<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-PROPOSAL

CONFIG-IKE-POLICY

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-proposal)# description "my proposal"
```

dh-group

Данной командой устанавливается номер группы метода Диффи-Хеллмана. Номер группы определяет уровень защищенности IKE-соединения при обмене ключами – защищенность возрастает с ростом номера группы, но увеличивается и время установления соединения.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`dh-group <DH-GROUP>`

`no dh-group`

Параметры

<DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-PROPOSAL

Пример

```
wlc-30(config-ike-proposal)# dh-group 5
```

encryption algorithm

Данной командой выбирается алгоритм шифрования, используемый при установлении IKE-соединения.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
encryption algorithm <ALGORITHM>
no encryption algorithm
```

Параметры

<ALGORITHM> – идентификатор протокола шифрования, принимает значения: des, 3des, blowfis28, blowfis92, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

Значение по умолчанию

3des

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-PROPOSAL

Пример

```
wlc-30(config-ike-proposal)# encryption algorithm aes128
```

ike-policy

Данной командой устанавливается привязка политики протокола IKE к шлюзу.

Использование отрицательной формы команды (no) удаляет привязку политики.

Синтаксис

```
[no] ike-policy <NAME>
```

Параметры

<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# ike-policy ike_pol1
```

ip prefix

Данной командой указывается пул адресов, из которого адреса будут выдаваться IPsec-клиентам.

Использование отрицательной формы команды (no) удаляет пул адресов, из которого адреса будут выдаваться IPsec-клиентам.

Синтаксис

```
ip prefix <ADDR/LEN>
no ip prefix
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Значение по умолчанию

Не задан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POOL

Пример

```
wlc-30(config-pool)# ip prefix 192.168.0.0/16
```

lifetime seconds

Данной командой задаётся время жизни соединения протокола IKE.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
lifetime seconds <SEC>
no lifetime seconds
```

Параметры

<SEC> – период времени, принимает значения [4 ..86400] секунд.

Значение по умолчанию

10800 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# lifetime 21600
```

local address

Данной командой устанавливается IP-адрес локального шлюза IPsec-туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес локального шлюза.

Синтаксис

```
local address <ADDR>
no local address
```

Параметры

<ADDR> – IP-адрес локального шлюза.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# local address 192.168.1.1
```

local interface

Данной командой устанавливается использование IP-адреса, назначенного на интерфейс в качестве локального шлюза IPsec-туннеля.

При использовании отрицательной формы команды (no) прекращается использование IP-адреса, назначенного на интерфейс в качестве локального шлюза.

Синтаксис

```
local interface <IF>
no local interface
```

Параметры

<IF> – тип и идентификатор интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GW

Пример

```
wlc-30(config-ike-gw)# local interface gigabitethernet 1/0/1
```

local network

Данной командой устанавливается IP-адрес подсети отправителя, а также IP-протокол и порт. Трафик, удовлетворяющий заданным критериям, будет направлен в IPsec-туннель.

Использование отрицательной формы команды (no) удаляет IP-адрес подсети отправителя.

Синтаксис

```
[no] local network <ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port <PORT> ] ]
```

Параметры

<ADDR/LEN> – IP-подсеть отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];

<PORT> – TCP/UDP-порт, принимает значения [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# local network 192.168.1.0/24 protocol tcp port 22
```

management-tunnel address

Данной командой устанавливается IP-адрес туннеля для постройки GRE management туннеля, передаваемого клиенту, подключаемому через IPsec с использованием динамического конфигурирования параметров. GRE management туннель должен быть поддержан на стороне клиента. (Требует ELTEX_MANAGEMENT_IP(28683).

Использование отрицательной формы команды (no) удаляет IP-адрес туннеля для постройки GRE management туннеля.

Синтаксис

```
management-tunnel address <ADDR>
no management-tunnel address
```

Параметры

<ADDR> – IP-адрес для постройки GRE management туннеля, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POOL

Пример

```
wlc-30(config-pool)# management-tunnel address 192.168.2.87
```

mobike disable

Данная команда отключает возможность инициатору соединения изменить свою точку подключения к сети (использовать IP-адрес в качестве параметра local address).

Использование отрицательной формы команды (no) активирует функцию автоматического выбора local addres при недоступности описанного в конфигурации.

Синтаксис

```
[ no ] mobike disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# mobike disable
```

mode

Данной командой устанавливается режим согласования первой фазы протокола IKE.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – режим первой фазы IKE, принимает значения:

- main – состоит из трех двусторонних обменов между отправителем и получателем:

    - Во время первого обмена согласуются алгоритмы аутентификации и шифрования, которые будут использоваться для защиты IKE-соединения посредством сопоставления профилей протокола IKE каждого узла;
    - Используя алгоритм Диффи-Хеллмана, стороны обмениваются общим секретным ключом. Также узлы проверяют идентификацию друг друга путем передачи и подтверждения последовательности псевдослучайных чисел;
    - Проверяется идентичность противоположной стороны. В результате выполнения основного режима создается безопасный канал для второй фазы протокола IKE.
- aggressive – этот режим обходится меньшим числом обменов и, соответственно, числом пакетов:
    - В первом сообщении (от инициатора) отправляется информация, которая используется для установления IKE-соединения: предложение параметров SA, инициирование обмена Диффи-Хеллмана, отправление псевдослучайного числа и идентификатора пакета;
    - Во втором сообщении ответчик принимает SA, аутентифицирует инициатора, отправляет псевдослучайное число и свой IKE-идентификатор;
    - В третьем сообщении инициатор аутентифицирует ответчика и подтверждает обмен.

Значение по умолчанию

main

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# mode aggressive
```

mode

Данной командой устанавливается режим перенаправления трафика в туннель.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`mode <MODE>`

`no mode`

Параметры

<MODE> – режим перенаправления трафика в туннель, принимает значения:

- policy-based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям;
- route-based – трафик перенаправляется на основе маршрутов, шлюзом у которых является туннельный интерфейс.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# mode route-based
```

password

Данная команда используется для установки пароля пользователя для IKE-GETWAY. Пароль может быть задан как в открытом виде, так и в виде хеш sha512.

Использование отрицательной формы команды (no) удаляет пароль пользователя для IKE-GETWAY из системы.

Синтаксис

```
password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [8..32] символов, принимает значения [0-9a-fA-F].

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой до 110 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROFILE

Пример

```
wlc-30(config-profile) password tteesstt
```

password local-crt-key

Данная команда используется для установки пароля от зашифрованной цепочки сертификатов (сертификаты назначаются при помощи команды certificate).

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
password local-crt-key ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no password local-crt-key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [8..32] символов, принимает значения [0-9a-fA-F].

<HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой до 110 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy) password tteesstt
```

pfs dh-group

Данной командой устанавливается номер группы метода Диффи-Хеллмана. Номер группы определяет уровень защищенности IPsec-соединения при обмене ключами – защищенность возрастает с ростом номера группы, но увеличивается и время установления соединения.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
pfs dh-group <DH-GROUP>
no pfs dh-group
```

Параметры

<DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-PROPOSAL

Пример

```
wlc-30(config-isec-proposal)# pfs dh-group 5
```

pre-shared-key

Данной командой устанавливается общий секретный ключ для аутентификации, должен совпадать у обоих сторон, устанавливающих туннель.

Использование отрицательной формы команды (no) удаляет установленный ключ.

Синтаксис

```
pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal { <HEX> | encrypted <ENCRYPTED-HEX> } }
```

```
no pre-shared-key
```

Параметры

<TEXT> – строка [1..64] ASCII символов;

<HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате(0xYYYY...) или (YYYY...);

<ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;

<ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.

Значение по умолчанию

none

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# pre-shared-key hexadecimal abc123
```

proposal

Данной командой устанавливается привязка профиля протокола IKE к политике.

Использование отрицательной формы команды (no) удаляет привязку профиля протокола IKE.

Синтаксис

```
[no] proposal <NAME>
```

Параметры

<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-POLICY

Пример

```
wlc-30(config-ike-policy)# proposal ike_prop1
```

remote address

Данной командой устанавливается IP-адрес удаленного шлюза IPsec-туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес удаленного шлюза.

Синтаксис

```
remote address { <ADDR> | any }
no remote address
```

Параметры

<ADDR> – IP-адрес удаленного шлюза.

any – ключ позволяющий принимать запросы на установление IKE-сессии от любого IP-адреса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# remote address 192.168.1.2
```

remote network

Данной командой устанавливается IP-адрес подсети получателя, а также IP-протокол и порт или назначается динамический пул адресов для удалённых клиентов, использующих XAUTH. Трафик, удовлетворяющий заданным критериям, будет направлен в IPsec-туннель.

Использование отрицательной формы команды (no) удаляет IP-адрес подсети отправителя.

Синтаксис

```
remote network { dynamic pool <POOL> | <ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port
<PORT> ] ] | any }
```

```
no remote network { dynamic pool |<ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port
<PORT> ] ] | any }
```

Параметры

<POOL> – выделенный динамический пул адресов для клиентов XAUTH;

<ADDR/LEN> – IP-подсеть получателя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];

<PORT> – TCP/UDP-порт, принимает значения [1..65535];

any – ключ, указывающий на необходимость шифрования любого исходящего трафика.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# remote network 192.168.0.0/24 protocol tcp port 22
```

remote network dynamic client

Данной командой включается получение списка удаленных сетей от IPsec-VPN-сервера.

При использовании отрицательной формы команды (no) отключается получение списка удаленных сетей от IPsec-VPN-сервера.

Синтаксис

```
[no] remote network dynamic client
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IKE-GW

Пример

```
wlc-30(config-ike-gw)# remote network dynamic client
```

security ike gateway

Данной командой осуществляется переход в командный режим конфигурирования шлюза IKE SECURITY IKE GATEWAY. Если шлюз IKE с указанным именем не существует в конфигурации, то он будет создан. Параметры шлюза включают в себя VTI-интерфейс, в который будет направляться трафик, политика и версия протокола IKE, а также режим перенаправления трафика в туннель.

Использование отрицательной формы команды (no) удаляет шлюз протокола IKE.

Синтаксис

```
[no] security ike gateway <NAME>
```

Параметры

<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IKE-шлюзы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ike gateway ike_gw1
wlc-30(config-ike-gw)#
```

security ike policy

Данной командой создается политика IKE, которая включает в себя профили протокола IKE, общий секретный ключ для аутентификации и режим согласования первой фазы протокола IKE.

Использование отрицательной формы команды (no) удаляет указанную политику. Команда устанавливает режим командной строки SECURITY IKE POLICY.

Синтаксис

```
[no] security ike policy <NAME>
```

Параметры

<NAME> – имя политики IKE, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IKE политики.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ike policy ike_pol1
wlc-30(config-ike-policy)#
```

security ike proposal

Данной командой создается профиль протокола IKE (Internet Key Exchange), который включает в себя параметры алгоритмов шифрования и аутентификации, метода Диффи-Хеллмана, которые будут использоваться при согласовании параметров IKE со встречной стороной VPN соединения при создании Security Association (SA). Кроме того, профиль задаёт предельное время действия SA. Использование отрицательной формы команды (no) удаляет заданный профиль.

Синтаксис

```
[no] security ike proposal <NAME>
```

Параметры

<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IKE-профили.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ike proposal ike_prop1
wlc-30(config-ike-proposal)#
```

security ike session uniqueids

Данной командой задается режим переподключения клиентов XAUTH с одним логином/паролем.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
security ike session uniqueids <MODE>
no security ike session uniqueids
```

Параметры

<MODE> – режим переподключения, принимает следующие значения:

- no – установленное подключение XAUTH будет удалено, если для нового подключения XAUTH инициатором соединения будет отправлено уведомление "INITIAL_CONTACT", будет назначен ранее использованный IP-адрес. В противном случае, установленное соединение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес.
- never – установленное подключение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес. Уведомление "INITIAL_CONTACT" будет в любом случае проигнорировано.
- replace – установленное подключение XAUTH будет удалено. Для нового подключения XAUTH будет использован ранее использованный IP-адрес.
- keep – установленное подключение XAUTH будет удержано. Новое подключение XAUTH будет отклонено.

Значение по умолчанию

never

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ike session uniqueids replace
```

show security ike

Команда используется для просмотра списка шлюзов, политик или профилей.

Синтаксис

```
show security ike { gateway | policy | proposal } [<NAME>]
```

Параметры

gateway – при указании команды «gateway» будет выведен список сконфигурированных шлюзов;

policy – при указании команды «policy» будет выведен список сконфигурированных политик;

proposal – при указании команды «proposal» будет выведен список сконфигурированных профилей;

<NAME> – имя. При указании определенного имени шлюза, политики, профиля будет выведена подробная информация.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ike proposal
   Proposal
   ~~~~~~~~
Name           Auth      Encryption         DH   Hash         Lifetime
------------   -------   ----------------   --   ----------   ----------
aaa            pre-sha   3des               1    sha1         3600
               red-key
 wlc-30# show security ike policy
   Policy
   ~~~~~~
Name                          Mode         Proposal
---------------------------   ----------   ----------------------------------
ike_pol1                      main         ike_prop1
 wlc-30# show security ike gateway ik_gw
Description:                 --
IKE Policy:                  ike_pol1
IKE Version:                 v1-only
Mode:                        route-based
Binding interface:           vti1
IKE Dead Peer Detection:
    Action:                  none
    Interval:                2
    Timeout:                 30
```

user

Данной командой задается имя пользователя для аутентификации IKE-GETWAY.

Использование отрицательной формы команды (no) удаляет указанного пользователя.

После выполнения данной команды контроллер переходит в режим конфигурирования пароля пользователя (config-profile).

Синтаксис

```
[no] user <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ACCESS-PROFILE

Пример

```
wlc-30(config-access-profile)# user connecter963
```

version

Данной командой задаётся версия протокола IKE.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`version <VERSION>`

`no version`

Параметры

<version> – версия IKE-протокола: v1-only или v2-only.

Значение по умолчанию

v1-only

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gw)# version v2-only
```

xauth access-profile

Данной командой указывается локальный список пользователей для авторизации XAUTH.

Использование отрицательной формы команды (no) удаляет заданный профиль.

Синтаксис

`[no] xauth access-profile <NAME> [client <USER-NAME>`

Параметры

<NAME> – название локального списка пользователей XAUTH, задаётся строкой до 31 символа;

<USER-NAME> – имя пользователя из прикрепленного xauth-профиля, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IKE-GATEWAY

Пример

```
wlc-30(config-ike-gateway)# xauth access-profile OFFICE
```

Управление VPN. Настройки IPsec

authentication algorithm

Данной командой устанавливается алгоритм аутентификации. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512.

Значение по умолчанию

sha1

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-PROPOSAL

Пример

```
wlc-30(config-ipsec-proposal)# authentication algorithm md5
```

description

Данной командой выполняется изменение описания.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN
CONFIG-IPSEC-PROPOSAL
CONFIG-IPSEC-POLICY

Пример

```
wlc-30(config-ipsec-vpn)# description "VPN to Moscow Office"
```

enable

Данной командой активируется IPsec VPN.
Использование отрицательной формы команды (no) деактивирует IPsec VPN.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# enable
```

encryption algorithm

Данной командой устанавливается алгоритм шифрования. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
encryption algorithm <ALGORITHM>
no encryption algorithm
```

Параметры

<ALGORITHM> – протокол шифрования, принимает значения: null, des, 3des, blowfis28, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

Значение по умолчанию

3des

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-PROPOSAL

Пример

```
wlc-30(config-ipsec-proposal)# encryption algorithm blowfish128
```

ike dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ike dscp <DSCP>
no ike dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

63

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike dscp 40
```

ike establish-tunnel

Командой устанавливается режим активации VPN. Данная команда актуальна, только если в VPN выбран режим согласования ключей «ike». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ike establish-tunnel <MODE>
no Ike establish-tunnel
```

Параметры

<MODE> – режим активации VPN:

- by-request – соединение активируется встречной стороной;
- route – соединение активируется при появлении трафика, маршрутизируемого в туннель;
- immediate – туннель активируется автоматически после применения конфигурации. Если произойдет закрытие соединения от удаленной стороны VPN при использовании режима immediate, тогда установить соединение повторно будет возможно только после перезагрузки контроллера или перезапуске VPN через CLI контроллера.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike establish-tunnel route
```

ike gateway

Данной командой осуществляется привязка IKE-шлюза к VPN. Данная команда актуальна, только если в VPN выбран режим согласования ключей «ike». Настройка режима согласования ключей описана в mode.

Синтаксис

```
ike gateway <NAME>
no ike gateway
```

Параметры

<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike gateway ike_gw1
```

ike idle-time

Данной командой устанавливается значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA.

Использование отрицательной формы команды (no) отключает данный таймер.

Синтаксис

```
ike idle-time <TIME>
no ike idle-time
```

Параметры

<TIME> – интервал в секундах, принимает значения [4..86400].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike idle-time 3600
```

ike rekey disable

Данной командой отключается пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт.

Использование отрицательной формы команды (no) включает пересогласование ключей.

Синтаксис

```
[no] ike rekey disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike rekey disable
```

ike rekey margin

Данной командой можно настроить начало пересогласования ключей IKE-соединения до истечения времени жизни.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
Ike rekey margin { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }
no ike rekey margin { seconds | packets | kilobytes }
```

Параметры

<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetime seconds, см. lifetime). Принимает значения [4..86400].

<PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetime packets, см. lifetime). Принимает значения [4..86400].

<KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetime kilobytes, см. lifetime). Принимает значения [4..86400].

Значение по умолчанию

Пересогласование ключей до истечения времени – за 540 секунд.

Пересогласование ключей до истечения объема трафика и количества пакетов – отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike rekey margin seconds 1800
```

ike rekey randomization

Данной командой устанавливается уровень случайного разброса значений параметров margin seconds, margin packets, margin kilobytes.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ike rekey randomization <VALUE>
no ike rekey randomization
```

Параметры

<VALUE> – максимальный процент разброса значений, принимает значения [1..100].

Значение по умолчанию

100%

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike rekey randomization 10
```

ike ipsec-policy

Данная команда устанавливает привязку IPsec-политики к VPN. Данная команда актуальна, только если в VPN выбран режим согласования ключей «ike». Настройка режима согласования ключей описана в mode.

Синтаксис

```
ike ipsec-policy <NAME>
no ike ipsec-policy
```

Параметры

<NAME> – имя IPsec-политики, задаётся строка до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
```

lifetime

Данной командой устанавливается время жизни IPsec-туннеля.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
lifetime { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }
no lifetime { seconds | packets | kilobytes }
```

Параметры

<SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд;

<PACKETS> – количество пакетов, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400];

<KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд.

Значение по умолчанию

3600 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-POLICY

Пример

```
wlc-30(config-ipsec-proposal)# lifetime seconds 3600
```

manual authentication algorithm

Данной командой устанавливается алгоритм аутентификации. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`manual authentication algorithm <ALGORITHM>`

`no manual authentication algorithm`

Параметры

<ALGORITHM> – алгоритм аутентификации, принимает значения [md5, md5-128, sha1, sha1-160, aesxcbc, sha2-256, sha2-384, sha2-512].

Значение по умолчанию

none

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual authentication algorithm sha1
```

manual authentication key

Данной командой устанавливается ключ аутентификации. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Синтаксис

```
manual authentication key { ascii-text {<TEXT> | encrypted <ENCRYPTED-TEXT>} |
hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }
```

```
no manual authentication key
```

Параметры

<TEXT> – строка [1..64] ASCII символов;

<HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...);

<ENCRYPTED_TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;

<ENCRYPTED_HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual authentication key hexadecimal abcdef
```

manual bind-interface vti

Данной командой указывается туннельный интерфейс, через который будет проходить трафик в режиме туннеля route-based. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
manual bind-interface vti <VTI>
```

```
no manual bind-interface vti
```

Параметры

<VTI> – индекс интерфейса VTI, принимает значения [1..250].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual bind-interface vti 0
```

manual encryption algorithm

Данной командой устанавливается алгоритм шифрования. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) удаляет установленное значение.

Синтаксис

```
manual encryption algorithm <ALGORITHM>
no manual encryption algorithm
```

Параметры

<ALGORITHM> – алгоритм шифрования, принимает значения: des, 3des, blowfis28, blowfis92, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

Значение по умолчанию

3des

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual encryption algorithm blowfis28
```

manual encryption key

Данной командой устанавливается ключ шифрования. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) удаляет установленное значение.

Синтаксис

```
manual encryption key { ascii-text { < TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal
{ <HEX> | encrypted <ENCRYPTED-HEX> } }

no manual encryption key
```

Параметры

<TEXT> – строка [1..36] ASCII символов;

<HEX> – число размером [1..24] байт задаётся строкой [2..72] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...);

<ENCRYPTED-TEXT> – зашифрованный пароль размером [1..24] байт, задаётся строкой [2..72] символов;

<ENCRYPTED-HEX> – зашифрованное число размером [2..36] байт, задаётся строкой [2..144] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual encryption key hexadecimal 0x123456
```

manual mode

С помощью данной команды осуществляется установка режима перенаправления трафика в туннель. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
manual mode <MODE>

no manual mode
```

Параметры

<MODE> – режим прохождения трафика:

- policy-based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям;
- route-based – трафик перенаправляется на основе маршрутов, у которых шлюзом является туннельный интерфейс.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual mode route-based
```

manual protocol

Данной командой устанавливается инкапсулирующий протокол. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`manual protocol <TYPE>`

`no manual protocol`

Параметры

<TYPE> – тип протокола, принимает значения:

- ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется;
- esp – данный протокол осуществляет аутентификацию и шифрование трафика.

Значение по умолчанию

esp

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual protocol ah
```

manual spi

Данной командой устанавливается индекс параметров безопасности. Данная команда актуальна, только если в VPN выбран режим согласования ключей «manual». Настройка режима согласования ключей описана в mode.

Использование отрицательной формы команды (no) удаляет индекс параметров безопасности.

Синтаксис

```
manual spi <HEX>
no manual spi
```

Параметры

<HEX> – индекс параметров безопасности, задаётся значение размером 32 бита (8 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# manual spi FF
```

mode

Данной командой устанавливается режим согласования данных, необходимых для активации VPN.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – режим работы VPN:

- ike – согласование алгоритмов аутентификации и шифрования, ключей аутентификации и шифрования, индекса параметра безопасности и других данных осуществляется через протокол IKE;
- manual – пользователь должен сам настроить идентичные параметры на обоих узлах для работы VPN. При данном режиме не происходит установления IKE-соединения между узлами. Каждый из узлов шифрует и дешифрует пакеты, основываясь только на заданных параметрах.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-ipsec-vpn)# mode ike
```

proposal

Данной командой к политике привязываются профили набора протоколов IPsec.

Использование отрицательной формы команды (no) удаляет привязку к указанному профилю.

Синтаксис

```
[no] proposal <NAME>
```

Параметры

<NAME> – имя профиля набора протоколов IPsec, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-POLICY

Пример

```
wlc-30(config-ipsec-policy)# proposal ipsec_prop1
```

protocol

Данной командой устанавливается инкапсулирующий протокол.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
protocol <PROTOCOL>
no protocol
```

Параметры

<PROTOCOL> – инкапсулирующий протокол, принимает значения:

- ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется;
- esp – данный протокол осуществляет аутентификацию и шифрование трафика.

Значение по умолчанию

esp

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-PROPOSAL

Пример

```
wlc-30(config-ipsec-proposal)# protocol ah
```

security ipsec policy

Данной командой создается политика набора протоколов IPsec, которая включает в себя профили набора протоколов IPsec для согласования второй фазы протокола IKE.

Использование отрицательной формы команды (no) удаляет установленное значение.

Команда устанавливает режим командной строки SECURITY IPSEC POLICY.

Синтаксис

```
[no] security ipsec policy <NAME>
```

Параметры

<NAME> – имя политики IPsec, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IPsec-политики.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ipsec policy ipsec_pol1
wlc-30(config-ipsec-policy)#
```

security ipsec proposal

Данной командой создается профиль для набора протоколов IPsec. Профиль IPsec включает в себя параметры алгоритмов шифрования и аутентификации, протокола защиты соединения IPsec-туннеля, а также время жизни соединения.

Использование отрицательной формы команды (no) удаляет указанный профиль.

Команда устанавливает режим командной строки SECURITY IPSEC PROPOSAL.

Синтаксис

```
[no] security ipsec proposal <NAME>
```

Параметры

<NAME> – имя профиля IPsec, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IPsec-профили.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ipsec proposal ipsec_prop1
wlc-30(config-ipsec-proposal)#
```

security ipsec vpn

Данной командой создается VPN на основе набора протоколов IPsec и устанавливается командный режим SECURITY IPSEC VPN.

Использование отрицательной формы команды (no) удаляет сконфигурированный VPN.

Синтаксис

```
[no] security ipsec vpn <NAME>
```

Параметры

<NAME> – имя VPN, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все VPN.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ipsec vpn ipsec_vpn1
wlc-30(config-ipsec-vpn)#
```

show security ipsec

Данной командой выполняется просмотр конфигураций VPN, политик и профилей набора протоколов IPsec.

Синтаксис

```
show security ipsec { vpn configuration | policy | proposal } [<NAME>]
```

Параметры

vpn configuration – при указании данной команды будет выведена конфигурация всех VPN;

policy – при указании данной команды будет выведен список сконфигурированных политик набора протоколов IPsec;

proposal – при указании команды будет выведен список сконфигурированных профилей набора протоколов IPsec;

<NAME> – имя. При указании определенного имени VPN, политики или профиля будет выведена подробная информация.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ipsec proposal
   Proposal
   ~~~~~~~~
Name                     Prot   Enc. alg.          Auth. alg.        Lifetime
----------------------   ----   -----------------  ---------------   -----------
ipsec_prop1              esp    aes128             sha1              28800 sec
wlc-30# show secu   rity ipsec policy
Name                   Description           Proposal
--------------------   -------------------   ------------------------------------
ipsec_pol1                                   ipsec_prop1
Master# show security ipsec vpn configuration IPSECVPN
Description:                --
State:                      Enabled
IKE:
    Establish tunnel:           immediate
    IPsec policy:               IPSECPOLICY
    IKE gateway:                IKEGW
    IKE DSCP:                   63
    IKE idle-time:              0s
    IKE rekeying:               Enabled
        Margin time:                540s
        Margin kilobytes:           0
        Margin packets:             0
        Randomization:              100%
```

show security ipsec vpn authentication

Данная команда позволяет посмотреть список и параметры подключившихся IPsec-VPN-клиентов.

Синтаксис

```
show security ipsec vpn authentication <NAME> [ vrf <VRF> ]
```

Параметры

<NAME> – имя созданного IPsec VPN, задаётся строкой до 31 символа.

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет включено разрешение DNS-имен.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ipsec vpn authentication
Local host        Remote host       Local subnet          Remote subnet         Authentication
State
---------------   ---------------   -------------------   -------------------
-----------------------------------------   -----------
2.2.2.1           2.2.2.2           192.168.2.0/24        192.168.1.1/32        Xauth PSK,
login: ipsec                     Established
```

show security ipsec vpn status

Данной командой выполняется просмотр статуса всех VPN, которые устанавливают соединение через IKE-протокол либо определенного VPN при указании его имени.

Синтаксис

```
show security ipsec vpn status [ vrf <VRF> ] [ <NAME> ]
```

Параметры

<NAME> – имя VPN, задаётся строкой до 31 символа;

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ipsec vpn status
Name      Local host   Remote host  Initiator spi       Responder spi        State
--------- ------------ ------------ ----------------    ---------------      ------
ipsec_vpn1 10.100.14.1 10.100.14.2  0x05d8e0ac3543f0cb  0xcfa1c4179d001154   Established
```

type

Данной командой задается тип инкапсуляции IPsec.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
type <TYPE>
no type
```

Параметры

<TYPE> – тип инкапсуляции IPsec, принимает значения:

- tunnel;
- transport.

Значение по умолчанию

tunnel

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPSEC-VPN

Пример

```
wlc-30(config-access-vpn)# type transport
```

23 Управление VPN. Настройки удаленного доступа

- Общие команды настройки удаленного доступа
  - authentication required disable
  - clear remote-access counters
  - clear remote-access session
  - description
  - enable
  - encryption mppe
  - remote-access
  - show remote-access configuration
  - show remote-access counters
  - show remote-access status
- Настройка L2TP over IPsec/PPTP-сервера
  - authentication mode
  - authentication method
  - dns-servers
  - dscp
  - ipsec authentication method
  - ipsec authentication pre-shared-key
  - ipsec ike proposal
  - ipsec proposal
  - local-address
  - mtu
  - outside-address
  - remote-address
  - remote network
  - remote networks
  - username
  - wins-servers
- Настройка OpenVPN-сервера
  - address-range
  - authentication algorithm
  - bridge-group
  - certificate
  - client-isolation
  - client-max
  - compression
  - dns-server
  - duplicate-cn
  - encryption algorithm
  - ip address
  - login authentication
  - network
  - port
  - protocol
  - redirect-gateway
  - route
  - timers holdtime
  - timers keepalive
  - subnet
  - tunnel
  - username
  - wins-server

Общие команды настройки удаленного доступа

authentication required disable

Данной командой отключается обязательная аутентификация PPP-клиентов для PPTP- или L2TP-сервера.

Использование отрицательной формы команды (no) включается обязательная аутентификация PPP для PPTP- или L2TP-сервера.

Синтаксис

```
[no] authentication required disable
```

Параметры

Отсутствуют.

Значение по умолчанию

Не задан.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-pptp-server)# authentication required disable
```

clear remote-access counters

Данной командой осуществляется сброс счетчиков соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Синтаксис

```
clear remote-access counters [ pptp | l2tp | openvpn ] [ server <SERVER-NAME> ]
[ username <USER-NAME> ] [ ip-address <ADRR> ]
```

Параметры

<SERVER-NAME> – имя профиля OpenVPN, PPTP или L2TP over IPsec-сервера;

<USER-NAME> – имя OpenVPN, PPTP или L2TP over IPsec-пользователя;

<ADDR> – IP-адрес OpenVPN, PPTP или L2TP over IPsec-пользователя.

При выполнении команды без параметра будут сброшены все счетчики соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear remote-access counters
```

clear remote-access session

Данной командой осуществляется завершение соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Синтаксис

```
clear remote-access session [ pptp | l2tp | openvpn] [ server <SERVER-NAME> ] [ username <USER-NAME> ] [ip-address <ADRR> ]
```

Параметры

<SERVER-NAME> – имя профиля OpenVPN, PPTP или L2TP over IPsec-сервера;

<USER-NAME> – имя OpenVPN, PPTP или L2TP over IPsec-пользователя;

<ADDR> – IP-адрес OpenVPN, PPTP или L2TP over IPsec-пользователя. При выполнении команды без параметра будут завершены все OpenVPN, PPTP и L2TP over IPsec-соединения.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear remote-access session
```

description

Команда используется для изменения описания профиля OpenVPN, PPTP и L2TP over IPsec-серверов.

Использование отрицательной формы команды (no) удаляет описание профиля.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER
CONFIG-L2TP-SERVER
CONFIG-OPENVPN-SERVER

Пример

Установить описание для профиля PPTP-сервера:

```
wlc-30(config-pptp-server)# description "Our remote workers"
```

enable

Данной командой активируется конфигурируемый профиль серверов удаленного доступа.
Использование отрицательной формы команды (no) деактивирует конфигурируемый профиль.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER
CONFIG-L2TP-SERVER
CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-pptp-server)# enable
```

encryption mppe

Данная команда включает шифрование MPPE (Microsoft Point-to-Point Encryption) для PPTP-соединений.
Использование отрицательной формы команды (no) отключает шифрование.

Синтаксис

```
[no] encryption mppe
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPTP-SERVER

Пример

```
wlc-30(config-pptp-server)# encryption mppe
```

remote-access

Данной командой создается профиль сервера удаленного доступа.
Использование отрицательной формы команды (no) удаляет указанный профиль.

Синтаксис

```
[no] remote-access <SERVER-TYPE> <NAME>
```

Параметры

<SERVER-TYPE> – тип сервера удаленного доступа. Может принимать значения l2tp, openvpn, pptp;
<NAME> – имя профиля сервера удаленного доступа, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# remote-access l2tp remote-workers
wlc-30(config-l2tp-server)#
```

show remote-access configuration

Командой выполняется просмотр параметров профилей OpenVPN, PPTP и L2TP over IPsec-серверов.

Синтаксис

```
show remote-access configuration { pptp | l2tp | openvpn } [ <NAME> ]
```

Параметры

<NAME> – имя профиля OpenVPN, PPTP или L2TP over IPsec-сервера.

При выполнении команды без параметра будут показаны параметры всех OpenVPN, PPTP или L2TP over IPsec-серверов.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show remote-access configuration pptp pptp1
State:                      Enabled
Description:                --
Security zone:              trusted
Authentication mode:        local
MTU:                        1500
Local address:              192.168.1.1
Remote address:             rem_pptp(10.0.10.20-10.0.10.40)
Outside address:            115.0.0.1
DNS server:                 --
WINS server:                --
   Users
   ~~~~~
#     Name                    State      Encrypted password
---   --------------------    --------   ------------------------------
0     pptp                    Enabled    8CB5107EA7005AFF
1     petr                    Enabled    CCE5513EE45A1EAC
```

show remote-access counters

Командой выполняется просмотр счетчиков соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Синтаксис

```
show remote-access counters [ pptp | l2tp | openvpn ] [ server <SERVER-NAME> ] [ username <USER-NAME> ] [ ip-address <ADRR> ]
```

Параметры

<SERVER-NAME> – имя профиля PPTP или L2TP over IPsec-сервера;

<USER-NAME> – имя OpenVPN, PPTP или L2TP over IPsec-пользователя;

<ADDR> – IP-адрес OpenVPN, PPTP или L2TP over IPsec-пользователя;

При выполнении команды без параметра будут показаны счетчики всех соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show remote-access counters
User            IP-address        UC recv      Bytes recv   Err recv     MC recv
-------------   ---------------   ----------   ----------   ----------   ----------
ivan            10.20.20.5        262          25365        0            0
fedor           20.20.20.160      59           5236         0            0
User            IP-address        UC sent      Bytes sent   Err sent
-------------   ---------------   ----------   ----------   ----------
ivan            10.20.20.5        249          29298        0
fedor           20.20.20.160      16           739          0
wlc-30# show remote-access counters l2tp
PPTP Server: remote-workers
User: ivan(10.20.20.5)
 Packets received:               231
 Bytes received:                 22229
 Dropped on receive:             0
 Receive errors:                 0
 Multicasts received:            0
 Receive length errors:          0
 Receive buffer overflow errors: 0
 Receive CRC errors:             0
 Receive frame errors:           0
 Receive FIFO errors:            0
 Receive missed errors:          0
 Receive compressed:             0
 Packets transmitted:            189
 Bytes transmitted:              21858
 Dropped on transmit:            0
 Transmit errors:                0
 Transmit aborted errors:        0
 Transmit carrier errors:        0
 Transmit FIFO errors:           0
 Transmit heartbeat errors:      0
 Transmit window errors:         0
 Transmit comressed:             0
 Collisions:                     0
```

show remote-access status

Командой выполняется просмотр состояния соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Синтаксис

```
show remote-access status [ pptp | l2tp | openvpn ] [ server <SERVER-NAME> ] [ username <USER-NAME> ] [ ip-address <ADRR> ]
```

Параметры

<SERVER-NAME> – имя профиля OpenVPN, PPTP или L2TP over IPsec-сервера;

<USER-NAME> – имя OpenVPN, PPTP или L2TP over IPsec-пользователя;

<ADDR> – IP-адрес OpenVPN, PPTP или L2TP over IPsec-пользователя.

При выполнении команды без параметра будет показано состояние всех соединений OpenVPN, PPTP и L2TP over IPsec-пользователей.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show remote-access status
User                IP-address         Server
-----------------   ---------------    ---------------------------------------
ivan                10.20.20.5         pptp(remote-workers)
fedor               20.20.20.160       l2tp(remote-workers-l2tp)
Count sessions: 2
```

Настройка L2TP over IPsec/PPTP-сервера

authentication mode

Данной командой устанавливается режим аутентификации удаленных пользователей, подключающихся по протоколам PPTP или L2TP over IPsec.

Использование отрицательной формы команды (no) удаляет установленный режим.

Синтаксис

```
authentication mode { local | radius }
```

```
no authentication mode
```

Параметры

- local – режим аутентификации, использующий локальную базу пользователей конфигурируемого профиля;
- radius – режим, при котором аутентификация пользователей проходит через RADIUS-сервер.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# authentication mode local
```

authentication method

Данной командой разрешается использование метода аутентификации удаленных пользователей, подключающихся по протоколам PPTP или L2TP over IPsec.

Использование отрицательной формы команды (no) удаляет установленный режим.

Синтаксис

```
[no] authentication method <METHOD>
```

Параметры

<METHOD> – метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap].

Значение по умолчанию

Разрешен только chap

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# authentication method mschap
```

dns-servers

Данной командой указывается список DNS-серверов, которые будут использовать удаленные пользователи, подключающиеся по протоколам PPTP и L2TP over IPsec.

Использование отрицательной формы команды (no) удаляет настроенные адреса DNS-серверов.

Синтаксис

```
dns-servers object-group <NAME>
no dns-servers
```

Параметры

<NAME> – имя профиля IP-адресов, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# dns-servers object-group pptp_dns
```

dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов PPTP и L2TP over IPsec-серверов.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
dscp <DSCP>
no dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

32

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# dscp 40
```

ipsec authentication method

Данной командой выбирается метод аутентификации по ключу для IKE-соединения. Аутентификация сообщений по ключу используется при установлении IKE-соединения, ключ задаётся командой «ipsec authentication pre-shared-key» (см раздел ipsec authentication pre-shared-key).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipsec authentication method pre-shared-key
no ipsec authentication method
```

Параметры

pre-shared-key – метод аутентификации, использующий предварительно полученные ключи шифрования.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-l2tp-server)# ipsec authentication method pre-shared-key
```

ipsec authentication pre-shared-key

Данной командой устанавливается общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.

Использование отрицательной формы команды (no) удаляет установленный ключ.

Синтаксис

```
ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }|
hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }
no ipsec authentication pre-shared-key
```

Параметры

<TEXT> – строка [1..64] ASCII символов;

<HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...);

<ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;

<ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-l2tp-server)# ipsec authentication pre-shared-key ascii-text password
```

ipsec ike proposal

Данной командой для L2TP-сервера назначается шаблон, ограничивающий используемые методы аутентификации и шифрования протокола IKE.

Использование отрицательной формы команды (no) удаляет ограничения на использование методов аутентификации и шифрования протокола IKE.

Синтаксис

```
[no] ipsec ike proposal <NAME>
```

Параметры

<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.

Значение по умолчанию

Ограничение отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-l2tp-server)# ipsec ike proposal IKE_PROPOSAL
```

ipsec proposal

Данной командой для L2TP-сервера назначается шаблон, ограничивающий используемые методы аутентификации и шифрования протокола IPsec.

Использование отрицательной формы команды (no) удаляет ограничения на использование методов аутентификации и шифрования протокола IPsec.

Синтаксис

```
[no] ipsec proposal <NAME>
```

Параметры

<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.

Значение по умолчанию

Ограничение отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-l2tp-server)# ipsec proposal IPSEC_PROPOSAL
```

local-address

Данной командой указывается IP-адрес, используемый PPTP или L2TP over IPsec сервером в качестве локального IP-адреса туннеля.

Использование отрицательной формы команды (no) удаляет настроенный локальный IP-адрес туннеля.

Синтаксис

```
local-address { object-group <NAME> | ip-address <ADDR> }
no local-address
```

Параметры

<NAME> – имя профиля IP-адресов, который содержит локальный IP-адрес туннеля, задаётся строкой до 31 символа;

<ADDR> – локальный IP-адрес туннеля задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# local-address object-group pptp_local
```

mtu

Данной командой указывается MTU для интерфейсов, которые будут создаваться при подключении удаленных пользователей по протоколам PPTP и L2TP over IPsec.

Использование отрицательной формы команды (no) устанавливает значение MTU по умолчанию.

Синтаксис

```
mtu <MTU>
no mtu
```

Параметры

<MTU> – значение MTU, принимает значения в диапазоне [1280..1500].

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# mtu 1400
```

outside-address

Данной командой указывается IP-адрес, который будет прослушиваться PPTP или L2TP over IPsec-сервером на наличие входящих подключений.

Использование отрицательной формы команды (no) удаляет настроенный адрес для прослушивания.

Синтаксис

```
outside-address { object-group <NAME> | ip-address <ADDR> | interface { <IF> | <TUN> } }
no outside-address
```

Параметры

<NAME> – имя профиля IP-адресов, содержащий адрес, который будет прослушиваться PPTP или L2TP over IPsec-сервером на наличие входящих подключений, задаётся строкой до 31 символа;

<ADDR> – IP-адрес, который будет прослушиваться PPTP или L2TP over IPsec-сервером на наличие входящих подключений, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# outside-address object-group pptp_outside
```

remote-address

Данной командой указывается список IP-адресов, из которого PPTP или L2TP over IPsec-сервером выдаются динамические IP-адреса удаленным пользователям.

Использование отрицательной формы команды (no) удаляет список IP-адресов удаленных пользователей.

Синтаксис

```
remote-address { object-group <NAME>| address-range <FROM-ADDR>-<TO-ADDR> }
no remote-address
```

Параметры

<NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа;

<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# remote-address object-group pptp_remote
```

remote network

Данной командой устанавливается IP-адрес подсети, доступной при установлении динамического PPTP/L2TP-туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес подсети, доступной через динамический PPTP/L2TP-туннель.

Синтаксис

`remote network <ADDR/LEN>`

`no remote network`

Параметры

<ADDR/LEN> – IP-подсеть получателя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPP-USER

Пример

```
wlc-30(config-ppp-user)# remote network 192.168.54.0/24
```

remote networks

Данной командой устанавливается список IP-адрес подсетей, доступных при установлении PPTP/L2TP-туннеля.

Использование отрицательной формы команды (no) удаляет IP-адрес подсети, доступной через динамический PPTP/L2TP-туннель.

Синтаксис

`remote networks <OBJ-GROUP-NETWORK-NAME>`

`no remote network`

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP/IPv6-адресов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPP-USER

Пример

```
wlc-30(config-ppp-user)# remote network 192.168.54.0/24
```

username

Данной командой создается пользователь для подключения к PPTP или L2TP over IPsec-серверам. После выполнения данной команды, контроллер переходит в режим конфигурирования параметров PPP-пользователя.

Использование отрицательной формы команды (no) удаляет указанного пользователя.

Команда устанавливает режим командной строки PPTP USER или L2TP USER в зависимости от текущего командного режима.

Синтаксис

```
[no] username <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# username fedor
wlc-30(config-pptp-user)#
```

wins-servers

Данной командой указывается список WINS-серверов, которые будут использовать удаленные пользователи, подключающиеся по протоколам PPTP и L2TP over IPsec.

Использование отрицательной формы команды (no) удаляет настроенные адреса WINS-серверов.

Синтаксис

```
wins-servers object-group <NAME>
no wins-servers
```

Параметры

<NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PPTP-SERVER

CONFIG-L2TP-SERVER

Пример

```
wlc-30(config-pptp-server)# wins-servers object-group l2tp_wins
```

Настройка OpenVPN-сервера

address-range

Данной командой указывается список IP-адресов, из которого OpenVPN-сервером выдаются динамические IP-адреса удаленным пользователям в режиме L2.

Использование отрицательной формы команды (no) удаляет список IP-адресов удаленных пользователей.

Синтаксис

```
address-range <FROM-ADDR>-<TO-ADDR>
no address-range
```

Параметры

<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# address-range 192.168.1.10-192.168.1.250
```

authentication algorithm

Данная команда определяет алгоритм аутентификации клиентов OpenVPN.

Использование отрицательной формы команды (no) устанавливает режим аутентификации по умолчанию.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication-algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- 8-128 bits key size: md4, rsa-md4, md5, rsa-md5, mdc2, rsa-mdc2
- 8-160 bits key size: sha, sha1, rsa-sha, rsa-sha1, rsa-sha1-2, dsa, dsa-sha, dsa-sha1, dsa-sha1-old, ripemd160, rsa-ripemd160, ecdsa-with-sha1
- 8-224 bits key size: sha-224, rsa-sha-224
- 8-256 bits key size: sha-256, rsa-sha-256
- 8-384 bits key size: sha-384, rsa-sha-384
- 8-512 bits key size: sha-512, rsa-sha-512, whirlpool

Значение по умолчанию

sha

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# authentication algorithm cleartext
```

bridge-group

Данная команда используется для включения клиентских соединений по OpenVPN в L2-домен.

Использование отрицательной формы команды (no) исключает соединения из L2-домена.

Синтаксис

```
bridge-group <BRIDGE-ID>
no bridge-group
```

Параметры

<BRIDGE-ID> – идентификационный номер моста. Задается в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# bridge-group 15
```

certificate

Данной командой указываются сертификаты и ключи. Сертификаты и ключи должны быть предварительно скопированы на контроллер с помощью команды *copy*, описанной в разделе copy.

Использование отрицательной формы команды (no) удаляет из профиля указанный сертификат.

Синтаксис

```
certificate <CERTIFICATE-TYPE> <NAME>
no certificate <CERTIFICATE-TYPE>
```

Параметры

<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения:

- ca – сертификат удостоверяющего сервера;
- crl – список отозванных сертификатов;
- dh – ключ Диффи-Хеллмана;
- server-crt – публичный сертификат сервера;
- server-key – приватный ключ сервера;
- ta – HMAC-ключ;
- client-key – приватный ключ OPENVPN-клиента;
- client-crt – сертификат OPENVPN-клиента.

<NAME> – имя сертификата или ключа, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# certificate ca ca.crt
```

client-isolation

Данной командой включается блокировка передачи данных между клиентами.

Использование отрицательной формы команды (no) снимает блокировку.

Синтаксис

```
[no] client-isolation
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# client-isolation
```

client-max

Данной командой устанавливается максимальное количество одновременных пользовательских сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
client-max <VALUE>
no client-max
```

Параметры

<VALUE> – максимальное количество пользователей, принимает значения [1..65535].

Значение по умолчанию

Не ограничено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# clients-max 500
```

compression

Данной командой включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN.

Использование отрицательной формы команды (no) отключает механизм сжатия передаваемых данных.

Синтаксис

```
[no] compression
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# compression
```

dns-server

Данной командой указывается список DNS-серверов, которые будут использовать удаленные пользователи.

Использование отрицательной формы команды (no) удаляет настроенные адреса DNS-серверов.

Синтаксис

```
dns-server <ADDR>
no dns-server { <ADDR> | all }
```

Параметры

<ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

all – удалить все сконфигурированные диапазоны IP-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# dns-server 1.1.1.1
```

duplicate-cn

Данная команда разрешает подключение множества пользователей с одним сертификатом.

Использование отрицательной команды (no) запрещает использование одного сертификата более чем одному пользователю.

Синтаксис

```
[no] duplicate-cn
```

Параметры

Команда не имеет параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# duplicate-cn
```

encryption algorithm

Данной командой выбирается алгоритм шифрования, используемый при передачи данных.

Использование отрицательной формы команды (no) отключает шифрование.

Синтаксис

```
encryption algorithm <ALGORITHM>
no encryption algorithm
```

Параметры

<ALGORITHM> – идентификатор протокола шифрования, принимает значения: des, blowfish128, aes128, des-ede, aes192, 3des, desx, aes256.

Значение по умолчанию

Шифрование отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# encryption algorithm aes128
```

ip address

Данная команда определяет статический IP-адрес для указанного клиента. Использование отрицательной формы команды (no) удаляет статический IP-адрес у клиента.

Синтаксис

```
[no] ip address <ADDR>
```

Параметры

<ADDR> – IP-адрес, имеет следующий формат:

- AAA.BBB.CCC.DDD – IP-адрес подсети с маской в форме префикса, где AAA–DDD принимают значения [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-USER

Пример

```
wlc-30(config-openvpn-server)# username client
wlc-30(config-openvpn-user)# ip address 10.10.100.15
```

login authentication

Данной командой осуществляется активация списка аутентификации пользователей для их авторизации.

В конфигурации по умолчанию активным является список с именем «default», данный список содержит один способ аутентификации – «local».

Использование отрицательной формы команды (no) деактивирует список аутентификации.

Синтаксис

`login authentication <NAME>`

`no login authentication`

Параметры

<NAME> – имя списка, задаётся строкой до 31 символа.

Значение по умолчанию

default

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# login authentication OPENVPN-LIST
```

network

Данной командой определяется подсеть, из которой выдаются IP-адреса пользователям. Первый IP-адрес в подсети выступает шлюзом для пользовательских сессий.

Использование отрицательной формы команды (no) удаляет данную подсеть.

Синтаксис

```
network <ADDR/LEN>
no network
```

Параметры

<ADDR/LEN> – IP-подсеть подсети, имеет один из следующих форматов:

- AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# network 192.168.25.0/24
```

port

Данной командой устанавливается TCP/UDP-порт, который будет прослушивается OpenVPN-сервером.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – TCP/UDP-порт, принимает значения [1..65535].

Значение по умолчанию

1194

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# port 5000
```

protocol

Данной командой устанавливается инкапсулирующий протокол.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
protocol <PROTOCOL>
no protocol
```

Параметры

<TYPE> – тип инкапсуляции, возможные значения:

- TCP-инкапсуляция в TCP-сегменты;
- UDP-инкапсуляция в UDP-дейтаграммы.

Значение по умолчанию

Установлено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# protocol udp
```

redirect-gateway

Данная команда включает анонсирование маршрута по умолчанию для OpenVPN-соединений, что приводит к замене маршрута по умолчанию на клиентской стороне. Новым шлюзом по умолчанию станет IP-адрес OpenVPN-сервера.

Использование отрицательной формы команды (no) отключает анонсирование маршрута по умолчанию.

Синтаксис

```
[no] redirect-gateway
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# redirect-gateway
```

route

Данной командой включается анонсирование указанных подсетей, шлюзом является IP адрес OpenVPN-сервера (первый IP-адрес из подсети, заданной с помощью команды network, описанной в разделе network).

Использование отрицательной формы команды (no) отключает анонсирование указанных подсетей.

Синтаксис

```
route <ADDR/LEN>
no route { <ADDR/LEN> | all }
```

Параметры

<ADDR/LEN> – IP-подсеть, имеет следующий формат:

- AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# route 192.168.25.0/24, 192.168.26.0/24
```

timers holdtime

Данной командой устанавливается временной интервал, по истечении которого встречная сторона считается недоступной. Таймер запускается после установления отношений соседства и начинает отсчёт от 0. Таймер сбрасывается при получении каждого ответа на keepalive сообщение от встречной стороны. Рекомендуется устанавливать значение таймера, не менее *3 * keepalive*.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers holdtime <TIME>
no timers holdtime
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# timers holdtime 360
```

timers keepalive

Данной командой устанавливается временной интервал, по истечении которого идет проверка соединения со встречной стороной.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers keepalive <TIME>
no timers keeaplive
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# timers keepalive 120
```

subnet

Данная команда определяет подсеть, которая должна быть доступна через подключение указанного пользователя OpenVPN-сервера. После подключения пользователя к OpenVPN-серверу в таблице маршрутизации появляется маршрут в указанную подсеть через динамически созданный туннель.

Использование отрицательной формы команды (no) удаляет подсеть, работающую за данным пользователем.

Синтаксис

```
[no] subnet <ADDRLEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, имеет следующий формат:

- AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-USER

Пример

```
wlc-30(config-openvpn-server)# username client
wlc-30(config-openvpn-user)# subnet 192.168.25.128/28
```

tunnel

Данной командой определяется тип соединения с частной сетью через OpenVPN-сервер.

Использование отрицательной формы команды (no) удаляет текущее значение.

Синтаксис

```
tunnel <TYPE>
no tunnel
```

Параметры

<TYPE> – инкапсулирующий протокол, принимает значения:

- ip – соединение точка-точка;
- ethernet – подключение к L2-домену.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# tunnel ip
```

username

Данная команда позволяет перейти в режим конфигурирования для указанного пользователя OpenVPN-сервера.

Использование отрицательной формы команды (no) восстанавливает настройки пользователя по умолчанию.

Синтаксис

```
[no] username { <NAME> | all }
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

all – ключ, используемый для удаления всех ранее созданных пользователей.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# username client
wlc-30(config-openvpn-user)#
```

wins-server

Данной командой указывается список WINS-серверов, которые будут использовать удаленные пользователи.

Использование отрицательной формы команды (no) удаляет настроенные адреса WINS-серверов.

Синтаксис

```
wins-server <ADDR>
no wins-server { <ADDR> | all }
```

Параметры

<ADDR> – IP-адрес WINS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

all – удалить все сконфигурированные IP-адреса DNS-серверов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OPENVPN-SERVER

Пример

```
wlc-30(config-openvpn-server)# wins-servers 1.1.1.1
```

24 Маршрутизация

- Общие настройки маршрутизации
- Общие команды анонсирования и приема маршрутов
- Маршрутизация на основе политик (PBR)
- Настройка связок ключей
- Настройка протокола BFD
- Настройка статических маршрутов IPv4/IPv6
- Настройка протокола BGP
- Настройка протоколов RIP и RIPNG
- Настройка протоколов OSPF и OSPFv3
- Настройка протокола IS-IS

Общие настройки маршрутизации

- authentication algorithm
- authentication key
- enable
- graceful-restart
- graceful-restart timeout
- ip path-mtu-discovery
- ip protocols max-routes
- ip protocols preference
- ipv6 protocols max-routes
- ipv6 tcp adjust-mss
- show ip protocols
- show ip route
- show ipv6 protocols
- show ipv6 route

authentication algorithm

Данная команда определяет алгоритм аутентификации.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом (доступно только для режимов CONFIG-RIP и CONFIG-OSPF-VLINK);
- md5 – пароль хешируется по алгоритму md5.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-BGP

CONFIG-BGP-VRF

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-OSPF-VLINK

Пример

```
wlc-30(config-rip)# authentication algorithm cleartext
```

authentication key

Данная команда устанавливает пароль для аутентификации с соседом.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов.

<ENCRYPTED-TEXT> – зашифрованный пароль размером 8-16 байт (16-32 символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-BGP

CONFIG-BGP-VRF

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-OSPF-VLINK

Пример

```
wlc-30(config-bgp-af)# authentication key ascii-text 123456789
wlc-30(config-bgp-af)# authentication key ascii-text encrypted CDE65039E5591FA3F1
```

enable

Данной командой включается конфигурируемый протокол маршрутизации, область, виртуальное соединение, соседство.

Использование отрицательной формы команды (no) отключает RIP-протокол.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-RIPNG

CONFIG-OSPF

CONFIG-OSPF-AREA

CONFIG-OSPF-VLINK

CONFIG-OSPFV3

CONFIG-OSPFV3-AREA

CONFIG-OSPFV3-VLINK

CONFIG-ISIS

CONFIG-BGP

CONFIG-BGP-VRF

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример 1

```
wlc-30(config-rip)# enable
```

Пример 2

```
wlc-30(config-ospf)# enable
```

Пример 3

```
 wlc-30(config-isis)# enable
```

Пример 4

```
wlc-30(config-bgp-neighbor)# enable
```

graceful-restart

Данной командой включается механизм поддержание активного состояния соседства с сохранением маршрутной информации на момент перезапуска протокола маршрутизации.

Использование отрицательной формы команды (no) отключает данный механизм.

Синтаксис

```
[no] graceful-restart
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-OSPF

CONFIG-OSPFV3

Пример

```
wlc-30(config-bgp-neighbor)# graceful-restart
```

graceful-restart timeout

Данной командой устанавливается временной интервал, в течении которого поддерживать активное состояние соседства на момент перезапуска протокола маршрутизации. По истечению временного интервала встречная сторона считается недоступной. Используется совместно с командой graceful-restart.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
graceful-restart timeout <TIME>
no graceful-restart timeout
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-OSPF

CONFIG-OSPFV3

Пример

```
wlc-30(config-bgp-neighbor)# graceful-restart timeout 60
```

ip path-mtu-discovery

Данная команда разрешает/запрещает поиск PMTU для протоколов TCP, SCTP, DCCP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip path-mtu-discovery <ACT>
no ip path-mtu-discovery
```

Параметры

<ACT> – назначаемое действие:

- enable – разрешает поиск PMTU для протоколов TCP, SCTP, DCCP;
- disable – запрещает поиск PMTU для протоколов TCP, SCTP, DCCP.

Значение по умолчанию

Поиск PMTU разрешен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip path-mtu-discovery disable
```

ip protocols max-routes

Данная команда позволяет настроить емкость таблиц маршрутизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip protocols <PROTOCOL> max-routes <VALUE>
no ip protocols <PROTOCOL> max-routes
```

Параметры

<PROTOCOL> – вид протокола, принимает значения: rip (только в глобальном режиме), ospf, isis, bgp;

<VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне:

- BGP – [0..2500000],
- OSPF и IS-IS – [0..300000];
- RIP – [0..10000].

Значение по умолчанию для глобального режима

BGP – 2500000;

OSPF и IS-IS – 300000;

RIP – 10000.

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-VRF

Пример

```
wlc-30(config)# ip protocols ospf max-routes 4400
```

ip protocols preference

Данная команда позволяет настроить приоритетность протоколов маршрутизации для основной таблицы маршрутизации.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip protocols <PROTOCOL> preference <VALUE>`

`no ip protocols <PROTOCOL> preference`

Параметры

<PROTOCOL> – вид протокола, принимает значения: static, rip, ospf, isis, bgp, dhcp, l2tp, pppoe, pptp;

<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255].

Значение по умолчанию

BGP (170)

IS-IS (160)

OSPF (150)

RIP (100)

DHCP (40)

L2TP (50)

PPPoE (50),

PPTP (50)

Static (1)

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip protocols ospf preference 44
```

ipv6 protocols max-routes

Данная команда позволяет настроить емкость таблиц маршрутизации IPv6.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 protocols <PROTOCOL> max-routes <VALUE>
no ipv6 protocols <PROTOCOL> max-routes
```

Параметры

<PROTOCOL> – вид протокола, принимает значения: rip (только в глобальном режиме), ospf, isis, bgp;

<VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне:

- BGP – [0..2500000],
- OSPFv3 и IS-IS – [0..300000];
- IPv6 BGP – [0..1500000].

Значение по умолчанию для глобального режима

OSPFv3 – 300000;

IPv6 BGP – [1..2500000].

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-VRF

Пример

```
wlc-30(config)# ipv6 protocols ospf max-routes 4400
```

ipv6 tcp adjust-mss

Данной командой переопределяется значение поля MSS (Maximum segment size) во входящих TCP-пакетах.

Использование отрицательной формы команды (no) отключает корректировку значение поля MSS.

Синтаксис

```
ipv6 tcp adjust-mss <MSS>
no ipv6 tcp adjust-mss
```

Параметры

<MSS> – значение MSS, принимает значения в диапазоне [40..1940].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ipv6 tcp adjust-mss 1400
```

show ip protocols

Данная команда выводит информацию о настройках протоколов IP-маршрутизации.

Синтаксис

```
show ip protocols [ <PROTOCOL> ] [ vrf <VRF> ]
```

Параметры

<PROTOCOL> – протокол маршрутизации, по которому должна быть отображена информация:

- bgp;
- ospf;
- isis;
- rip;
- static;
- dhcp;
- pptp;
- pppoe;
- l2tp.

Без указания протокола маршрутизации, выводится информация о настройках всех протоколов маршрутизации.

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh ip protocols
BGP:
    Max routes:    --
    Preference:    170
OSPF:
    Max routes:    --
    Preference:    150
RIP:
    Max routes:    --
    Preference:    100
Static:
    Preference:    1
```

show ip route

Данная команда позволяет просмотреть таблицу маршрутизации устройства. Если задан параметр <SUBNET>, то детально отображаются маршруты к данной подсети. Если задан параметр <VRF>, то команда отображает таблицу маршрутизации указанного экземпляра VRF.

Синтаксис

```
show ip route [ vrf <VRF> ] [ { <SUBNET> [ long-prefix ] | all | summary | arp-proxy |
<PROTOCOL> } ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<SUBNET> – адрес назначения, опциональный параметр, может быть задан в следующих видах:

- AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
- AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32];
- all – выводит информацию о всех маршрутах, включая не выбранные для FIB;
- long-prefix – выводит информацию о маршрутах до сетей являющихся подсетью заданной;
- summary – выводит суммарную статистику протоколов маршрутизации;
- arp-proxy – выводит информацию о настроенных пулах arp-nat-proxy на интерфейсах итуннелях;
- <PROTOCOL> – фильтрация по типу протоколу (bgp, connected, ospf , isis, rip, static).

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip route
Codes: C - connected, S - static, R - RIP derived,
        O - OSPF derived, IA - OSPF inter area route,
        E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
        B - BGP derived, D - DHCP derived, K - kernel route,
        * - FIB route
C     * 192.168.1.0/24    [0/0]   dev br1                           [direct 01:14:16]
C     * 10.100.100.0/24   [0/0]   dev gi1/0/5                       [direct 01:14:17]
wlc-30# show ip route summary
Direct Connected: 12
Static:           46
RIP:              0
OSPF:             2000
BGP:              100000
```

show ipv6 protocols

Данная команда выводит информацию о настройках протоколов IPv6-маршрутизации.

Синтаксис

```
show ipv6 protocols [ <PROTOCOL> ] [ vrf <VRF> ]
```

Параметры

<PROTOCOL> – протокол маршрутизации, по которому должна быть отображена информация:

- bgp;
- ospf;
- isis;
- static;
- dhcp;
- pppoe;
- pptp;
- l2tp.

Без указания протокола маршрутизации выводится информация о настройках всех протоколов маршрутизации

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh ipv6 protocols
BGP:
    Max routes:    --
    Preference:    170
OSPF:
    Max routes:    --
    Preference:    150
Static:
    Preference:    1
```

show ipv6 route

Команда для просмотра таблицы маршрутизации устройства. Если задан параметр <SUBNET>, то детально отображаются маршруты к данной подсети. Если задан параметр <VRF>, то команда отображает таблицу маршрутизации указанного экземпляра VRF.

Синтаксис

```
show ipv6 route [ vrf <VRF> ] [ { <SUBNET> | all | summary | <PROTOCOL> } ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<SUBNET> – адрес назначения, опциональный параметр, может быть задан в следующих видах:

- X:X:X:X::X – IPv6-адрес хоста, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF];
- X:X:X:X::X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];
- all – выводит информацию о всех маршрутах, включая неактивные;
- summary – выводит суммарную статистику протоколов маршрутизации;
- <PROTOCOL> – фильтрация по типу протоколу (bgp, connected, ospf , isis, static).

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 route
 Codes: C - connected, S - static, R - RIP derived,
        O - OSPF derived, IA - OSPF inter area route,
        E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
        B - BGP derived, D - DHCP derived, K - kernel route,
        * - FIB route
S     * ::/0              [1/0]   via fc00::1 on gi1/0/5           [static 03:16:23]
S     * 2001::/120        [1/6]   dev gi1/0/5                      [static 03:16:23]
C     * fc00::/120        [0/0]   dev gi1/0/5                      [direct 03:16:23]
S     * fc00:3::1/128     [1/0]   via fc00::1 on gi1/0/5           [static 03:16:23]
wlc-30# show ipv6 route summary
Direct Connected: 1
Static:           3
RIP:              0
OSPF:             0
BGP:              0
```

Общие команды анонсирования и приема маршрутов

- default-information-originate
- description
- ip prefix-list
- ipv6 prefix-list
- network
- permit/deny
- prefix-list
- redistribute bgp
- redistribute connected
- redistribute ipv6 bgp
- redistribute ipv6 ospf
- redistribute isis
- redistribute ospf
- redistribute rip
- redistribute static

default-information-originate

Данной командой включается генерация и отправка маршрута по умолчанию, если он прописан в таблице маршрутизации FIB, для:

- NSSA-области (анонсирование маршрута) в качестве NSSA-LSA;
- BGR IPv4/IPv6 address family.

Использование отрицательной формы команды (no) отключает генерацию маршрута по умолчанию.

Синтаксис

```
[no] default-information-originate
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-BGP-VRF

CONFIG-OSPF-AREA

CONFIG-OSPFV3-AREA

Пример

```
wlc-30(config-ospf-area)# default-information-originate
```

description

Данная команда используется для изменения описания конфигурируемого списка IP-подсетей или IPv6-подсетей.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание списка IP-подсетей или IPv6-подсетей, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PL

CONFIG-IPV6-PL

Пример

```
wlc-30(config-pl)# description "Drop Local NETs"
```

ip prefix-list

Данной командой создается список IP-подсетей, который в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.

Использование отрицательной формы команды (no) удаляет список префиксов.

Синтаксис

```
[no] ip prefix-list <NAME>
```

Параметры

<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip prefix-list ospf_in
```

ipv6 prefix-list

Данной командой создается список IPv6-подсетей, который в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IPv6-маршрутов.

Использование отрицательной формы команды (no) удаляет список префиксов.

Синтаксис

```
[no] ipv6 prefix-list <NAME>
```

Параметры

<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 prefix-list ospfv3_in
```

network

Данной командой включается анонсирование указанной подсети.

Использование отрицательной формы команды (no) отключает анонсирование указанной подсети.

Синтаксис

```
[no] network <ADDR/LEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, имеет один из следующих форматов:

- AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32];
- X:X:X:X::X/EE – IPv6-адрес и маска подсети, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-RIPNG

CONFIG-OSPF-AREA

CONFIG-OSPFV3-AREA

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

Пример

```
wlc-30(config-rip)# network 192.168.25.0/24
```

permit/deny

Данной командой разрешаются (permit) или запрещаются (deny) списки префиксов.

Синтаксис

```
permit [ { object-group <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN> | <IPV6-ADDR/LEN> } ]
[ { eq <LEN> | le <LEN> | ge <LEN> [ le <LEN> ] } ]
```

```
deny [ { object-group <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN > | <IPV6-ADDR/LEN> } ] [ { eq
<LEN> | le <LEN> | ge <LEN> [ le <LEN> ] } ]
```

```
no { object-group <OBJ-GROUP-NETWORK-NAME> | prefix { <ADDR/LEN> | <IPV6-ADDR/LEN> } }
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP/IPv6-адресов, задаётся строкой до 31 символа;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов и [1..128] в IPv6-списках префиксов;

eq – при указании команды длина префикса должна соответствовать указанной;

le – при указании команды длина префикса должна быть меньше либо соответствовать указанной;

ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PL

CONFIG-IPV6-PL

Пример

```
wlc-30(config-pl)# permit static ge 24 le 28
```

prefix-list

Данной командой добавляется фильтрация подсетей во входящих или исходящих обновлениях.

Использование отрицательной формы команды (no) отключает фильтрацию.

Синтаксис

```
prefix-list <PREFIX-LIST-NAME> { in | out }
no prefix-list { in| out }
```

Параметры

<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа:

in – фильтрация входящих маршрутов;

out – фильтрация анонсируемых маршрутов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMALY

CONFIG-BGP-VRF-NEIGHBOR-FAMALY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-ripng)# prefix-list rip_in in
```

redistribute bgp

Данной командой включается анонсирование маршрутов автономной системы BGP.

Использование отрицательной формы команды (no) отключает анонсирование маршрутов автономной системы BGP.

Синтаксис

```
redistribute bgp <AS> [ route-map <NAME> ] [ <LEVEL> ]
no redistribute bgp <AS>
```

Параметры

<AS> – номер автономной системы из которой будут анонсироваться маршруты, может принимать значения [1..4294967295];

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-bgp-family)# redistribute bgp 30
wlc-30(config-ospf)# redistribute bgp 35
wlc-30(config-rip)# redistribute bgp 300
```

redistribute connected

Данной командой включается анонсирование напрямую подключенных подсетей.

Использование отрицательной формы команды (no) отключает анонсирование напрямую подключенных подсетей.

Синтаксис

```
redistribute connected [ route-map <NAME> ] [ <LEVEL> ]
no redistribute connected
```

Параметры

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.

<LEVEL> – уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-rip)# redistribute connected
```

redistribute ipv6 bgp

Данной командой включается анонсирование ipv6-маршрутов автономной системы BGP.

Использование отрицательной формы команды (no) отключает анонсирование ipv6-маршрутов автономной системы BGP.

Синтаксис

```
redistribute ipv6 bgp <AS> [ route-map <NAME> ] [ <LEVEL> ]
no redistribute ipv6 bgp <AS>
```

Параметры

<AS> – номер автономной системы из которой будут анонсироваться ipv6-маршруты, может принимать значения [1..4294967295];

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых BGP-ipv6-маршрутов, задаётся строкой до 31 символа;

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# redistribute ipv6 bgp 30 level 2
```

redistribute ipv6 ospf

Данной командой включается анонсирование маршрутов из базы OSPFv3-процесса согласно выбранным условиям.

Использование отрицательной формы команды (no) отключает анонсирование маршрутов из базы OSPFv3-процесса.

Синтаксис

```
redistribute ipv6 ospf <ID> [ <ROUTE-TYPE1> ] [ <ROUTE-TYPE2> ] [ <ROUTE-TYPE3> ]
[ <ROUTE-TYPE4> ] [ route-map <NAME> ] [ <LEVEL> ]
```

```
no redistribute ipv6 ospf <ID>
```

Параметры

<ID> – номер процесса, может принимать значение [1..65535];

<ROUTE-TYPE> – типы маршрутов которые будут анонсироваться:

- intra-area – анонсирование маршрутов OSPFv3-процесса в пределах зоны;
- inter-area – анонсирование маршрутов OSPFv3-процесса между зонами;
- external1 – анонсирование внешних маршрутов OSPFv3-формата 1;
- external2 – анонсирование внешних маршрутов OSPFv3-формата 2.

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых OSPFv3-маршрутов, задаётся строкой до 31 символа;

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# redistribute ospf 10 external2
```

redistribute isis

Данной командой включается анонсирование маршрутов из базы ISIS согласно выбранным условиям. Использование отрицательной формы команды (no) отключает анонсирование маршрутов из базы ISIS.

Синтаксис

```
redistribute isis <ID> <ROUTE-TYPE> [ route-map <NAME> ]
no redistribute isis <ID>
```

Параметры

<ID> – номер процесса, может принимать значение [1..65535].

<ROUTE-TYPE> – тип маршрута:

- level-1 – анонсирование маршрутов ISIS-процесса уровня 1;
- level-2 – анонсирование маршрутов ISIS-процесса уровня 2;
- inter-area – анонсирование межзоновых маршрутов ISIS-процесса.

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых ISIS-маршрутов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-rip)# redistribute isis 1 level-1 level-2
```

redistribute ospf

Данной командой включается анонсирование маршрутов из базы OSPF-процесса согласно выбранным условиям.

Использование отрицательной формы команды (no) отключает анонсирование маршрутов из базы OSPF-процесса.

Синтаксис

```
redistribute ospf <ID> <ROUTE-TYPE1> [ <ROUTE-TYPE2> ] [ <ROUTE-TYPE3> ] [ <ROUTE-TYPE4> ] [ route-map <NAME> ] [ <LEVEL> ]

no redistribute ospf <ID>
```

Параметры

<ID> – номер процесса, может принимать значение [1..65535];

<ROUTE-TYPE> – типы маршрутов которые будут анонсироваться:

- intra-area – анонсирование маршрутов OSPF-процесса в пределах зоны;
- inter-area – анонсирование маршрутов OSPF-процесса между зонами;
- external1 – анонсирование внешних маршрутов OSPF-формата 1;
- external2 – анонсирование внешних маршрутов OSPF-формата 2.

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа;

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-bgp-family)# redistribute ospf 10 external2
```

redistribute rip

Данной командой включается анонсирование маршрутов из базы маршрутов RIP.

Использование отрицательной формы команды (no) отключает анонсирование маршрутов из базы RIP.

Синтаксис

```
redistribute rip [ route-map <NAME> ] [ <LEVEL> ]
no redistribute rip
```

Параметры

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

Пример

```
wlc-30(config-bgp-family)# redistribute rip
```

redistribute static

Данной командой включается анонсирование статических ipv4/ipv6-маршрутов.

Использование отрицательной формы команды (no) отключает анонсирование статических маршрутов.

Синтаксис

```
redistribute static [ route-map <NAME> ] [ <LEVEL> ]
no redistribute static
```

Параметры

<NAME> – имя маршрутной карты, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа;

<LEVEL> — уровень протокола IS-IS в который происходит анонсирование маршрутов (актуально только в режиме конфигурирования CONFIG-ISIS):

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-FAMILY

CONFIG-BGP-VRF-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-bgp-family)# redistribute static
```

Маршрутизация на основе политик (PBR)

- action
- action set as-path prepend
- action set community
- action set extcommunity
- action set ip bgp-next-hop
- action set ip next-hop
- action set ip next-hop verify-availability
- action set ipv6 bgp-next-hop
- action set ipv6 next-hop
- action set local-preference
- action set metric bgp
- action set metric isis
- action set metric ospf
- action set metric rip
- action set origin
- action set tag ospf
- action set tag rip
- action set weight bgp
- description
- ip local policy route-map
- ip policy route-map
- match as-path
- match community
- match extcommunity
- match ip access-group
- match ip address
- match ip address object-group
- match ip next-hop
- match ip route-source
- match ipv6 address
- match ipv6 address object-group
- match ipv6 next-hop
- match ipv6 route-source
- match metric bgp
- match metric ospf
- match metric rip
- match tag ospf
- match tag rip
- match weight bgp
- route-map
- route-map
- rule
- show ip route-map

action

Данная команда используется для указания действия, которое должно быть применено для маршрутной информации, удовлетворяющей заданным критериям. Используется только для фильтрации маршрутов протоколов динамической маршрутизации и не имеет действия при конфигурировании PBR.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
action <ACT>
no action
```

Параметры

<ACT> – назначаемое действие:

- permit – прием/анонсирование маршрутной информации разрешено;
- deny – прием/анонсирование маршрутной информации запрещено.

Значение по умолчанию

permit

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action deny
```

action set as-path prepend

Данной командой устанавливается значение атрибута BGP AS-Path, которое будет добавляться в начало списка автономных систем в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set as-path prepend <AS-PATH> [ track <TRACK-ID> ]
no set as-path
```

Параметры

<AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, где каждая часть принимает значения [1..4294967295]. Можно указать до 10 номеров автономных систем.

<TRACK-ID> – идентификатор tracking объекта, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set as-path prepend 100,200,300
```

action set community

Данной командой задается значение атрибута BGP Community, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set community { <COMMUNITY-LIST> | no-advertise | no-export }
no action set community
```

Параметры

<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:N,AS:N, где AS часть принимает значения [0..65535], N часть принимает значения [0..65535]. Можно указать до 64 community;

no-advertise – при указании команды маршруты, которые передаются с данным значением атрибута community, не должны анонсироваться другим BGP-соседям;

no-export – при указании команды маршруты, которые передаются с таким значением атрибута community, не должны анонсироваться за пределы конфедерации (автономная система, которая не является частью конфедерации считается конфедерацией). То есть, маршруты не анонсируются eBGP-соседям, но анонсируются внешним соседям в конфедерации.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set community no-advertise
```

action set extcommunity

Данной командой задается значение атрибута BGP ExtCommunity, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set extcommunity <EXTCOMMUNITY-LIST>
no action set extcommunity
```

Параметры

<EXTCOMMUNITY-LIST> – список community, задаётся в виде KIND:AS:N,KIND:AS:N,KIND:AS:N, где

- KIND – тип extcommunity, принимает значения rt (Route Target) и ro (Route Origin);
- AS – номер автономной системы, принимает значения [1..4294967295];
- N – номер extcommunity, определяющий политику маршрутизации трафика, принимает значения [1..65535].

Можно указать до 64 ExtCommunity.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set extcommunity ro:435:6
```

action set ip bgp-next-hop

Данной командой задается значение атрибута BGP Next-Hop, которое будет установлено в маршруте при анонсировании по BGP.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set ip bgp-next-hop <ADDR>
no action set ip next-hop
```

Параметры

<ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set ip bgp-next-hop 10.100.100.1
```

action set ip next-hop

Данной командой задается значение Next-Hop, которое будет установлено в маршруте, полученном по BGP.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set ip next-hop { <NEXTHOP> | blackhole | unreachable | prohibit }
no action set ip next-hop
```

Параметры

<NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]:

- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13).

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set ip next-hop prohibit
```

action set ip next-hop verify-availability

Данной командой задается Next-Hop для пакетов, которые попадают под критерия в указанном списке доступа (ACL).

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set ip next-hop verify-availability <NEXTHOP> <METRIC> [ track <TRACK-ID> ]
no action set ip next-hop verify-availability { <NEXTHOP> | all }
```

Параметры

<NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

[METRIC] – метрика маршрута, принимает значения [1..255];

<TRACK-ID> – идентификатор tracking объекта, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set ip next-hop verify-availability 1.1.1.1 25
```

action set ipv6 bgp-next-hop

Данной командой задается значение атрибута BGP Next-Hop для IPv6, которое будет установлено в маршруте при анонсировании по BGP.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set ipv6 bgp-next-hop <ADDR>
no action set ipv6 next-hop
```

Параметры

<IPV6-ADDR> – IPv6-адрес шлюза, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set ipv6 bgp-next-hop 2002::765:1
```

action set ipv6 next-hop

Данной командой задается значение Next-Hop для IPv6, которое будет установлено в маршруте, полученном по BGP.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set ipv6 next-hop <NEXTHOP>
no action set ipv6 next-hop
```

Параметры

<NEXTHOP> – IPv6-адрес шлюза, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set ipv6 next-hop 55::205:2
```

action set local-preference

Данной командой задается значение атрибута BGP Local Preference, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set local-preference <PREFERENCE>
no action set local-preference
```

Параметры

<PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [1..2147483647].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set local-preference 120
```

action set metric bgp

Данной командой задается значение атрибута BGP MED, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set metric bgp <METRIC> [ track <TRACK-ID> ]
no action set metric bgp
```

Параметры

<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295];

<TRACK-ID> – идентификатор tracking объекта, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set metric bgp 10
```

action set metric isis

Данной командой задается значение атрибута IS-IS Metric, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set metric isis <METRIC>
no action set metric isis
```

Параметры

<METRIC> – значение атрибута IS-IS Metric, принимает значения [1..16777215].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set metric isis 10
```

action set metric ospf

Данной командой задается значение атрибута OSPF Metric, которое будет установлено в маршруте. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set metric ospf <TYPE> <METRIC>
no action set metric ospf
```

Параметры

<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2;
<METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set metric ospf type-1 10
```

action set metric rip

Данной командой задается значение атрибута RIP Metric, которое будет установлено в маршруте. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set metric rip <METRIC>
no action set metric rip
```

Параметры

<METRIC> – значение атрибута RIP Metric, принимает значения [0..16].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set metric rip 5
```

action set origin

Данной командой задается значение атрибута BGP Origin, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set origin <ORIGIN>
no action set origin
```

Параметры

<ORIGIN> – значение атрибута BGP Origin, принимает следующие значения:

- egp – маршрут выучен по протоколу Exterior Gateway Protocol (EGP);
- igp – маршрут получен внутри исходной автономной системы;
- incomplete – маршрут выучен другим образом.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set origin igp
```

action set tag ospf

Данной командой задается значение атрибута OSPF Tag, которое будет установлено в маршруте.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set tag ospf <TAG>
```

```
no action set tag ospf
```

Параметры

<TAG> – значение атрибута OSPF Tag, принимает значения [0..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set tag ospf 20
```

action set tag rip

Данной командой задается значение атрибута RIP Tag, которое будет установлено в маршруте. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set tag rip <RIP>
no action set tag rip
```

Параметры

<RIP> – значение атрибута RIP Tag, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set tag rip 20
```

action set weight bgp

Данной командой задается значение атрибута BGP weight, которое будет установлено в маршруте. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
action set weight bgp <WEIGHT>
no action set weight bgp
```

Параметры

<WEIGHT> – значение атрибута BGP weight, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# action set weight bgp 200
```

description

Данная команда используется для изменения описания конфигурируемого правила маршрутной карты. Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание правила маршрутной карты, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# description "Drop Local NETs"
```

ip local policy route-map

Данной командой назначается политика маршрутизации на основе списков доступа (ACL). Данная политика маршрутизации работает для пакетов, которые генерирует сам контроллер.

Использование отрицательной формы команды (no) удаляет политику маршрутизации.

Синтаксис

```
ip local policy [vrf <VRF>] route-map <NAME>
no local ip policy [vrf <VRF>] route-map
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра политика маршрутизации будет работать только в определенном VRF;

<NAME> – имя сконфигурированной политики маршрутизации, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip local policy route-map drop-local-net
```

ip policy route-map

Данной командой на интерфейс назначается политика маршрутизации на основе списков доступа (ACL). Данная политика маршрутизации работает для пакетов приходящих через интерфейс, на котором она назначена.

Использование отрицательной формы команды (no) удаляет политику маршрутизации.

Синтаксис

```
ip policy route-map <NAME>
no ip policy route-map
```

Параметры

<NAME> – имя сконфигурированной политики маршрутизации, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

Пример

```
wlc-30(config-subif)# ip policy route-map drop-local-net in
```

match as-path

Данной командой устанавливается значение атрибута BGP AS-Path в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match as-path [ begin | end | contain ] <AS-PATH>
no match as-path
```

Параметры

<AS-PATH> – список номеров автономных систем, задаётся в виде AS,AS,AS, где каждая часть принимает значения [1..4294967295]. Можно указать до 10 номеров автономных систем.

Опциональные параметры, с помощью которых задаётся частичное соответствие атрибута:

- begin – значение атрибута начинается с указанного списка номеров автономных систем;
- end – значение атрибута оканчивается на указанный список номеров автономных систем;
- contain – значение атрибута содержит указанный список номеров автономных систем.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match as-path begin 100,200,300
```

match community

Данной командой устанавливается значение атрибута BGP Community в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match community <COMMUNITY-LIST>
no match community
```

Параметры

<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:,AS, где AS часть принимает значения [0..65535], N часть принимает значения [0..65535]. Можно указать до 64 community.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match community 100:1,200:3,300:65000
```

match extcommunity

Данной командой устанавливается значение атрибута BGP ExtCommunity в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match extcommunity <EXTCOMMUNITY-LIST>
no match extcommunity
```

Параметры

<EXTCOMMUNITY-LIST> – список extcommunity, задаётся в виде KIND:AS:N, KIND:AS:N, KIND:AS:N, где:

- KIND – тип extcommunity, принимает значения rt (Route Target) или ro (Route Origin);
- AS – номер автономной системы, принимает значения [1..4294967295];
- N – номер extcommunity, определяющий политику маршрутизации трафика, принимает значения [1..65535].

Можно указать до 64 extcommunity.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match extcommunity ro:435:6
```

match ip access-group

Данной командой устанавливается ACL-группа, для которой должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip access-group <NAME>
no match ip access-group
```

Параметры

<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ip access-group ACCESS
```

match ip address

Данной командой устанавливается адреса маршрутов, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip address <ADDR/LEN> [ { eq <LEN> | le <LEN> | ge <LEN> [ le <LEN> ] }
no match ip address prefix
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<LEN> – длина префикса, принимает значения [1..32];

eq – при указании команды длина префикса должна соответствовать указанной;

le – при указании команды длина префикса должна быть меньше либо соответствовать указанной;

ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ip address 192.168.0.0/32 ge 16
```

match ip address object-group

Данной командой устанавливается профиль IP-адресов, содержащий значения подсетей назначения в маршруте, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip address object-group <OBJ-GROUP- NETWORK -NAME> [ { eq <LEN> | le <LEN> | ge
<LEN> [ le <LEN> ]
no match ip address object-group
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который должен содержать префиксы подсетей назначения, задаётся строкой до 31 символа;

eq – при указании команды длина префикса должна соответствовать указанной;

le – при указании команды длина префикса должна быть меньше либо соответствовать указанной;

ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ip address object-group local_nets
```

match ip next-hop

Данной командой устанавливается профиль IP-адресов, содержащий значения атрибута BGP Next-Hop в маршруте, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip next-hop object-group <OBJ-GROUP-NETWORK-NAME>
no match ip next-hop
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который должен содержать диапазоны IP-адресов шлюзов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ip next-hop object-group block_nexthop
```

match ip route-source

Командой устанавливается профиль IP-адресов. Профиль содержит IP-адреса контроллера, анонсировавшего маршрут. Используется для фильтрации по IP-адресу источника при анонсировании маршрутной информации.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip route-source object-group <OBJ-GROUP-NETWORK-NAME>
no match ip route-source
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который должен содержать диапазоны IP-адресов источника маршрутной информации, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ip route-source object-group source_routers
```

match ipv6 address

Данной командой устанавливается адреса IPv6-маршрутов, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ipv6 address <IPV6-ADDR/LEN> [ { eq <LEN> | le <LEN> | ge <LEN> [ le <LEN> ] }
no match ipv6 address prefix
```

Параметры

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<LEN> – длина префикса, принимает значения [1..128];

eq – при указании команды длина префикса должна соответствовать указанной;

le – при указании команды длина префикса должна быть меньше либо соответствовать указанной;

ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ipv6 address FF02:0:0:0:0:1:FF00::/104
```

match ipv6 address object-group

Данной командой устанавливается профиль IPv6-адресов, содержащий значения подсетей назначения в маршруте, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ipv6 address object-group <OBJ-GROUP- NETWORK -NAME> [ { eq <LEN> | le <LEN> | ge <LEN> [ le <LEN> ]
no match ipv6 address object-group
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IPv6-адресов, который должен содержать префиксы подсетей назначения, задаётся строкой до 31 символа;

eq – при указании команды длина префикса должна соответствовать указанной;

le – при указании команды длина префикса должна быть меньше либо соответствовать указанной;

ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ipv6 address object-group local_nets
```

match ipv6 next-hop

Данной командой устанавливается профиль IPv6-адресов, содержащий значения атрибута BGP Next-Hop в маршруте, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ipv6 next-hop object-group <OBJ-GROUP-NETWORK-NAME>
no match ipv6 next-hop
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IPv6-адресов, который должен содержать диапазоны IPv6-адресов шлюзов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ipv6 next-hop object-group block_nexthop
```

match ipv6 route-source

Командой устанавливается профиль IPv6-адресов. Профиль содержит IPv6-адреса контроллера, анонсировавшего маршрут. Используется для фильтрации по IPv6-адресу источника при анонсировании маршрутной информации.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ipv6 route-source object-group <OBJ-GROUP-NETWORK-NAME>
no match ipv6 route-source
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IPv6-адресов, который должен содержать диапазоны IPv6-адресов источника маршрутной информации, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match ipv6 route-source object-group source_routers
```

match metric bgp

Данной командой устанавливается значение атрибута BGP MED в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match metric bgp <METRIC>
```

```
no match metric bgp
```

Параметры

<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match metric bgp 10
```

match metric ospf

Данной командой устанавливается значение атрибута OSPF Metric в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match metric ospf <TYPE> <METRIC>
no match metric ospf
```

Параметры

<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2.

<METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match metric ospf type-1 10
```

match metric rip

Данной командой устанавливается значение атрибута RIP Metric в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match metric rip <METRIC>
no match metric rip
```

Параметры

<METRIC> – значение атрибута RIP Metric, принимает значения [0..16].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match metric rip 5
```

match tag ospf

Данной командой устанавливается значение атрибута OSPF Tag в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match tag ospf <TAG>
no match tag ospf
```

Параметры

<TAG> – значение атрибута OSPF Tag, принимает значения [0..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match tag ospf 20
```

match tag rip

Данной командой устанавливается значение атрибута RIP Tag в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match set tag rip <RIP>
no match set tag rip
```

Параметры

<RIP> – значение атрибута RIP Tag, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match tag rip 20
```

match weight bgp

Данной командой устанавливается значение атрибута BGP weight в маршруте, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match weight bgp <WEIGHT>
no match weight bgp
```

Параметры

<WEIGHT> – значение атрибута BGP weight, принимает значения [0..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP-RULE

Пример

```
wlc-30(config-route-map-rule)# match bgp weight 20
```

route-map

Командой добавляется фильтрация и модификация маршрутов во входящих или исходящих направлениях.

Использование отрицательной формы команды (no) отключает фильтрацию и модификацию маршрутов в соответствующем направлении.

Синтаксис

```
route-map <NAME> <DIRECTION>
no route-map <DIRECTION>
```

Параметры

<NAME> – имя сконфигурированной маршрутной карты, задаётся строкой до 31 символа;

<DIRECTION> – направление:

- in – фильтрация и модификация получаемых маршрутов;
- out – фильтрация и модификация анонсируемых маршрутов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

CONFIG-OSPF

CONFIG-OSPFV3

CONFIG-ISIS

CONFIG-RIP

CONFIG-RIPND

Пример

```
wlc-30(config-bgp-neighbor-family)# route-map drop-local-net in
```

route-map

Данной командой создается маршрутная карта, которая в дальнейшем будет использоваться для фильтрации и модификации анонсируемых и получаемых IP-маршрутов, и осуществляется переход в режим настройки параметров маршрутной карты.

Использование отрицательной формы команды (no) удаляет маршрутную карту.

Синтаксис

```
[no] route-map <NAME>
```

Параметры

<NAME> – имя конфигурируемой маршрутной карты, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# route-map drop-local-net
wlc-30(config-route-map)#
```

rule

Данной командой создается правило маршрутной карты с определённым номером и осуществляется переход в режим настройки параметров правила. Правила обрабатываются устройством в порядке возрастания номеров правил.

Использование отрицательной формы команды (no) удаляет правило по номеру либо все правила.

Синтаксис

```
[no] rule <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1 .. 10000].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ROUTE-MAP

Пример

```
wlc-30(config-route-map)# rule 2
wlc-30(config-route-map-rule)#
```

show ip route-map

Данная команда используется для просмотра маршрутных карт.

Синтаксис

```
show ip route-map <NAME> [ <ORDER> ]
```

Параметры

<NAME> – имя маршрутной карты, задаётся строкой до 31 символа;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будет показана информация только по данному правилу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip route-map drop-local-net
Order:                                  2
Description:                            Drop route to private nets
Matching pattern:
    Access group                            --
    AS path                                 --
    Community                               --
    Extcommunity                            --
    BGP metric (MED):                       --
    Address (object-group):                 local_net
    Next hop (object-group):                --
    Route source (object-group):            --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
Actions:
    Decision:                               Deny
    Route next hop address:                 --
    Route IPv6 next hop address:            --
    Route next hop:                         --
    AS path (prepand):                      --
    Community:                              --
    Extcommunity:                           --
    Local preference:                       --
    BGP next hop address:                   --
    BGP IPv6 next hop address:              --
    BGP metric (MED):                       --
    Origin:                                 --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
```

Настройка связок ключей

- accept-lifetime
- key
- key-chain
- key-string
- send-lifetime

accept-lifetime

Данная команда определяет период времени, в течение которого данный ключ может использоваться для аутентификации принятых пакетов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
accept-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>
no accept-lifetime
```

Параметры

<TIME_B> – устанавливаемое время начала использования ключа, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

<DAY_B> – день месяца начала использования ключа, принимает значения [1..31];

<MONTH_B> – месяц начала использования ключа, принимает значения:

- January;
- February;
- March;
- April;
- May;
- June;
- July;
- August;
- September;
- October;
- November;
- December.

<YEAR_B> – год начала использования ключа, принимает значения [2001..2037];

<TIME_E> – устанавливаемое время окончания использования ключа, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

<DAY_E> – день месяца окончания использования ключа, принимает значения [1..31];

<MONTH_E> – месяц окончания использования ключа, принимает значения:

- January;
- February;
- March;
- April;

- May;
- June;
- July;
- August;
- September;
- October;
- November;
- December.

<YEAR_E> – год окончания использования ключа, принимает значения [2001..2037].

Значение по умолчанию

Ключ действителен постоянно.

Необходимый уровень привилегий

15

Командный режим

CONFIG-KEYCHAIN-KEY

Пример

```
wlc-30(config-keychain-key)# accept-lifetime 16:35:00 10 May 2015 16:35:00 10 June 2021
```

key

Данной командой добавляется ключ в связку ключей и осуществляется переход в режим настройки параметров ключа.

Использование отрицательной формы команды (no) удаляет указанный ключ.

Синтаксис

```
[no] key <ID>
```

Параметры

<ID> – идентификатор ключа, задается в диапазоне [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-KEYCHAIN

Пример

```
wlc-30(config-keychain)# key 25
```

key-chain

Командой добавляется связка ключей в систему и осуществляется переход в режим настройки параметров связки ключей.

Использование отрицательной формы команды (no) удаляет указанный список.

Синтаксис

```
[no] key-chain <KEYCHAIN>
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, строка до 16 ASCII символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# key-chain lock
```

key-string

Данной командой устанавливается пароль для аутентификации.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
key-string ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no key-string
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;
<ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-KEYCHAIN-KEY

Пример

```
wlc-30(config-keychain-key)# key-string ascii-text 123456789
wlc-30(config-keychain-key)# key-string ascii-text encrypted CDE65039E5591FA3F1
```

send-lifetime

Данная команда определяет период времени, в течение которого данный ключ может использоваться для аутентификации при отправке пакетов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
send-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>
no send-lifetime
```

Параметры

<TIME_B> – устанавливаемое время начала использования ключа, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

<DAY_B> – день месяца начала использования ключа, принимает значения [1..31];

<MONTH_B> – месяц начала использования ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December];

<YEAR_B> – год начала использования ключа, принимает значения [2001..2037];

<TIME_E> – устанавливаемое время окончания использования ключа, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

<DAY_E> – день месяца окончания использования ключа, принимает значения [1..31];

<MONTH_E> – месяц окончания использования ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December];

<YEAR_E> – год окончания использования ключа, принимает значения [2001..2037].

Значение по умолчанию

Ключ действителен постоянно.

Необходимый уровень привилегий

15

Командный режим

CONFIG-KEYCHAIN-KEY

Пример

```
wlc-30(config-keychain-key)# send-lifetime 16:35:00 15 May 2014 16:35:00 21 June 2018
```

Настройка протокола BFD

- bfd-enable
- ip bfd idle-tx-interval
- ip bfd log-adjacency-changes
- ip bfd min-rx-interval
- ip bfd min-tx-interval
- ip bfd multiplier
- ip bfd neighbor
- ip bfd passive
- ip ospf bfd-enable
- ipv6 bfd log-adjacency-changes
- ipv6 bfd neighbor
- ipv6 ospf bfd-enable
- show ip bfd

bfd-enable

Данной командой включается BFD-протокол на конфигурируемом BGP-соседе.

Использование отрицательной формы команды (no) отключает BFD-протокол.

Синтаксис

```
[no] bfd-enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# bfd-enable
```

ip bfd idle-tx-interval

Данной командой задаётся интервал, по истечении которого происходит отправка BFD-сообщения соседу. Данный параметр служит для уменьшения числа генерируемых сообщений для тех случаев, когда BFD-сосед недоступен или на нем выключен протокол BFD.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip bfd idle-tx-interval <TIMEOUT>
no ip bfd idle-tx-interval
```

Параметры

<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [300..65535].

Значение по умолчанию

1 секунда

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config)# ip bfd idle-tx-interval 4000
```

ip bfd log-adjacency-changes

Данной командой включается логирование изменений состояния BFD-протокола.

Использование отрицательной формы команды (no) отключает логирование изменений состояния BFD-протокола.

Синтаксис

```
ip bfd log-adjacency-changes
no ip bfd log-adjacency-changes
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip bfd log-adjacency-changes
```

ip bfd min-rx-interval

Данной командой задаётся минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Данный параметр анонсируется соседу.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip bfd min-rx-interval <TIMEOUT>
no ip bfd min-rx-interval
```

Параметры

<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [300..65535].

Значение по умолчанию

300 мс

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config)# ip bfd min-rx-interval 1000
```

ip bfd min-tx-interval

Данной командой задаётся минимальный интервал, по истечении которого происходит отправка BFD сообщения соседу. Данный параметр используется только когда BFD-сессия активна, в иных случаях используется ip bfd idle-tx-interval.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip bfd min-tx-interval <TIMEOUT>
no ip bfd min-tx-interval
```

Параметры

<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседу, принимает значение в миллисекундах в диапазоне [300..65535].

Значение по умолчанию

300 мс

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config)# ip bfd min-tx-interval 1000
```

ip bfd multiplier

Данной командой задаётся число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Время обнаружения недоступности в каждом из направлений рассчитывается из данного числа умноженного на tx/rx интервал.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip bfd multiplier <COUNT>`

`no ip multiplier`

Параметры

<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config)# ip bfd multiplier 10
```

ip bfd neighbor

Данной командой запускается работа механизма BFD с определенным IP-адресом. Работа такого механизма необходима для удаления статических маршрутов из таблицы маршрутизации при недоступности next-hop (ключ bfd команды ip route. см. раздел ip route)

Использование отрицательной формы команды (no) останавливает работа механизма BFD с определенным IP-адресом.

Синтаксис

```
ip bfd neighbor <ADDR> [ { interface <IF> | tunnel <TUN> } ] [ local-address <ADDR>
[ multihop ] ] [ vrf <VRF> ]
```

```
no ip bfd neighbor <ADDR> [vrf <VRF>]
```

Параметры

<ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip bfd neighbor 192.168.0.2
```

ip bfd passive

Данной командой BFD-сессия переводится в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ip bfd passive
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Активный режим.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

Пример

```
wlc-30(config)# ip bfd passive
```

ip ospf bfd-enable

Данной командой на интерфейсе включается протокол BFD для протокола OSPF.

Использование отрицательной формы команды (no), на интерфейсе отключается протокол BFD для протокола OSPF.

Синтаксис

```
[no] ip ospf bfd-enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Протокол BFD для протокола OSPF отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LOOPBACK

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf bfd-enable
```

ipv6 bfd log-adjacency-changes

Данной командой включается логирование изменений состояния IPv6 BFD-протокола.

Использование отрицательной формы команды (no) отключает логирование изменений состояния IPv6 BFD-протокола.

Синтаксис

```
ipv6 bfd log-adjacency-changes
no ipv6 bfd log-adjacency-changes
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Логирование выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 bfd log-adjacency-changes
```

ipv6 bfd neighbor

Данной командой запускается работа механизма BFD с определенным IPv6-адресом. Работа такого механизма необходима для удаления bgp-маршрутов из таблицы маршрутизации при недоступности next-hop.

Использование отрицательной формы команды (no) останавливает работа механизма BFD с определенным IPv6-адресом.

Синтаксис

```
ipv6 bfd neighbor <IPV6-ADDR> [ interface <IF> ] [ local-address <IPV6-ADDR>
[ multihop ] ] [ vrf <VRF> ]
```

```
no ipv6 bfd neighbor <IPV6-ADDR> [ vrf <VRF> ]
```

Параметры

<IPV6-ADDR> IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 bfd neighbor FF02:0:0:0:0:1:FF00::/104
```

ipv6 ospf bfd-enable

Данной командой на интерфейсе включается протокол BFD для протокола OSPFv3.

Использование отрицательной формы команды (no), на интерфейсе отключается протокол BFD для протокола OSPFv3.

Синтаксис

```
[no] ipv6 ospf bfd-enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Протокол BFD для протокола OSPF отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf bfd-enable
```

show ip bfd

Данная команда отображает информацию о параметрах BFD-протокола или определенных интерфейсов при использовании фильтра.

Синтаксис

```
show ip bfd [ { interface <IF> | tunnel <TUN> } ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip bfd
Minimum RX interval: 200 ms
Minimum TX interval: 200 ms
Idle TX interval:    1000 ms
Multiplier:          5 packets
Passive:             No
wlc-30# show ip bfd interface gi1/0/1
Minimum RX interval: 200 ms
Minimum TX interval: 200 ms
Idle TX interval:    1000 ms
Multiplier:          10 packets
Passive:             Yes
```

Настройка статических маршрутов IPv4/IPv6

- ip route
- ipv6 route

ip route

Команда позволяет создать статический IP-маршрут к указанной подсети.

Использование отрицательной формы команды (no) удаляет указанный маршрут.

Синтаксис

```
ip route [ vrf <VRF> ] <SUBNET> { { <NEXTHOP> [ resolve ] [ bfd ] | interface <IF> |
tunnel <TUN> | blackhole | unreachable | prohibit } [ track <TRACK-ID> ]
[ name <NAME>] } | wan load-balance rule <RULE> } [ <METRIC> ]
no ip route [ vrf <VRF> ] <SUBNET> [ <METRIC> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<SUBNET> – адрес назначения, может быть задан в следующих видах:

- AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
- AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].

<NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

resolve – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;

<IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<RULE> – номер правила wan, задаётся в диапазоне [1..50];

blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;

unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);

prohibit – при указании команды, пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);

<METRIC> – метрика маршрута, принимает значения [0..255];

<TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте;

<NAME> – имя (описание) маршрута, текстовая переменная длинной до 31 символа;

bfd – при указании данного ключа, активируется удаление статического маршрута в случае недоступности next-hop. Для работы данного механизма должен быть запущен механизм BFD с IP-адресом next-hop (см. раздел ip bfd neighbor);

проверка next-hop при помощи протокола bfd. В случае недоступности next-hop маршрут удаляется.

⚠ Если в качестве подсети указать 0.0.0.0/0, то будет задан маршрут по умолчанию.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример 1

Задать маршрут до подсети 192.165.3.0/24 с метрикой 6 через шлюз 192.165.56.65:

```
wlc-30(config)# ip route 192.165.3.0/24 192.165.56.65 6
```

Пример 2

Задать маршрут до подсети 192.165.3.0/24 с метрикой 6 через интерфейс GigabitEthernet 1/0/5:

```
wlc-30(config)# ip route 192.165.3.0/24 interface gigabitethernet 1/0/5 6
```

Пример 3

Задать маршрут до подсети 192.165.3.0/24 через туннельный интерфейс vti 1:

```
wlc-30(config)# ip route 192.165.3.0/24 interface vti 1
```

ipv6 route

Данная команда позволяет создать статический IPv6-маршрут к указанной подсети.

Использование отрицательной формы команды (no) удаляет указанный маршрут.

Синтаксис

```
ipv6 route [ vrf <VRF> ] <SUBNET> { { <NEXTHOP> [ resolve ] [bfd] | interface <IF> |
blackhole | unreachable | prohibit [ <METRIC> ] [ name <NAME>] }
| wan load-balance rule <RULE> [ <METRIC> ] }
```

```
no ipv6 route [ vrf <VRF> ] <SUBNET> [ <METRIC> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

<SUBNET> – адрес назначения, может быть задан в следующих видах:

- X:X:X:X::X – IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
- X:X:X:X::X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

<NEXTHOP> – IPv6-адрес шлюза, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

resolve – при указании данного параметра IPv6-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;

<IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;

unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);

prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);

[METRIC] – метрика маршрута, принимает значения [0..255];

<NAME> – имя (описание) маршрута, текстовая переменная длинной до 31 символа;

bfd – при указании данного ключа, активируется проверка next-hop при помощи протокола bfd. В случае недоступности next-hop маршрут удаляется.

⚠ Если в качестве подсети указать ::/0, то будет задан маршрут по умолчанию.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример 1

Задать маршрут до подсети 2001::/120 с метрикой 6 через шлюз fc00::1:

```
wlc-30(config)# ipv6 route 2001::/120 fc00::1 6
```

Пример 2

Задать маршрут до подсети 2001::/120 с метрикой 6 через интерфейс GigabitEthernet 1/0/5:

```
wlc-30(config)# ipv6 route 2001::/120 interface gigabitethernet 1/0/5  6
```

Пример 3

Задать маршрут до подсети 2001::/120 через туннельный интерфейс vti 1:

```
wlc-30(config)# ipv6 route 2001::/120 interface vti 1
```

Настройка протокола BGP

- address-family
- address-family
- allow-local-as
- clear bgp
- cluster-id
- default-originate
- description
- ebgp-multihop
- flow-spec enable
- ipv6 router bgp log-neighbor-changes
- ipv6 router bgp maximum-paths
- neighbor
- next-hop-self
- peer-group
- peer-group
- preference
- remote-as
- remove-private-as
- router bgp
- router bgp log-neighbor-changes
- router bgp maximum-paths
- route-reflector-client
- router-id
- send-community extended
- show bgp flow-spec
- show bgp ipv4 unicast
- show bgp ipv6 unicast
- show bgp l2vpn vpls
- show bgp neighbors
- show bgp summary
- show bgp vpnv4 unicast
- timers error-wait
- timers holdtime
- timers keepalive
- update-source
- vrf
- weight

address-family

Данной командой осуществляется переход в режим настройки параметров передачи информации протоколов для процесса BGP.

Использование отрицательной формы команды (no) удаляет настроенные параметры передачи информации протоколов.

Синтаксис:

```
[no] address-family { ipv4 | ipv6 } unicast
```

Параметры:

- ipv4 – семейство ipv4;

- ipv6 – семейство ipv6.

Необходимый уровень привилегий:

10

Командный режим

CONFIG-BGP

CONFIG-BGP-VRF

Пример

```
wlc-30(config-bgp)# address-family ipv4
```

address-family

Данной командой определяется тип конфигурируемой маршрутной информации и переход в данный режим настройки.

Использование отрицательной формы команды (no) удаляет настроенные параметры передачи информации протоколов.

Синтаксис:

```
[no] address-family { ipv4 | ipv6 | vpnv4 | l2vpn vpls } unicast
```

Параметры:

- ipv4 – семейство ipv4;
- ipv6 – семейство ipv6;
- vpnv4 – семейство vpnv4;
- l2vpn vpls – семейство l2vpn.

Необходимый уровень привилегий:

10

Командный режим:

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# address-family ipv4
```

allow-local-as

Данной командой задается режим, в котором разрешен приём маршрутов в BGP-атрибуте, AS Path которых содержатся номера автономной системы процесса.

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
allow-local-as <NUMBER>
no allow-local-as
```

Параметры

<NUMBER> – пороговое число вхождений номера автономной системы процесса в атрибуте AS Path, при которых маршрут будет принят, диапазон допустимых значений [1..10].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# allow-local-as
```

clear bgp

Данная команда сбрасывает все или определенный BGP-процесс.

Синтаксис

```
clear bgp [ <AS> ] [ vrf <NAME_VRF> ] [ neighbor { <ADDR> | <IPV6_ADDR> } ]
```

Параметры

<AS> – номер автономной системы, принимает значения [1..4294967295];

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6_ADDR> – IPv6-адрес соседа, задается в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF];

<NAME-VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будут сброшены сессии протокол BGP.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear bgp
wlc-30# clear bgp 1000
```

cluster-id

Командой устанавливается идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс контроллера.

Использование отрицательной формы команды (no) удаляет идентификатор.

Синтаксис

`cluster-id <ID>`

`no cluster-id`

Параметры

<ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-BGP-VRF

Пример

```
wlc-30(config-bgp-af)# cluster-id 1.1.1.1
```

default-originate

Данной командой задается режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами отправляется маршрут по умолчанию.

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
[no] default-originate
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-neighbor)# default-originate
```

description

Данной командой определяется описание соседа.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание соседа, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# description "ISP_RTK"
```

ebgp-multihop

Данной командой разрешается подключение к соседям, которые находятся в не напрямую подключенных подсетях.

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
[no] ebgp-multihop <NUM>
```

Параметры

<NUM> – максимальное количество хопов при установке EBGP (используется для TTL).

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-NEIGHBOR

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# ebgp-multihop
```

flow-spec enable

Данной командой устанавливается режим трансляции flow-spec информации при работе с BGP-соседом или группой BGP-соседей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] flow-spec enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-group)# flow-spec enable
```

ipv6 router bgp log-neighbor-changes

Данной командой включается логирование изменений состояния IPv6-BGP-соседей.

Использование отрицательной формы команды (no) отключает логирование изменений состояния IPv6-BGP-соседей.

Синтаксис

```
[no] ipv6 router bgp log-neighbor-changes
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 router bgp log-neighbor-changes
```

ipv6 router bgp maximum-paths

Данной командой включается ECMP и определяется максимальное количество равноценных IPv6-маршрутов до цели.

Использование отрицательной формы команды (no) отключает ECMP.

Синтаксис

`ipv6 router bgp maximum-paths <VALUE>`

`no ipv6 router bgp maximum-paths`

Параметры

<VALUE> – количество допустимых равноценных IPv6-маршрутов до цели, принимает значения [1..16].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 router bgp maximum-paths 14
```

neighbor

Данной командой добавляется BGP-сосед и осуществляется переход в режим настройки параметров BGP-соседа. Использование отрицательной формы команды (no) удаляет параметры соседнего контроллера из конфигурации.

Синтаксис

`[no] neighbor {<ADDR> |<IPV6-ADDR>}`

Параметры

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-VRF-BGP

Пример

```
wlc-30(config-bgp)# neighbor 192.168.0.2
wlc-30(config-bgp-neighbor)#
```

next-hop-self

Данной командой задается режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального контроллера.

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
[no] next-hop-self
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-neighbor-af)# next-hop-self
```

peer-group

Данной командой создается группа BGP-соседей с заданным именем и осуществляется переход в режим конфигурирования параметров группы.

Использование отрицательной формы команды (no) удаляет BGP-группу с заданным именем.

Синтаксис

```
[no] peer-group <NAME>
```

Параметры

<NAME> – название группы, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-BGP-VRF

Пример

```
wlc-30(config-bgp)# peer-group list1
```

peer-group

Данной командой к BGP-группе или BGP-соседу применяются настройки описанные в заданной BGP-группе.

Использование отрицательной формы команды (no) отменяет применение настроек описанных в заданной BGP-группе.

Синтаксис

```
peer-group <NAME>
no peer-group
```

Параметры

<NAME> – название группы, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-af)# peer-group list1
```

preference

Данная команда определяет приоритетность маршрутов, получаемых от соседа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
preference <VALUE>
no preference
```

Параметры

<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255].

Значение по умолчанию

170

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-neighbor)# preference 30
```

remote-as

Данной командой устанавливается номер автономной системы BGP-соседа.

Использование отрицательной формы команды (no) удаляет номер автономной системы.

Синтаксис

```
remote-as <AS>
no remote-as
```

Параметры

<AS> – номер автономной системы, принимает значения [1..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# remote-as 20
```

remove-private-as

Данной командой задается режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996).

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
[no] remove-private-as <ACTION>
```

Параметры

<ACTION> – действие указывающее на то, какие приватные AS должны быть удалены или заменены. Принимает одно из значений:

- all – удалить все включения приватных AS из оригинального AS path;
- nearest – удалить все приватные AS до последней (правой) публичной AS в оригинальном AS path;
- replace – заменить все приватные AS на номер AS в процессе которого обрабатывается данная команда.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-neighbor-af)# remove-private-as
```

router bgp

Данной командой добавляется BGP-процесс в систему и осуществляется переход в режим настройки параметров BGP-процесса.

Использование отрицательной формы команды (no) удаляет BGP-процесс из системы.

Синтаксис

```
[no] router bgp <AS>
```

Параметры

<AS> – номер автономной системы процесса, принимает значения [1..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router bgp 1000
wlc-30(config-bgp)#
```

Добавлен BGP-процесс с автономной системой 1000.

router bgp log-neighbor-changes

Данной командой включается логирование изменений состояния BGP-соседей.

Использование отрицательной формы команды (no) отключает логирование изменений состояния BGP-соседей.

Синтаксис

```
[no] router bgp log-neighbor-changes
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router bgp log-neighbor-changes
```

router bgp maximum-paths

Данной командой включается ECMP и определяется максимальное количество равноценных маршрутов до цели.

Использование отрицательной формы команды (no) отключает ECMP.

Синтаксис

```
router bgp maximum-paths <VALUE>
no router bgp maximum-paths
```

Параметры

<VALUE> – количество допустимых равноценных маршрутов до цели, принимает значения [1..16].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router bgp maximum-paths 14
```

route-reflector-client

Данной командой указывается, что BGP-сосед является Route-Reflector клиентом.

Использование отрицательной формы команды (no) отключает данную функцию.

Синтаксис

```
[no] route-reflector-client
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# route-reflector-client
```

router-id

Данной командой устанавливается идентификатор контроллера.

Использование отрицательной формы команды (no) удаляет идентификатор.

Синтаксис

```
router-id <ID>
no router-id
```

Параметры

<ID> – идентификатор контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-BGP-VRF

Пример

```
wlc-30(config-bgp-af)# router-id 1.1.1.1
```

send-community extended

Включает отправку параметра extended community в отсылаемых соседу анонсах. По умолчанию параметры extended community удаляются из отправляемых анонсов. Для корректной работы VPNv4/ L2VPN отправку extended community необходимо включать.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] send-community extended
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Значение по умолчанию

Запрещено.

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR-FAMILY

CONFIG-BGP-VRF-NEIGHBOR-FAMILY

Пример

```
wlc-30(config-bgp-neighbor-af)# send-community extended
```

show bgp flow-spec

Данная команда отображает информацию о правилах flow-spec.

Синтаксис

```
show bgp [ vrf <VRF-NAME> ] flow-spec [ neighbor <ADDR> ] [ instance <AS-NUM> ]
```

Параметры

<AS-NUM> – номер автономной системы процесса, принимает значения [1..4294967295];

<ADDR> – IP-адрес, который задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<VRF-NAME> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show bgp flow-spec
-------------------------------------------------------------------------------
Destination Prefix: 192.168.54.2/32
IP Protocol:        17
Ext-community type: traffic-rate (0x8006)
```

show bgp ipv4 unicast

Данная команда отображает таблицу маршрутизации BGP или детальную информацию об определенном маршруте при использовании фильтров.

Синтаксис

```
show bgp [ vrf <VRF-NAME> ] ipv4 unicast [ { <IP-ADDR> | <IP-ADDR/LEN> } ] [ instance
<AS-NUM> ] [ neighbor <IP-ADDR> [ { advertise-routes | routes } ] ]
```

Параметры

<AS-NUM> – номер автономной системы процесса, принимает значения [1..4294967295];

<IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IP-ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

<VRF-NAME> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации;

routes – при указании команды отображается маршрутная информация, полученная от соседа;

advertise-routes – при указании команды отображается маршрутная информация, объявленная соседу.

Данная команда отображает таблицу маршрутизации BGP или детальную информацию об определенном маршруте при использовании фильтров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show bgp ipv4 unicast
Status codes: u - unicast, b - broadcast, m - multicast a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network              Next Hop             Metric  LocPrf  Path
*> u 10.0.10.0/24         10.115.0.1                   100      i
*> u 0.0.0.0/0            10.115.0.1                   100      i
*  u 14.0.10.0/24         10.115.0.1                   100      i
```

Пример 2

```
wlc-30# show bgp ipv4 unicast 75.0.0.0
75.0.0.0/24        via 115.0.0.40 on gi1/0/14        [bgp20 2000-01-15] (AS90?)
    Administrative Distance: 68
    Type:                    unicast
    Origin:                  Incomplete
    AS PATH:                 1 30 70 90
    Next Hop:                115.0.0.40
    MED:                     0
    Local Preference:        100
    Community:               (1:555)
    Valid, Best
```

show bgp ipv6 unicast

Данная команда отображает таблицу маршрутизации BGP или детальную информацию об определенном маршруте при использовании фильтров.

Синтаксис

```
show bgp [ vrf <VRF-NAME> ] ipv6 unicast [ { <IPV6-ADDR> | <IPV6-ADDR/LEN> } ] [ instance <AS-NUM> ] [ neighbor <IPV6-ADDR> [ { advertise-routes | routes } ] ]
```

Параметры

<AS-NUM> – номер автономной системы процесса, принимает значения [1..4294967295];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<IPV6-ADDR/LEN> – подсеть, задаётся в виде X:X:X:X::X/EE, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF],EE принимает значения [1..128];

<VRF-NAME> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации;

routes – при указании команды отображается маршрутная информация, полученная от соседа;

advertise-routes – при указании команды отображается маршрутная информация, объявленная соседу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30#  show bgp ipv6 unicast
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network              Next Hop             Metric  LocPrf      Weight Path
*> u 2600:380:180::/41    fc00:0:1409:2800::1  --      100         0      65054 12389 3356 ...
i
*> u 2804:2404:8000::/34  fc00:0:1409:2800::1  --      100         0      65054 12389
266925 ... i
*> u 2400:3800:8800::/37  fc00:0:1409:2800::1  --      100         0      65054 12389 2497 ...
i
*> u 2400:54c0:c0::/44    fc00:0:1409:2800::1  --      100         0      65054 12389 3356 ...
i
```

Пример 2

```
wlc-30# show bgp ipv6 unicast 2600:380:180::/41
2600:380:180::/41  via fc00:0:1409:2800::1 on gi1/0/1.2800 [bgp65514 14:08:30] (20057i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    AS PATH:                 65054 12389 3356 7018 20057
    Next Hop:                fc00:0:1409:2800::1 (fe80::aaf9:4bff:feaa:2dd5)
    Local Preference:        100
    Community:               (3356:3) (3356:22) (3356:86) (3356:575) (3356:666) (3356:903)
(3356:2059)
                             (12389:6)
    Weight:                  0
    Valid, Best
```

show bgp l2vpn vpls

Данная команда отображает информацию о всех принятых l2vpn-маршрутах.

Синтаксис

```
show bgp l2vpn vpls { all | rd <ASN:nn> } [ neighbor <ADDR> { advertise-routes | routes ]
[ ve-id <ID> block-offset <ID> ]
```

Параметры

- all – при указании команды all отображается полная информация l2vpn-маршрутов;
- rd – при указании команды rd отображается информация о маршрутах с заданным RD;
- routes – при указании команды отображается маршрутная информация, полученная от соседа;
- advertise-routes – при указании команды отображается маршрутная информация, объявленная соседу;
- <RD> – значение Route distinguisher, задается в одном из следующем виде:

  - <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535];
  - <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535];
  - <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].
- <IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- <ID> – принимает значение [1..65535], задает идентификатор vpls edge или block-offset.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30-R# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>i   65502:100             3     1     8     192.168.9.9         --         100        0
i
*>    65502:102             2     1     10    --                  --         --         --
*>    65502:100             2     1     10    --                  --         --         --
*>i   65502:102             1     1     10    192.168.7.7         --         100        0
i
*>i   65502:100             1     1     10    192.168.7.7         --         100        0
i
```

show bgp neighbors

Данная команда отображает информацию о всех или о выбранном BGP-пире.

Синтаксис

```
show bgp [vrf <VRF-NAME>] neighbors [instance <AS-NUM> ] { <ADDR> | <IPV6-ADDR> }
```

Параметры

<AS-NUM> – номер автономной системы процесса, принимает значения [1..4294967295];

<VRF-NAME> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации;

<ADDR> – IP- или IPv6-адрес пира, который задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] , или в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<IPV6-ADDR/LEN> – подсеть, задаётся в виде X:X:X:X::X/EE, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF],EE принимает значения [1..128].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show bgp instance 20
BGP neighbor is 10.115.0.1
    BGP state:        Established
    Neighbor address: 10.115.0.1
    Neighbor AS:      20
    Neighbor ID:      115.0.0.1
    Neighbor caps:    refresh restart-aware AS4
    Session:          internal multihop AS4
    Source address:   10.115.0.2
    Hold timer:       137/180
    Keepalive timer:  10/60
   Incoming prefix-list: from_ISP
    Outgoing prefix-list: to_ISP
    Incoming route-map:   comingS
    Outgoing route-map:   AS_prepend
    Uptime:               12 s
    BFD address:          192.168.1.2
    BFD state:            Up
    BFD interval:         3.000 s
    BFD timeout:          15.000 s
```

Пример 2

```
wlc-30#  show bgp neighbors 100.64.28.1
BGP neighbor is 100.64.28.1
    BGP state:                        Established
    Neighbor address:                 100.64.28.1
    Neighbor AS:                      65054
    Neighbor ID:                      5.5.0.111
    Neighbor caps:                    refresh enhanced-refresh restart-aware AS4
    Session:                          external AS4
    Source address:                   100.64.28.160
    Weight:                           0
    Hold timer:                       165/180
    Keepalive timer:                  38/60
    RR client:                        No
    Address family ipv4 unicast:
      Default originate:              No
      Default information originate: No
      Outgoing route-map:             RouteMap_out
      Preference:                     170
      Remove private AS:              No
      Next-hop self:                  No
    Uptime:                           12952 s
```

Пример 3

```
wlc-30# show bgp neighbors fc00:0:1409:2800::1
BGP neighbor is fc00:0:1409:2800::1
    BGP state:                        Established
    Neighbor address:                 fc00:0:1409:2800::1
    Neighbor AS:                      65054
    Neighbor ID:                      5.5.0.111
    Neighbor caps:                    refresh enhanced-refresh restart-aware AS4
    Session:                          external AS4
    Source address:                   fc00:0:1409:2800::16
    Weight:                           0
    Hold timer:                       174/180
    Keepalive timer:                  50/60
    RR client:                        No
    Address family ipv6 unicast:
      Default originate:              No
      Default information originate: No
      Incoming route-map:             RouteMap_in
      Outgoing route-map:             RouteMap_out
      Preference:                     170
      Remove private AS:              No
      Next-hop self:                  No
    Uptime:                           13003 s
```

show bgp summary

Данная команда отображает информацию о состоянии соединений с BGP-пирами.

Синтаксис

```
show bgp [vrf <VRF-NAME>] summary [instance <AS-NUM>]
```

Параметры

<AS-NUM> – номер автономной системы процесса, принимает значения [1..4294967295];

<VRF-NAME> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show bgp summary
Tue Sep 14 15:36:26 2021
  BGP router identifier 100.64.28.160, local AS number 65514
  BGP activity 984813/0 prefixes
  Neighbor                AS              MsgRcvd      MsgSent      Up/Down      St/PfxRcd
  ----------------------  --------------  -----------  -----------  -----------  ------------
  10.20.0.2               65058           0            0            01:28:02     Idle
  100.64.28.1             65054           861119       102          01:27:56     855897
```

show bgp vpnv4 unicast

Данная команда отображает информацию о vpnv4-маршрутах. Указание префикса в команде отображает детальную информацию по префиксу.

Синтаксис

```
show bgp vpnv4 unicast { all | rd <RD> | vrf <NAME_VRF> } [ neighbor <IP> { routes | advertise-routes } ] [ <PREFIX> ]
```

Параметры

all – при указании команды all отображается полная информация vpnv4-маршрутов;
rd – при указании команды rd отображается информация о маршрутах с заданным RD;
vrf – при указании команды vrf отображается информация vpnv4-маршрутов для указанного VRF;
routes – при указании команды отображается маршрутная информация, полученная от соседа;
advertise-routes – при указании команды отображается маршрутная информация, объявленная соседу;
<RD> – значение Route distinguisher, задается в одном из следующем виде:

- <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535];
- <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535];
- <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];
- <NAME_VRF> – имя экземпляра VRF, задается строкой до 31 символа.

<IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
<PREFIX> – Префикс, имеет вид – AAA.BBB.CCC.DDD/EE, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes   Route Distinguisher   IP Prefix            Next hop         Metric   Label     LocPrf
Weight Path
-----  ---------------------  ------------------ --------------- ---------- ------- ----------
------ ----------------
*>i          65000:10001      10.100.106.1/32        6.6.6.6           --       16         100
0      ?
*>           65000:10002      10.20.0.0/24           --                --       17         --
--     ?
*>           65000:10002      10.20.1.0/24           --                --       17         --
--     ?
*>i          65000:10001      10.100.0.4/30          2.2.2.2           --       16        100
0      i
*>           65000:10002      172.18.0.0/30          --                --       17        --
--     ?
*>i          65000:10002      10.30.0.0/24           5.5.5.5           --       17        100
55     i
*>i          65000:10001      10.100.104.0/24        2.2.2.2           --       16        100
0      i
*>           65000:10001      10.100.105.0/24        --                --       16        --
--     ?
*>i          65000:10001      10.100.106.0/24        6.6.6.6           --       16        100
0      ?
*>           65000:10001      203.203.203.203/32     --                --       16        --
--     ?
*>           65000:10001      202.202.202.202/32     --                --       16        --
--     ?
*>i          65000:10001      10.100.100.0/24        2.2.2.2           --       16        100
0      i
*>           65000:10001      10.100.0.0/30          --                --       16        --
--     ?
*>           65000:10001      10.100.102.0/24        --                --       16        --
--     ?
```

Пример 2

```
wlc-30# show bgp vpnv4 unicast all 10.100.106.0/24
BGP routing table entry for 65000:10001 10.100.106.0/24
Next hop: 6.6.6.6
Label: 16
AS path: --
Origin: Incomplete
Local preference: 100
Extended Community: RT:65000:10001
Weight: 0
```

timers error-wait

Данной командой устанавливается время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers error-wait <TIME1> <TIME2>
no timers error-wait
```

Параметры

<TIME1> – время в секундах, принимает значения [1..65535];

<TIME2> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

60 и 300

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-VRF-BGP

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-af)# timers error-wait 90 450
```

timers holdtime

Данной командой устанавливается временной интервал, по истечении которого встречная сторона считается недоступной. Таймер запускается после установления отношений соседства и начинает отсчёт от 0. Таймер сбрасывается при получении каждого ответа на keepalive-сообщение от встречной стороны. Рекомендуется устанавливать значение таймера равное *3 * keepalive*.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers holdtime <TIME>
no timers holdtime
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

180

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-VRF-BGP

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-af)# timers holdtime 360
```

timers keepalive

Данной командой устанавливается временной интервал, по истечении которого идет проверка соединения со встречной стороной.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`timers keepalive <TIME>`

`no timers keepalive`

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

60

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

CONFIG-VRF-BGP

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-af)# timers keepalive 120
```

update-source

Данной командой определяется IP/IPv6-адрес контроллера, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых обновлениях маршрутной информации BGP.

Использование отрицательной формы команды (no) удаляет указанный IP/IPv6-адрес источника.

Синтаксис

```
update-source { <ADDR> | <IPV6-ADDR> }
no source-address
```

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# update-source 10.100.100.2
```

vrf

Данной командой в системе создается экземпляр BGP процесса в VRF и осуществляется переход в режим настройки параметров BGP процесса в указанном VRF.

Использование отрицательной формы команды (no) удаляет экземпляр BGP VRF из системы.

Синтаксис

```
[no] ip vrf <VRF>
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP

Пример

```
wlc-30(config-bgp)# vrf xx
wlc-30(config-bgp-vrf)#
```

weight

Данной командой устанавливается вес маршрутов, принимаемый от данного BGP-соседа или группы BGP-соседей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
weight <WEIGHT>
no weight
```

Параметры

<WEIGHT> – значение веса маршрута, принимает значения [0..65535].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-BGP-GROUP

CONFIG-BGP-VRF-GROUP

CONFIG-BGP-NEIGHBOR

CONFIG-BGP-VRF-NEIGHBOR

Пример

```
wlc-30(config-bgp-neighbor)# weight 200
```

Настройка протоколов RIP и RIPNG

- authentication key-chain
- clear ip rip
- clear ipv6 rip
- ip rip metric
- ip rip mode
- ip rip neighbor
- ip rip summary-address
- ipv6 rip metric
- ipv6 rip summary-address
- ipv6 router rip
- passive-interface
- passive-interface
- router rip
- show ip rip
- show ipv6 rip
- timers flush
- timers invalid
- timers update

authentication key-chain

Данная команда определяет список паролей для аутентификации через алгоритм хеширования md5.

Использование отрицательной формы команды (no) удаляет привязку к списку паролей.

Синтаксис

```
authentication key-chain <KEYCHAIN>
no authentication key-chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

Пример

```
wlc-30(config-rip)# authentication key-chain lock
```

clear ip rip

Данная команда удаляет содержимое базы маршрутов RIP.

Синтаксис

```
clear ip rip
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip rip
```

clear ipv6 rip

Данная команда удаляет содержимое базы маршрутов RIPNG.

Синтаксис

```
clear ipv6 rip
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ipv6 rip
```

ip rip metric

Данная команда устанавливает величину метрики на интерфейсе.

Использование отрицательной формы команды (no) устанавливает значение метрики по умолчанию.

Синтаксис

```
ip rip metric <VALUE>
no ip rip metric
```

Параметры

<VALUE> – величина метрики, задаётся в размере [1..15].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip rip metric 11
```

ip rip mode

Данная команда устанавливает режим анонсирования маршрутов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip rip mode <MODE>
no ip rip mode
```

Параметры

<MODE> – режим анонсирования маршрутов:

- multicast – маршруты анонсируются в многоадресном режиме;
- broadcast – маршруты анонсируются в широковещательном режиме;

- unicast – маршруты анонсируются в unicast-режиме соседям, настроенным с помощью команды ***ip rip neighbor <ADDR>***.

Значение по умолчанию

multicast

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip rip mode broadcast
```

ip rip neighbor

Данной командой статически задается IP-адрес соседа для установления отношения в unicast-режиме анонсирования маршрутов.

Использование отрицательной формы команды (no) удаляет статически заданный адрес соседа.

Синтаксис

```
[no] ip rip neighbor <ADDR>
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip rip neighbor 10.100.100.5
```

ip rip summary-address

Данной командой включается суммаризация подсетей.

Использование отрицательной формы команды (no) отключает суммаризацию подсетей.

Синтаксис

```
[no] ip rip summary-address <ADDR/LEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip rip summary-address 10.200.200.0/24
```

ipv6 rip metric

Данная команда устанавливает величину метрики на интерфейсе.

Использование отрицательной формы команды (no) устанавливает значение метрики по умолчанию.

Синтаксис

```
ipv6 rip metric <VALUE>
no ipv6 rip metric
```

Параметры

<VALUE> – величина метрики, задаётся в размере [1..15].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 rip metric 11
```

ipv6 rip summary-address

Данной командой включается суммаризация подсетей IPv6.

Использование отрицательной формы команды (no) отключает суммаризацию подсетей.

Синтаксис

```
[no] ipv6 rip summary-address <ADDR/LEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 rip summary-address fb00::1/20
```

ipv6 router rip

Данной командой осуществляется переход в режим настройки параметров RIPNG-процесса.

Использование отрицательной формы команды (no) устанавливает параметры RIPNG-процесса на значения по умолчанию.

Синтаксис

```
[no] ipv6 router rip
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 router rip
wlc-30(config-ripng)#
```

passive-interface

Данная команда выключает анонсирования маршрутов по интерфейсу.

Использование отрицательной формы команды (no) восстанавливает анонсирования маршрутов.

Синтаксис

`[no] passive-interface { <IF> | <TUN> }`

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

Пример

```
wlc-30(config-rip)# passive-interface gigabitethernet 1/0/15
```

passive-interface

Данная команда выключает анонсирования маршрутов по интерфейсу.

Использование отрицательной формы команды (no) восстанавливает анонсирования маршрутов.

Синтаксис

`[no] passive-interface <IF>`

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIPNG

Пример

```
wlc-30(config-ripng)# passive-interface gigabitethernet 1/0/15
```

router rip

Данной командой осуществляется переход в режим настройки параметров RIP-процесса.

Использование отрицательной формы команды (no) устанавливает параметры RIP-процесса на значения по умолчанию.

Синтаксис

```
[no] router rip
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router rip
wlc-30(config-rip)#
```

show ip rip

Данная команда отображает таблицу маршрутизации RIP.

Синтаксис

```
show ip rip
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip rip Sword# sho ip rip
10.10.0.1/32    via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
10.1.90.0/24    via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
192.168.16.0/24 via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
```

show ipv6 rip

Данная команда отображает таблицу маршрутизации RIPNG.

Синтаксис

```
show ipv6 rip
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 rip Sword# sho ip rip
10.10.0.1/32    via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
10.1.90.0/24    via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
192.168.16.0/24 via 115.0.0.10 on gi1/0/15 [rip 21:31:17] * (100/6)
```

timers flush

Данной командой устанавливается временной интервал, по истечении которого производиться удаление маршрута. При установке значения нужно учитывать следующее правило: «timers invalid + 60».

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers flush <TIME>
no timers flush
```

Параметры

<TIME> – время в секундах, принимает значения [12..65535].

Значение по умолчанию

240 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-rip)# timers flush 300
```

timers invalid

Данной командой определяется временной интервал корректности маршрутной записи без обновления. По истечению срока, без получения обновления, маршрут помечается как не доступный.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timers invalid <TIME>
no timers invalid
```

Параметры

<TIME> – время в секундах, принимает значения [12..65535].

Значение по умолчанию

180

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-rip)# timers invalid 240
```

timers update

Данной командой устанавливается временной интервал, по истечении которого производится анонсирование.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`timers update <TIME>`

`no timers update`

Параметры

<TIME> – время в секундах, принимает значения [12..65535].

Значение по умолчанию

30

Необходимый уровень привилегий

10

Командный режим

CONFIG-RIP

CONFIG-RIPNG

Пример

```
wlc-30(config-rip)# timers update 25
```

Настройка протоколов OSPF и OSPFv3

- area
- area-type
- authentication key
- authentication key chain
- clear ip ospf
- clear ipv6 ospf
- compatible rfc1583
- dead-interval
- hello-interval
- ip ospf
- ip ospf area
- ip ospf authentication algorithm
- ip ospf authentication key
- ip ospf authentication key-chain
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf instance
- ip ospf mtu-ignore
- ip ospf neighbor
- ip ospf network
- ip ospf poll-interval
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf wait-interval
- ipv6 ospf
- ipv6 ospf area
- ipv6 ospf cost
- ipv6 ospf dead-interval
- ipv6 ospf hello-interval
- ipv6 ospf instance
- ipv6 ospf mtu-ignore
- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf poll-interval
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf wait-interval
- ipv6 router ospf
- ipv6 router ospf log-adjacency-changes
- preference
- retransmit-interval
- router ospf
- router ospf log-adjacency-changes
- router-id
- show ip ospf
- show ip ospf database
- show ip ospf interface
- show ip ospf neighbors
- show ip ospf virtual-links
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbors

- show ipv6 ospf virtual-links
- summary-address
- virtual-link
- wait-interval

area

Данной командой устанавливается идентификатор области.

Использование отрицательной формы команды (no) удаляет созданную область.

Синтаксис

```
[no] area <AREA_ID>
```

Параметры

<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF

CONFIG-OSPFV3

Пример 1

```
wlc-30(config-ospf)# area 11.11.11.51
```

Пример 2

```
wlc-30(config-ipv6-ospf)# area 11.11.11.51
```

area-type

Команда определяет тип области.

Использование отрицательной формы команды (no) устанавливает тип области как стандартный.

Синтаксис

```
[no] area-type <TYPE> [ no-summary ]
```

Параметры

<TYPE> – тип области:

- normal – устанавливает значение standart (стандартная область);
- stub – устанавливает значение stub (тупиковая область).

no-summary – команда в связке с параметром «stub» образует область «totally stubby» (для передачи информации за пределы области используется только маршрут по умолчанию);

- nssa – устанавливает значение nssa (область NSSA).

no-summary – в связке с параметром nssa образует область totally nssa (автоматически генерирует маршрут по умолчанию как межобластной).

Значение по умолчанию

normal

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-AREA

CONFIG-OSPFV3-AREA

Пример 1

```
wlc-30(config-ospf-area)# area-type stub
```

Пример 2

```
wlc-30(config-ipv6-ospf-area)# area-type nssa
```

authentication key

Данная команда определяет пароль для аутентификации через алгоритм хеширования md5 с соседом.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 1 до 8 символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером до 8 байт (от 2 до 16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-OSPF-VLINK

Пример

```
wlc-30(config-ospf-vlink)# authentication key ascii-text 12345678
```

authentication key chain

Данная команда определяет список паролей для аутентификации через алгоритм хеширования md5 с соседом.

Использование отрицательной формы команды (no) удаляет привязку к списку паролей.

Синтаксис

```
authentication key chain <KEYCHAIN>
no authentication key chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-OSPF-VLINK

Пример

```
wlc-30(config-ospf-vlink)# authentication key chain key2
```

clear ip ospf

Данная команда сбрасывает все или определенный OSPF-процесс.

Синтаксис

```
clear ip ospf [ <ID> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, для которого будут сброшены все или определенный OSPF-процесс, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip ospf
wlc-30# clear ip ospf 1000
```

clear ipv6 ospf

Данная команда сбрасывает все или определенный OSPFv3-процесс.

Синтаксис

```
clear ipv6 ospf [ <ID> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, для которого будут сброшены все или определенный OSPFv3-процесс, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ipv6 ospf
wlc-30# clear ipv6 ospf 1000
```

compatible rfc1583

Включается совместимость с RFC 1583.

Использование отрицательной формы команды (no) отключает совместимость с RFC 1583.

Синтаксис

```
[no] compatible rfc1583
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF

CONFIG-OSPFV3

Пример

```
wlc-30(config-ospf)# compatible rfc1583
```

dead-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого сосед будет считаться недоступным. Этот интервал должен быть кратным значению «hello-interval». Как правило, «dead-interval» равен 4 интервалам отправки hello-пакетов, то есть 40 секундам.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

`dead-interval <TIME>`

`no dead-interval`

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-VLINK

CONFIG-OSPFV3-VLINK

Пример

```
wlc-30(config-ospf-vlink)# dead-interval 60
```

hello-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер отправляет следующий hello-пакет.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
hello-interval <TIME>
no hello-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-VLINK

CONFIG-OSPFV3-VLINK

Пример

```
wlc-30(config-ospf-vlink)# hello-interval 8
```

ip ospf

Данной командой включают маршрутизацию по протоколу OSPF на интерфейсе.

Использование отрицательной формы команды (no) отключает маршрутизацию по протоколу OSPF на интерфейсе.

Синтаксис

```
[no] ip ospf
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf
```

ip ospf area

Данная команда определяет принадлежность интерфейса к определенной области OSPF-процесса.

Использование отрицательной формы команды (no) удаляет принадлежность интерфейса к определенной области OSPF-процесса.

Синтаксис

`ip ospf area <AREA_ID>`

`no ip ospf area`

Параметры

<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-ip4ip4)# ip ospf area 1.1.1.1
```

ip ospf authentication algorithm

Данная команда определяет алгоритм аутентификации.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
ip ospf authentication algorithm <ALGORITHM>
no ip ospf authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом;
- md5 – пароль хешируется по алгоритму md5.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf authentication algorithm cleartext
```

ip ospf authentication key

Данная команда устанавливает пароль для аутентификации с соседом при передаче пароля открытым текстом.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
ip ospf authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no ip ospf authentication key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 1 до 8 символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером до 8 байт (от 2 до 16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf authentication key ascii-text 123456789
wlc-30(config-if-gi)# ip ospf authentication key ascii-text encrypted CDE65039E5591FA3F1
```

ip ospf authentication key-chain

Данная команда определяет список паролей для аутентификации через алгоритм хеширования md5 с соседом.

Использование отрицательной формы команды (no) удаляет привязку к списку паролей.

Синтаксис

```
ip ospf authentication key-chain <KEYCHAIN>
no ip ospf authentication key-chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf authentication key-chain lock
```

ip ospf cost

Данная команда устанавливает величину метрики на интерфейсе или туннеле.

Использование отрицательной формы команды (no) устанавливает значение метрики по умолчанию.

Синтаксис

```
ip ospf cost <VALUE>
no ip ospf cost
```

Параметры

<VALUE> – величина метрики, задаётся в размере [0..32767].

Значение по умолчанию

150

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf cost 11
```

ip ospf dead-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого сосед будет считаться недоступным. Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов, то есть 40 секундам.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ip ospf dead-interval <TIME>
no ip ospf dead-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf dead-interval 60
```

ip ospf hello-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер отправляет следующий hello-пакет.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ip ospf hello-interval <TIME>
no ip ospf hello-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..255].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf hello-interval 8
```

ip ospf instance

Данная команда определяет принадлежность интерфейса к определенному OSPF-процессу.

Использование отрицательной формы команды (no) удаляет принадлежность интерфейса к OSPF-процессу.

Синтаксис

```
ip ospf instance <ID>
no ip ospf instance
```

Параметры

<ID> – номер процесса, принимает значения [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-ip4ip4)# ip ospf instance 300
```

ip ospf mtu-ignore

Данной командой включается режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах.

Использование отрицательной формы команды (no) отключает режим игнорирования MTU интерфейса.

Синтаксис

```
[no] ip ospf mtu-ignore
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf mtu-ignore
```

ip ospf neighbor

Данной командой статически задается IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях. Использование отрицательной формы команды (no) удаляет статически заданный адрес соседа.

Синтаксис

```
[no] ip ospf neighbor <IP> [ eligible ]
```

Параметры

<IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

eligible – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля, команда изменения приоритета описана в разделе ip ospf priority.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf neighbor 10.0.0.2
```

ip ospf network

Данная команда определяет тип сети.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip ospf network <TYPE>
no ip ospf network
```

Параметры

<TYPE> – тип сети:

- broadcast – тип соединения широковещательный;
- non-broadcast – тип соединения NBMA;
- point-to-multipoint – тип соединения точка-многоточие;
- point-to-multipoint non-broadcast – тип соединения NBMA точка-многоточие;
- point-to-point – тип соединения точка-точка.

Значение по умолчанию

broadcast

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf network point-to-point
```

ip ospf poll-interval

Данная команда устанавливает интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ip ospf poll-interval <TIME>
no ip ospf poll-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1 .. 255].

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf poll-interval 60
```

ip ospf priority

Данной командой устанавливается приоритет контроллера, который используется для выбора DR и BDR.

В качестве DR выбирается контроллер с наибольшим приоритетом.

При равных приоритетах в качестве DR выбирается контроллер с наибольшим router id.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip ospf priority <VALUE>
no ip ospf priority
```

Параметры

<VALUE> – приоритет интерфейса, принимает значения [0..255].

Значение по умолчанию

128

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf priority 200
```

ip ospf retransmit-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты).

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ip ospf retransmit-interval <TIME>
no ip ospf retransmit-interval
```

Параметры

<TIME> – время в секундах, принимает значения [2..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)#ip ospf restransmit-interval 4
```

ip ospf wait-interval

Данной командой определяется интервал времени в секундах, по истечении которого контроллер выберет DR в сети.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ip ospf wait-interval <TIME>
no ip ospf wait-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ip ospf  wait-interval 60
```

ipv6 ospf

Данной командой включают маршрутизацию по протоколу OSPFv3 на интерфейсе.

Использование отрицательной формы команды (no) отключает маршрутизацию по протоколу OSPFv3 на интерфейсе.

Синтаксис

```
[no] ipv6 ospf
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf
```

ipv6 ospf area

Данная команда определяет принадлежность интерфейса к определенной области OSPFv3-процесса.

Использование отрицательной формы команды (no) удаляет принадлежность интерфейса к определенной области OSPFv3-процесса.

Синтаксис

`ipv6 ospf area <AREA_ID>`

`no ipv6 ospf area`

Параметры

<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf area 1.1.1.1
```

ipv6 ospf cost

Данная команда устанавливает величину метрики на интерфейсе или туннеле.

Использование отрицательной формы команды (no) устанавливает значение метрики по умолчанию.

Синтаксис

```
ipv6 ospf cost <VALUE>
no ipv6 ospf cost
```

Параметры

<VALUE> – величина метрики, задаётся в размере [1..65535].

Значение по умолчанию

150

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf cost 11
```

ipv6 ospf dead-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого сосед будет считаться недоступным. Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов, то есть 40 секундам.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ipv6 ospf dead-interval <TIME>
no ipv6 ospf dead-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf dead-interval 60
```

ipv6 ospf hello-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер отправляет следующий hello-пакет.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ipv6 ospf hello-interval <TIME>
no ipv6 ospf hello-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..255].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf hello-interval 8
```

ipv6 ospf instance

Данная команда определяет принадлежность интерфейса к определенному OSPFv3-процессу.

Использование отрицательной формы команды (no) удаляет принадлежность интерфейса к OSPFv3-процесс.

Синтаксис

```
ipv6 ospf instance <ID>
no ipv6 ospf instance
```

Параметры

<ID> – номер процесса, принимает значения [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf instance 300
```

ipv6 ospf mtu-ignore

Данной командой включается режим, в котором OSPFv3-процесс будет игнорировать значение MTU интерфейса во входящих Database Description пакетах.

Использование отрицательной формы команды (no) отключает режим игнорирования MTU интерфейса.

Синтаксис

```
[no] ipv6 ospf mtu-ignore
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf mtu-ignore
```

ipv6 ospf neighbor

Данной командой статически задается IPv6-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях. Использование отрицательной формы команды (no) удаляет статически заданный адрес соседа.

Синтаксис

```
[no] ipv6 ospf neighbor <IPV6-ADDR> [ eligible ]
```

Параметры

<IPV6-ADDR> – IPv6-адрес соседа, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

eligible – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля, команда изменения приоритета описана в разделе ip ospf priority.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf neighbor fc00::2
```

ipv6 ospf network

Данная команда определяет тип сети.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 ospf network <TYPE>
no ipv6 ospf network
```

Параметры

<TYPE> – тип сети:

- broadcast – тип соединения широковещательный;
- non-broadcast – тип соединения NBMA;
- point-to-multipoint – тип соединения точка-многоточие;
- point-to-multipoint non-broadcast – тип соединения NBMA точка-многоточие;
- point-to-point – тип соединения точка-точка.

Значение по умолчанию

broadcast

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf network point-to-point
```

ipv6 ospf poll-interval

Данная команда устанавливает интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить hello-пакет соседу, даже в случае, если сосед неактивен.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ipv6 ospf poll-interval <TIME>
no ipv6 ospf poll-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..255].

Значение по умолчанию

120 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-BRIDGE
CONFIG-LOOPBACK
CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf poll-interval 60
```

ipv6 ospf priority

Данной командой устанавливается приоритет контроллера, который используется для выбора DR и BDR. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 ospf priority <VALUE>
no ipv6 ospf priority
```

Параметры

<VALUE> – приоритет интерфейса, принимает значения [0..255].

Значение по умолчанию

120

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf priority 300
```

ipv6 ospf retransmit-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты).

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
ipv6 ospf retransmit-interval <TIME>
no ipv6 ospf retransmit-interval
```

Параметры

<TIME> – время в секундах, принимает значения [2..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)#ipv6 ospf restransmit-interval 4
```

ipv6 ospf wait-interval

Данной командой определяется интервал времени в секундах, по истечении которого контроллер выберет DR в сети.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

`ipv6 ospf wait-interval <TIME>`

`no ipv6 ospf wait-interval`

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 ospf  wait-interval 60
```

ipv6 router ospf

Командой добавляется OSPFv3-процесс в систему и осуществляется переход в режим настройки параметров OSPFv3-процесса.

Использование отрицательной формы команды (no) удаляет OSPFv3-процесс из системы.

Синтаксис

```
[no] ipv6 router ospf <ID> [vrf <VRF>]
```

Параметры

<ID> – номер автономной системы процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, в котором будет работать OSPFv3-процесс, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 router ospf 300
wlc-30(config-ipv6-ospf)#
```

ipv6 router ospf log-adjacency-changes

Данная команда позволяет включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPFv3.

Использование отрицательной формы команды (no) отключает вывод информации.

Синтаксис

```
[no] ipv6 router ospf log-adjacency-changes
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 router ospf log-adjacency-changes
```

preference

Данная команда определяет приоритетность маршрутов процесса OSPF/OSPFv3.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
preference <VALUE>
no preference
```

Параметры

<VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF

CONFIG-OSPFV3

Пример 1

```
wlc-30(config-ospf)# preference 30
```

Пример 2

```
wlc-30(config-ipv6-ospf)# preference 30
```

retransmit-interval

Данной командой устанавливается интервал времени в секундах, по истечении которого контроллер повторно отправит пакет, который не получил подтверждение о получении (например, Database Description пакет или Link State Request пакеты).

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
retransmit-interval <TIME>
no retransmit-interval
```

Параметры

<TIME> – время в секундах, принимает значения [2..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-VLINK

CONFIG-OSPFV3-VLINK

Пример

```
wlc-30(config-ospf-vlink)# restransmit-interval 4
```

router ospf

Данной командой добавляется OSPF-процесс в систему и осуществляется переход в режим настройки параметров OSPF-процесса.

Использование отрицательной формы команды (no) удаляет OSPF-процесс из системы.

Синтаксис

```
[no] router ospf <ID> [vrf <VRF>]
```

Параметры

<ID> – номер автономной системы процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router ospf 300
wlc-30(config-ospf)#
```

router ospf log-adjacency-changes

Данная команда позволяет включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPFv2.

Использование отрицательной формы команды (no) отключает вывод информации.

Синтаксис

```
[no] router ospf log-adjacency-changes
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router bgp log-adjacency-changes
```

router-id

Данной командой устанавливается идентификатор контроллера.

Использование отрицательной формы команды (no) удаляет идентификатор.

Синтаксис

```
router-id <ID>
no router-id
```

Параметры

<ID> – идентификатор контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF

CONFIG-OSPFV3

Пример

```
wlc-30(config-ospf)# router-id 1.1.1.1
```

show ip ospf

Данная команда отображает таблицу маршрутизации OSPF, если не указан аргумент. При указании процесса выводит информацию о конфигурации интерфейсов по данному процессу.

Синтаксис

```
show ip ospf [ <ID> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, для которого будет отображена таблица маршрутизации OSPF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

Отображение таблицы маршрутизации.

```
wlc-30# show ip ospf
O       2.2.2.0/24         [150/10] dev gi1/0/1                        [ospf2 19:40:31]
(2.2.2.2)
```

show ip ospf database

Данная команда отображает таблицу данных OSPF.

Синтаксис

```
show ip ospf <ID> [ vrf <VRF> ] database
```

Параметры

<ID> – номер OSPF-процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF для OSPF-процесса, в котором будет отображена таблица данных, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip ospf 111 dababase
Global
 Type   LS ID           Router           Age  Sequence  Checksum
 0005  10.166.11.12    10.1.0.1         1020  80000013    01b7
 0005  0.0.0.0         10.166.11.1       245  80000010    aa48
 0005  10.62.19.128    10.166.11.1       725  8000000e    6d2b
 0005  10.62.20.0      10.166.11.1       731  8000000d    69af
 0005  10.62.20.128    10.166.11.1       244  80000010    5e37
 0005  10.62.21.128    10.166.11.1       244  80000010    5341
 0005  10.166.11.0     10.166.11.1       245  80000010    cc6d
 0005  10.166.11.12    10.166.11.1       245  80000010    54d9
Area 0.0.11.1
 Type   LS ID           Router           Age  Sequence  Checksum
 0001  10.1.0.1        10.1.0.1         1015  80000067    989e
 0001  10.166.11.1     10.166.11.1      1021  80000018    8d96
 0002  10.166.11.14    10.166.11.1      1021  80000001    68a5
```

show ip ospf interface

Данная команда отображает информацию об OSPF-интерфейсе.

Синтаксис

```
show ip ospf interface [  vrf <VRF> ] [ <IF> | <TUN> ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<VRF> – имя экземпляра VRF для OSPF-процесса, в котором будет отображена информация об OSPF-интерфейсе, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip ospf interface gi1/0/1
Interface:                      gigabitethernet 1/0/1
Internet Address:               25.25.0.1/24
Router ID:                      6.0.0.1
Network Type:                   broadcast
Area:                           0.0.0.0 (0)
Interface has:                  no authentication
Transmit:                       1
State:                          dr
Priority:                       128
Cost:                           10
ECMP weight:                    1
Hello timer:                    10
Wait timer:                     40
Dead timer:                     40
Retransmit timer:               5
Designed router (ID):           6.0.0.1
Designed router (IP):           25.25.0.1
Backup designed router (ID):    6.0.0.3
Backup designed router (IP):    25.25.0.3
Neighbor Count:                 0
Adjacent neighbor count:        0
```

show ip ospf neighbors

Данная команда отображает информацию о всех соседях или соседях определенного OSPF-процесса.

Синтаксис

`show ip ospf [ <ID> [ vrf <VRF> ] ] neighbors`

`show ip ospf neighbors[ <ID> [ vrf <VRF> ] ]`

Параметры

<ID> – номер OSPF-процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF для OSPF-процесса, в котором будет отображена информация по соседям, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip ospf neighbors
Router ID       Pri      State      DTime   Interface  Router IP
160.0.0.2         0     full/ptp    00:53   vlink0     160.0.0.2
95.0.0.1          1     full/dr     00:31   gi1_15     115.0.0.10
10.100.100.2    128     full/ptp    00:37   gre_25     25.25.0.2
153.0.0.1         1     full/bdr    00:30   po1        1.1.0.2
10.100.100.2    128     2way/other  00:34   gi1_14.25  14.25.0.2
24.24.24.24      15     full/bdr    00:32   te1_1      24.0.0.2
```

show ip ospf virtual-links

Данная команда отображает информацию о виртуальных соединениях.

Синтаксис

`show ip ospf <ID> [ vrf <VRF> ] virtual-links`

Параметры

<ID> – номер OSPF-процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF для OSPF-процесса, в котором будет отображена информация по виртуальным соединениям, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip ospf 10 virtual-links
Virtual Link to router 160.0.0.2 is ptp
Peer IP: 160.0.0.2
Transit area: 1.1.1.1
Interface has no authentication
Timer intervals configured Hello 10, Dead 60, Retransmit 5, Wait 60
Adjacency State full
```

show ipv6 ospf

Данная команда отображает таблицу маршрутизации OSPFv3, если не указан аргумент. При указании процесса выводит информацию о конфигурации интерфейсов по данному процессу.

Синтаксис

`show ipv6 ospf [ <ID> ] [ vrf <VRF> ]`

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, для которого будет отображена таблица маршрутизации OSPFv3, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

Отображение таблицы маршрутизации:

```
wlc-30# show ipv6 ospf
O       fc00::/120          [150/10] dev gi1/0/5              [ospf2 19:39:18]  (2.2.2.2)
```

show ipv6 ospf database

Данная команда отображает таблицу данных OSPFv3.

Синтаксис

```
show ipv6 ospf <ID> [vrf <VRF>] database
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF для OSPFv3-процесса, в котором будет отображена таблица данных, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 ospf 111 dababase
Global
 Type    LS ID           Router           Age  Sequence  Checksum
 0005  10.166.11.12    10.1.0.1         1020  80000013    01b7
 0005  0.0.0.0         10.166.11.1       245  80000010    aa48
 0005  10.62.19.128    10.166.11.1       725  8000000e    6d2b
 0005  10.62.20.0      10.166.11.1       731  8000000d    69af
 0005  10.62.20.128    10.166.11.1       244  80000010    5e37
 0005  10.62.21.128    10.166.11.1       244  80000010    5341
 0005  10.166.11.0     10.166.11.1       245  80000010    cc6d
 0005  10.166.11.12    10.166.11.1       245  80000010    54d9
Area 0.0.11.1
 Type    LS ID           Router           Age  Sequence  Checksum
 0001  10.1.0.1        10.1.0.1         1015  80000067    989e
 0001  10.166.11.1     10.166.11.1      1021  80000018    8d96
 0002  10.166.11.14    10.166.11.1      1021  80000001    68a5
```

show ipv6 ospf interface

Данная команда отображает информацию об интерфейсах, на которых включен протокол OSPFv3.

Синтаксис

```
show ipv6 ospf interface [ vrf <VRF> ] [ <IF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, для OSPFv3-процесса в котором будет отображена информация об OSPFv3-интерфейсе, задается строкой до 31 символа;

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 ospf interface gigabitethernet 1/0/14
wlc-30# Interface:                    gigabitethernet 1/0/14
Internet Address:             IID 0
Router ID:                    88.88.88.88
Network Type:                 broadcast
Area:                         0.0.0.0 (0)
Transmit:                     1
State:                        backup
Priority:                     128
Cost:                         10
ECMP weight:                  1
Hello timer:                  10
Wait timer:                   40
Dead timer:                   40
Retransmit timer:             5
Designed router (ID):         77.0.0.1
Designed router (IP):         fe80::c602:46ff:feed:0
Backup designed router (ID):  88.88.88.88
Backup designed router (IP):  fe80::1:2ff:fe03:463
Neighbor Count:               1
Adjacent neighbor count:      1
Adjacent with neighbor:    77.0.0.1 (dr)
```

show ipv6 ospf neighbors

Данная команда отображает информацию о всех соседях или соседях определенного OSPFv3-процесса.

Синтаксис

```
show ipv6 ospf [<ID> [vrf <VRF>]] neighbors
```

Параметры

<ID> – номер процесса, принимает значения [1..65535], опциональный параметр.

<VRF> – имя экземпляра VRF для OSPFv3-процесса, в котором будет отображена информация по соседям, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 ospf neighbor
Router ID          Pri      State      DTime   Interface  Router IP
77.0.0.1             1     full/dr     00:32   gi1_14     fe80::c602:46ff:feed:0
33.33.33.33        128     full/bdr    00:35   gi1_18     fe80::20:3ff:fea0:498
```

show ipv6 ospf virtual-links

Данная команда отображает информацию о виртуальных соединениях.

Синтаксис

```
show ipv6 ospf <ID> [vrf <VRF>] virtual-links
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF для OSPFv3-процесса, в котором будет отображена информация по виртуальным соединениям, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 ospf 10 virtual-links
Virtual Link to router 160.0.0.2 is ptp
Peer IP: fe80::20:3ff:fea0:498
Transit area: 1.1.1.1
Interface has no authentication
Timer intervals configured: Hello 10, Dead 60, Retransmit 5, Wait 60
Adjacency State full
```

summary-address

Командой включается суммаризация или скрытие подсетей.

Использование отрицательной формы команды (no) отключает суммаризацию или скрытие подсетей.

Синтаксис

```
summary-address { <ADDR/LEN> | <IPV6-ADDR/LEN> } { advertise | not-advertise }
no summary-address <ADDR/LEN>
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA–DDD принимает значения [0..255] и EE принимает значения [1..32];

<IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];

advertise – при указании команды вместо указанных подсетей будет анонсироваться суммарная подсеть;

not-advertise – при указании команды подсети, входящие в указанную подсеть, анонсироваться не будут.

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-AREA

CONFIG-OSPFV3-AREA

Пример

```
wlc-30(config-ospf-area)# summary-address 192.168.16.0/24
```

virtual-link

Данной командой устанавливается виртуальное соединение между основной и удаленными областями, имеющими несколько областей между ними.

Использование отрицательной формы команды (no) удаляет созданное виртуальное соединение.

Синтаксис

```
[no] virtual-link <ID>
```

Параметры

<ID> – идентификатор контроллера, с которым устанавливается виртуальное соединение, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-AREA

CONFIG-OSPFV3-AREA

Пример

```
wlc-30(config-ospf-area)# virtual-link 160.0.0.2
```

wait-interval

Данной командой определяется интервал времени в секундах, по истечении которого контроллер выберет DR в сети.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
wait-interval <TIME>
no wait-interval
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

40

Необходимый уровень привилегий

10

Командный режим

CONFIG-OSPF-VLINK

CONFIG-OSPFV3-VLINK

Пример

```
wlc-30(config-ospf-vlink)# ospf wait-interval 60
```

Настройка протокола IS-IS

- address-family
- authentication area algorithm
- authentication area key
- authentication area key chain
- authentication domain algorithm
- authentication domain key
- authentication domain key chain
- clear isis
- hostname dynamic
- is-type
- isis adjacency point-to-point mode
- isis authentication algorithm
- isis authentication key
- isis authentication key chain
- isis circuit-type
- isis csnp-interval
- isis enable
- isis hello-interval
- isis hello-multiplier
- isis instance
- isis lsp-interval
- isis lsp-retransmit-interval
- isis metric
- isis network point-to-point
- isis priority
- isis psnp-interval
- lsp-refresh-interval
- max-lsp-lifetime
- metric-style
- net
- no isis hello-padding
- preference
- router isis
- show ip isis
- show ipv6 isis
- show isis database
- show isis hostname
- show isis neighbors
- show isis topology
- spf-timeout

address-family

Данная команда включает обмен маршрутами указанного семейства по протоколу IS-IS.
Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
[no] address-family { ipv4 | ipv6 }
```

Параметры

- ipv4 – семейство адресов IPv4;
- ipv6 – семейство адресов IPv6.

Значение по умолчанию

ipv4 – включено;

ipv6 – отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# address-family ipv4
```

authentication area algorithm

Данная команда позволяет выбрать алгоритм аутентификации для L1-уровня, шифроваться будут LSP/SNP-пакеты.

Использование отрицательной формы команды (no) устанавливает значение временного интервала по умолчанию.

Синтаксис

```
authentication area algorithm <ALGORITHM>
no authentication area algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом;
- md5 – пароль хешируется по алгоритму md5.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication area algorithm cleartext
```

authentication area key

Данная команда устанавливает пароль аутентификации для L1-уровня, этим паролем будут шифроваться LSP/SNP-пакеты.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
authentication area key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication area key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой, длинной [8..16] символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication area key ascii-text password
```

authentication area key chain

Данная команда устанавливает список ключей для аутентификации для L1-уровня.

Использование отрицательной формы команды (no) удаляет привязку к списку ключей.

Синтаксис

```
authentication area key chain <KEYCHAIN>
no authentication area key chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой [1..16] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication area key chain key-1
```

authentication domain algorithm

Данная команда устанавливает алгоритм аутентификации для L2-уровня, шифроваться будут LSP/SNP-пакеты.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
authentication domain algorithm <ALGORITHM>
no authentication domain algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом;
- md5 – пароль хешируется по алгоритму md5.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication domain algorithm cleartext
```

authentication domain key

Данная команда устанавливает пароль аутентификации для L2-уровня, этим паролем будут шифроваться LSP/SNP-пакеты.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
authentication domain key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication domain key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой, длинной [8..16] символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication domain key ascii-text password
```

authentication domain key chain

Данная команда устанавливает список ключей для аутентификации для L2-уровня.

Использование отрицательной формы команды (no) удаляет привязку к списку ключей.

Синтаксис

```
authentication domain key chain <KEYCHAIN>
no authentication domain key chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой [1..16] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# authentication domain key chain key-1
```

clear isis

Данная команда перезапускает определенный IS-IS процесс. Команда без параметров перезапускает все процессы IS-IS, настроенные на контроллере.

Синтаксис

```
clear isis [ <ID> ] [ vrf <VRF_NAME> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear isis 15
```

hostname dynamic

Данная команда включает использование TLV 137, которое позволяет передавать hostname контроллера в LSP.

Использование отрицательной формы команды (no) отключает данную возможность.

Синтаксис

```
[no] hostname dynamic
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# hostname dynamic
```

is-type

Данная команда определяет, на каком уровне маршрутизации будет работать текущий процесс IS-IS.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
is-type <LEVEL>
no is-type
```

Параметры

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-1-2 – работа производится и на 1, и на 2 уровне;
- level-2-only – работа производится только на 2 уровне.

Значение по умолчанию

level-1-2

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# is-type level-1
```

isis adjacency point-to-point mode

Данная команда устанавливает способ установления соседства в режиме "точка-точка".

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
isis adjacency point-to-point mode <MODE>
no isis adjacency point-to-point mode
```

Параметры

<MODE> – режим установления соседства:

- two-way-only – IIH с TLV 240 "Point-to-Point Three-Way Adjacency" будут обрабатываться, но сам TLV 240 игнорируется;
- three-way-only – IIH без TLV 240 обрабатываться не будут;
- two-way-three-way – возможность работы как с TLV 240 так и без.

Значение по умолчанию

Разрешены оба способа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis adjacency point-to-point mode three-way-only
```

isis authentication algorithm

Данная команда устанавливает алгоритм аутентификации для hello-пакетов (IIH), выходящих с данного интерфейса.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
isis authentication algorithm <ALGORITHM> [ <LEVEL> ]
no isis authentication algorithm [ <LEVEL> ]
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом;
- md5 – пароль хешируется по алгоритму md5;

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis authentication algorithm cleartext level-1
```

isis authentication key

Данная команда устанавливает пароль для аутентификации hello-пакетов (IIH).

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
isis authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
[ <LEVEL> ]
no isis authentication key [ <LEVEL> ]
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой, длинной [8..16] символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis authentication key ascii-text password level-1
```

isis authentication key chain

Данная команда устанавливает список ключей для аутентификации hello-пакетов (IIH).

Использование отрицательной формы команды (no) удаляет привязку к списку ключей.

Синтаксис

```
isis authentication key chain <KEYCHAIN> [ <LEVEL> ]
no isis authentication key chain [ <LEVEL> ]
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой [1..16] символов.

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis authentication key chain key-1 level-1
```

isis circuit-type

Данная команда определяет на каком уровне маршрутизации будет работать текущий процесс IS-IS на конкретном интерфейсе.

Использование отрицательной формы команды (no) устанавливает уровень работы протокола IS-IS на интерфейсе в соответствии с конфигурацией самого IS-IS процесса.

Синтаксис

```
isis circuit-type <LEVEL>
no isis circuit-type
```

Параметры

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-1-2 – работа производится и на 1, и на 2 уровне;
- level-2-only – работа производится только на 2 уровне.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis circuit-type level-1
```

isis csnp-interval

Данная команда устанавливает интервал генерации и отправки Complete Sequence Number Protocol Data Units (CSNP PDUs).

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis csnp-interval <TIME> [ <LEVEL> ]
no isis csnp-interval [ <LEVEL> ]
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis csnp-interval 33 level-1
```

isis enable

Данная команда включает работу протокола IS-IS на интерфейсе.

Использование отрицательной формы команды (no) выключает IS-IS процесс.

Синтаксис

```
isis enable
no isis enable
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis enable
```

isis hello-interval

Данная команда устанавливает интервал отправки hello-пакетов (IIH) с интерфейса контроллера.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis hello-interval <TIME> [ <LEVEL> ]
no isis hello-interval [ <LEVEL> ]
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis hello-interval 33 level-1
```

isis hello-multiplier

Данная команда устанавливает множитель для вычисления и отправки Hold Time (Hold Time = hello-timer * hello-multiplier) в hello пакетах(IIH).

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis hello-multiplier <VALUE> [ <LEVEL> ]
no isis hello-multiplier [ <LEVEL> ]
```

Параметры

<VALUE> – число, принимающее значения [3..1000];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

3

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis hello-multiplier 34 level-1
```

isis instance

Данная команда определяет принадлежность интерфейса к определенному IS-IS процессу.

Использование отрицательной формы команды (no) удаляет принадлежность интерфейса к IS-IS процессу.

Синтаксис

```
isis instance <ID>
no isis instance
```

Параметры

<ID> – номер процесса, принимает значения [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis instance 35
```

isis lsp-interval

Данная команда задает интервал между успешными последовательными передачами Link-state Packets (LSPs) в Broadcast сети.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis lsp-interval <TIME> [ <LEVEL> ]
no isis lsp-interval [ <LEVEL> ]
```

Параметры

<TIME> – время в миллисекундах, принимает значения [1-10000];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

100

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis lsp-interval 36 level-2
```

isis lsp-retransmit-interval

Данная команда задает интервал повторного распространения всех Link-state Packets (LSPs) в PtP-сети.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis lsp-retransmit-interval <TIME> [ <LEVEL> ]
no isis lsp-retransmit-interval [ <LEVEL> ]
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis lsp-retransmit-interval 37 level-2
```

isis metric

Данная команда устанавливает определенное значение метрики для интерфейса.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis metric <VALUE> [<LEVEL>]
no isis metric [<LEVEL>]
```

Параметры

<VALUE> – число, принимающее значения [1..16777215];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-BRIDGE
CONFIG-E1
CONFIG-MULTILINK
CONFIG-IP4IP4
CONFIG-GRE
CONFIG-LOOPBACK
CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis metric 38 level-1
```

isis network point-to-point

Данная команда переводит текущий интерфейс в режим работы point-to-point протокола IS-IS. Использование отрицательной формы команды (no) прекращает работу в данном режиме.

Синтаксис

```
[no] isis network point-to-point
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-gre)# isis network point-to-point
```

isis priority

Данная команда устанавливает приоритет при выборе DIS.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis priority <VALUE> [ <LEVEL> ]
no isis priority [ <LEVEL> ]
```

Параметры

<VALUE> – число, принимающее значения [0..127];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

64

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis priority 39 level-2
```

isis psnp-interval

Данная команда устанавливает интервал генерации и отправки Partial Sequence Number Protocol Data Units (PSNP PDUs).

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
isis psnp-interval <TIME> [ <LEVEL> ]
no isis psnp-interval [ <LEVEL> ]
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis psnp-interval 40 level-1
```

lsp-refresh-interval

Данная команда устанавливает интервалы обновления/генерации собственных LSP.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
lsp-refresh-interval { min | max } <TIME> [ <LEVEL> ]
no lsp-refresh-interval { min | max } [ <LEVEL> ]
```

Параметры

min — минимальный интервал обновления/генерации;

max — максимальный интервал обновления/генерации;

<TIME> — время в секундах, принимает значения [1..65535];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

min 30

max 900

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# lsp-refresh-interval min 41 level-1
```

max-lsp-lifetime

Данная команда задает время жизни собственных LSP.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
max-lsp-lifetime <TIME> [ <LEVEL> ]
no max-lsp-lifetime [ <LEVEL> ]
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535];

<LEVEL> – уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

1200

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# max-lsp-lifetime 42 level-2
```

metric-style

Данная команда устанавливает тип метрики, который будет использоваться в работе IS-IS процесса.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
metric-style { narrow | wide | transition } [ <LEVEL> ]
no metric-style [ <LEVEL> ]
```

Параметры

narrow — информация о достижимости сетей распространяется с помощью TLV 128;

wide — информация о достижимости сетей распространяется с помощью TLV 135;

transition — информация о достижимости сетей распространяется обоими способами;

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

narrow

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# metric-style wide level-1
```

net

Данная команда устанавливает NET (Network Entity Title) адрес. Он репрезентует AFI (Authority and Format Identifier), Area ID (зону к которой принадлежит контроллер), System ID (идентификатор контроллера) и значение Selector.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
[no] net <NET>
```

Параметры

<NET> – NET адрес, формат: ff[.ffff.ffff.ffff.ffff.ffff.ffff].ffff.ffff.ffff.00, где f – может принимать значения от [1..F].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# net 49.0123.1010.1010.1010.00
```

no isis hello-padding

Данная команда задает отключает режим использования TLV 8 в hello-пакетах (IIH).

Использование положительной формы команды (без ключа no) устанавливает значению по умолчанию.

Синтаксис

```
[no] isis hello-padding
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-LOOPBACK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# isis hello-padding
```

preference

Данная команда устанавливает приоритетность маршрутов данного IS-IS процесса для основной таблицы маршрутизации.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
preference <VALUE>
no preference
```

Параметры

<VALUE> – принимает значения [1..255].

Значение по умолчанию

160

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# preference 43
```

router isis

Данная команда создаёт IS-IS процесс и осуществляет переход в режим настройки параметров этого процесса.

Использование отрицательной формы команды (no) удаляет IS-IS процесс из системы.

Синтаксис

```
[no] router isis <ID> [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# router isis 44
```

show ip isis

Данная команда выводит внутреннюю таблицу маршрутизации.

Синтаксис

```
show ip isis [ <ID> ] [ <ADDR/LEN> ] [ <LEVEL> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<ADDR/LEN> – адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip isis 45
IPv4 local Level 1 RIB for IS-IS process
Last update: 2020-01-24 06:51:02.110
Address                       Type Metric Via
3.3.3.11/32                   L1   20     2.2.2.11 on gi1/0/2

IPv4 local Level 2 RIB for IS-IS process
Last update: 2020-01-24 06:51:12.440
Address                       Type Metric Via
3.3.3.22/32                   IA   20     1.1.1.2 on gi1/0/1
```

show ipv6 isis

Данная команда выводит внутреннюю ipv6-таблицу маршрутизации.

Синтаксис

```
show ipv6 isis [ <ID> ] [ <IPV6-ADDR/LEN> ] [ <LEVEL> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<IPV6-ADDR/LEN> – IPv6-адрес подсети с маской, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 isis 46
IPv6 local Level 1 RIB for IS-IS process
Last update: 2020-01-24 07:08:37.761
Address                       Type Metric Via
6666::/64                     L1   20     fe80::aaf9:4bff:feab:813a on gi1/0/2

IPv6 local Level 2 RIB for IS-IS process
Last update: 2020-01-24 07:07:22.917
Address                       Type Metric Via
2001::/64                     IA   20     fe80::aaf9:4bff:feac:b4a1 on gi1/0/1
```

show isis database

Данная команда выводит информацию по локальной базе всех полученных и сгенерированных LSP (LSDB).

Синтаксис

```
show isis database [ <ID> ] [ <LEVEL> ] [ <LSP-ID> ] [ detailed ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

<LSP-ID> – ID LSP-пакета, задаётся в виде xxxx.xxxx.xxxx.yy-zz, где на месте x – System-ID, y – Pseudonode-ID, z – номер фрагмента. Все числа могут принимать значения [0..F];

detailed – развёрнутая информация о выбранном пункте;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show isis database 47
IS-IS Level 1 Link State Database
LSPID                 Hostname          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
1010.1010.1010.00-00 * wlc-30-l1l2          0x0000000f   0x5eba        960           1/0/0
1111.1111.1111.00-00   wlc-30-l1            0x00000010   0x4402        1071          0/0/0
1111.1111.1111.01-00   wlc-30-l1            0x00000004   0x1a99        985           0/0/0

IS-IS Level 2 Link State Database
LSPID                 Hostname          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
1010.1010.1010.00-00 * wlc-30-l1l2          0x00000010   0x7776        1082          0/0/0
1222.1222.1222.01-00   wlc-30-l2            0x00000003   0xb87a        997           0/0/0
1222.1222.1222.00-00   wlc-30-l2            0x0000000e   0x84c4        997           0/0/0
```

show isis hostname

Данная команда выводит соответствие System-id и имени роутера.

Синтаксис

```
show isis hostname [ <ID> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show isis hostname 48
IS-IS 12
Level  System ID        Dynamic Hostname
   1   1010.1010.1010 * wlc-30-l1l2
   1   1111.1111.1111   wlc-30-l1
   2   1010.1010.1010 * wlc-30-l1l2
   2   1222.1222.1222   wlc-30-l2
```

show isis neighbors

Данная команда отображает информацию по состоянию IS-IS соседств.

Синтаксис

```
show isis neighbors [ <ID> ] [ <LEVEL> ] [ detailed ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

detailed – развёрнутая информация о выбранном пункте;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show isis neighbors 49 detailed
IS-IS Level 1 Neighbors
System ID       Hostname          Interface         State         Holdtime  SNPA
1111.1111.1111  wlc-30-l1            gi1/0/2           Up            10        a8f9.4bab.813a

IS-IS Level 2 Neighbors
System ID       Hostname          Interface         State         Holdtime  SNPA
1222.1222.1222  wlc-30-l2            gi1/0/1           Up            10        a8f9.4bac.b4a1
```

show isis topology

Данная команда выводит полную таблицу достижимости всех сетей и узлов.

Синтаксис

```
show isis topology [ <ID> ] [ <LEVEL> ] [ ipv4 | ipv6 ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..65535];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

ipv4 – семейство адресов IPv4;

ipv6 – семейство адресов IPv6;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show isis topology 50 level-2 Ipv4
IS-IS path to Level 2 routers (narrow metric-style)
Last update: 2020-01-24 07:08:47.783
Vertex                        Type             Metric   Next-Hop           Interface
1.1.1.0/24                    IPv4 Internal    0        --

IS-IS path to Level 2 routers (wide metric-style)
Last update: 2020-01-24 07:08:47.783
Vertex                        Type             Metric   Next-Hop           Interface
3.3.3.22/32                   IPv4 IA          20       wlc-30-l2             gi1/0/1
1.1.1.0/24                    IPv4             0        --
```

spf-timeout

Данная команда устанавливает таймаут перед следующим расчётом SPF.

Использование отрицательной формы команды (no) устанавливает значению по умолчанию.

Синтаксис

```
spf-timeout <TIME> [ <LEVEL> ]
no spf-timeout [ <LEVEL> ]
```

Параметры

<TIME> — время в миллисекундах, принимает значения [1..10000];

<LEVEL> — уровень работы протокола IS-IS:

- level-1 – работа производится только на 1 уровне;
- level-2 – работа производится только на 2 уровне.

Значение по умолчанию

5000

Необходимый уровень привилегий

10

Командный режим

CONFIG-ISIS

Пример

```
wlc-30(config-isis)# spf-timeout 51 level-1
```

25 Настройки MPLS

- Общие настройки MPLS
  - forwarding interface
  - history statistics
  - l2vpn
  - ldp
  - mpls
  - system cpu load-balance mpls passenger
- Настройки протокола LDP
  - address-family
  - advertise-labels
  - clear mpls ldp neighbor
  - description
  - discovery hello holdtime
  - discovery hello interval
  - discovery targeted-hello accept
  - discovery targeted-hello interval
  - discovery targeted-hello holdtime
  - egress-label-type
  - enable
  - interface
  - keepalive
  - neighbor
  - password
  - router-id
  - show mpls ldp binding
  - show mpls ldp discovery
  - show mpls forwarding-table
  - show mpls ldp neighbor
  - targeted
  - transport-address
- Настройки MPLS L2VPN
  - autodiscovery bgp
  - ignore encapsulation-mismatch
  - ignore mtu-mismatch
  - mtu
  - rd
  - route-target
  - ve id
  - ve range
  - vpn id
  - bridge-group
  - description
  - enable
  - encapsulation mpls mtu
  - encapsulation mpls status-tlv disable
  - interface
  - neighbor-address
  - p2p
  - pw
  - pw-class
  - pw-class
  - transport-mode
  - vpls
  - show mpls l2vpn bindings

- show mpls l2vpn pseudowire
- show mpls l2vpn p2p
- show mpls l2vpn pw-class
- show mpls l2vpn vpls

Общие настройки MPLS

forwarding interface

Данной командой включается передача MPLS-пакетов на интерфейсе.

Использование отрицательной формы команды (no) отключает передачу MPLS-пакетов на интерфейсе.

Синтаксис

```
[no] forwarding interface { <IF> | <TUN> }
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-MPLS

Пример

```
wlc-30(config-mpls)# forwarding interface gi 1/0/14
```

history statistics

Данной командой включается запись статистики использования псевдопровода/динамического псевдопровода.

Использование отрицательной формы команды (no) отключает запись статистики использования псевдопровода/динамического псевдопровода.

Синтаксис

```
[no] history statistics
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

CONFIG-L2VPN-PW

Пример

```
wlc-30(config-autodiscovery-bgp)# history statistics
```

l2vpn

Данной командой осуществляется переход в контекст настройки MPLS-L2-туннелей.

Использование отрицательной формы команды (no) удаляет все настройки MPLS-L2-туннели.

Синтаксис

`[no] l2vpn`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-MPLS

Пример

```
wlc-30(config-mpls)# l2vpn
```

ldp

Данной командой осуществляется переход в контекст настройки протокола LDP.

Использование отрицательной формы команды (no) удаляет все настройки протокола LDP.

Синтаксис

`[no] ldp`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-MPLS

Пример

```
wlc-30(config-mpls)# ldp
```

mpls

Данной командой осуществляется переход в контекст настройки функционала MPLS.

Использование отрицательной формы команды (no) удаляет все настройки функционала LDP.

Синтаксис

```
[no] mpls
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# mpls
```

system cpu load-balance mpls passenger

Данной командой включается функционал балансировки трафика между CPU контроллера.

Использование отрицательной формы команды (no) отключает функционал балансировки.

Синтаксис

```
system cpu load-balance mpls passenger [ <OPTION> ]
no system cpu load-balance mpls passenger [ <OPTION> ]
```

Параметры

Параметр <OPTION> принимает значения:

- ip – включает поиск и добавление в расчет хеша ip-src и ip-dst;
- ipoe-pw-with-cw – возможность явно указать, что используется заголовок с Control Word;
- ipoe-pw-without-cw – возможность явно указать, что не используется заголовок с Control Word.

Значение по умолчанию

Отключено. В расчете хеш не используются ip-src и ip-dst.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# system cpu load-balance mpls passenger ip
```

Настройки протокола LDP

address-family

Команда позволяет перейти в режим конфигурации параметров LDP для выбранной address family.

Использование отрицательной формы команды (no) удаляет все параметры из конфигурации.

Синтаксис

```
[no] address-family ipv4
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# address-family ipv4
```

advertise-labels

Команда позволяет задать FEC, для которых протокол LDP будет выделять и распространять метки.

Использование отрицательной формы команды (no) возвращает значение по умолчанию.

Синтаксис

```
advertise-labels <OBJ-GROUP-NETWORK-NAME>
no advertise-labels
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Метки выделяются и анонсируются для всех FEC

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# advertise-labels mpls_adv
```

clear mpls ldp neighbor

Данная команда служит для очистки таблицы LDP-соседей.

Синтаксис

```
clear mpls ldp neighbor [ <ADDR> ]
```

Параметры

<ADDR> – IP-адрес LDP соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# clear mpls ldp neighbor 1.1.1.1
```

description

Данная команда позволяет добавить описание для LDP-соседа.

Использование отрицательной формы команды (no) удаляет описание LDP-соседа.

Синтаксис

```
description <STRING>
no description
```

Параметры

<STRING> – строка от 1 до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp-neigh)# description wlc1
```

discovery hello holdtime

Данная команда устанавливает значение параметра holdtime. Holdtime – интервал времени в течении которого должно прийти хотя бы одно LDP Hello сообщение.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
discovery hello holdtime <TIME>
no discovery hello holdtime
```

Параметры

<TIME> – время в секундах в интервале [3..65535].

Значение по умолчанию

15

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

CONFIG-LDP-AF-IPV4-IF

Пример

```
wlc-30(config-ldp-af-ipv4-if)# discovery hello holdtime 45
```

discovery hello interval

Данная команда устанавливает значение параметра hello interval. Hello interval – промежуток времени между отправкой LDP hello сообщения.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
discovery hello interval <TIME>
no discovery hello interval
```

Параметры

<TIME> – время в секундах в интервале [1..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

CONFIG-LDP-AF-IPV4-IF

Пример

```
wlc-30(config-ldp-af-ipv4-if)# discovery hello interval 15
```

discovery targeted-hello accept

Данная команда разрешает прием targeted-hello сообщений.

Использование отрицательной формы команды (no) запрещает прием targeted-hello сообщений.

Синтаксис

```
discovery targeted-hello accept
no targeted-hello accept
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-AF-IPV4

Пример

```
wlc-30(config-ldp-af-ipv4)# discovery targeted-hello accept
```

discovery targeted-hello interval

Данная команда устанавливает значение параметра hello interval. Hello interval – промежуток времени между отправкой LDP hello сообщений для targeted-соседа.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
discovery targeted-hello interval <TIME>
no discovery targeted-hello interval
```

Параметры

<TIME> – время в секундах в интервале [1..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp-neigh)# discovery targeted-hello interval 15
```

discovery targeted-hello holdtime

Данная команда устанавливает значение параметра holdtime для targeted-соседа. Holdtime – интервал времени, в течение которого должно прийти хотя бы одно LDP Hello сообщение.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
discovery targeted-hello holdtime <TIME>
no discovery targeted-hello holdtime
```

Параметры

<TIME> – время в секундах в интервале [3..65535].

Значение по умолчанию

45

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp)# discovery hello holdtime 45
```

egress-label-type

С помощью данной команды устанавливается режим, когда для FEC, у которых контроллер является egress lsr, анонсируется метка explicit-null (0) вместо implicit null (3).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
egress-label-type explicit-null
no egress-label-type
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Анонсируется IMPLICIT NULL (3)

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# egress-label-type explicit-null
```

enable

Данной командой включает процесс LDP.

Использование отрицательной формы команды (no) отключает процесс LDP.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# enable
```

interface

Данная команда включает прием и рассылку LDP hello сообщений на интерфейсе для определенной address-family.

Использование отрицательной формы команды (no) отключает прием и рассылку LDP hello сообщений на интерфейсе.

Синтаксис

```
[no] interface { <IF> | <TUN> }
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-AF-IPV4

Пример

```
wlc-30(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
```

keepalive

С помощью данной команды устанавливается время ожидания от соседа keepalive-сообщения. В случае истечения таймера сосед считается недоступным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
keepalive <TIMER>
no keepalive
```

Параметры

<TIMER> – время в секундах [3..65535].

Значение по умолчанию

180

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp)# keepalive 120
wlc-30(config-ldp-neigh)# keepalive 160
```

neighbor

Данная команда позволяет создать и перейти в режим конфигурации LDP-targeted соседа.

Использование отрицательной формы команды (no) удаляет targeted соседа из конфигурации.

Синтаксис

```
[no] neighbor <ADDR>
```

Параметры

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# neighbor 2.2.2.2
```

password

Данная команда устанавливает пароль для аутентификации с соседом.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
password { <TEXT> | encrypted <ENCRYPTED-TEXT> }
no password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой, длинной [8..16] символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp-neigh)# password cleartextpassword
```

router-id

Данной командой устанавливается идентификатор контроллера для LDP-протокола.

Использование отрицательной формы команды (no) удаляет идентификатор контроллера для LDP-протокола.

Синтаксис

```
router-id <ID>
no router-id
```

Параметры

<ID> – идентификатор контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP

Пример

```
wlc-30(config-ldp)# router-id 1.1.1.1
```

show mpls ldp binding

Данная команда позволяет вывести информацию по выделенным меткам.

Синтаксис

```
show mpls ldp binding [ detailed ] [ { <ADDR/LEN> | neighbor <ADDR> | [ local <LABEL-ID> ] [ remote <LABEL-ID> ] } ]
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA–DDD принимает значения [0..255] и EE принимает значения [1..32];

<LABEL-ID> – метка, задается в виде числа в диапазоне [0-104875];

<ADDR> – IP-адрес LDP-соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

detailed – информация выдается в детализированном формате.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh mpls ldp bindings
10.10.0.4/32:
    local label:    16
    remote label:   16        lsr: 10.10.0.1
    remote label:   149       lsr: 10.10.0.3
    remote label:   imp-null  lsr: 10.10.0.4       inuse
10.10.0.2/32:
    local label:    imp-null
    remote label:   34        lsr: 10.10.0.1
    remote label:   152       lsr: 10.10.0.3
    remote label:   142       lsr: 10.10.0.4
10.10.0.1/32:
    local label:    20
    remote label:   imp-null  lsr: 10.10.0.1       inuse
    remote label:   139       lsr: 10.10.0.3
    remote label:   127       lsr: 10.10.0.4
```

show mpls ldp discovery

Данная команда позволяет вывести оперативную информацию по состоянию процесса обнаружения LDP.

Синтаксис

```
show mpls ldp discovery [ detailed ]
```

Параметры

detailed – информация выдается в детализированном формате.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show mpls ldp discovery detailed
Local LDP ID: 1.1.1.1
Discovery sources:
Interfaces:
gigabitethernet 1/0/1:
Hello interval: 5 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 10.10.10.2
Transport IP address: 4.4.4.4
Hold time: 15 seconds
Proposed hold time: 15/15 (local/peer) seconds
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
Hello interval: 5 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
Hold time: 45 seconds
Proposed hold time: 45/45 (local/peer) seconds
```

show mpls forwarding-table

Данная команда позволяет вывести таблицу коммутации по меткам (LFIB).

Синтаксис

```
show mpls forwarding-table [ { <ADDR/LEN> | label <LABLE-ID> | nexthop <ADDR> | tunnel <ID> } ]
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA–DDD принимает значения [0..255] и EE принимает значения [1..32];

<LABEL-ID> – метка, задается в виде числа в диапазоне [0..104875];

<ADDR> – IP-адрес LDP-соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<ID> – идентификатор в виде числа в диапазоне [1..2000000].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show mpls forwarding-table
Local     Outgoing                   Prefix                       Outgoing
Next Hop
label      label              or tunnel ID Interface
-------- -------- ------------------------------------------- ----------------
---------------------------------------
18         16                     PW   ID 100                        --
4.4.4.4
17       imp-null                  4.4.4.4/32                      gi1/0/1
10.10.10.2
```

show mpls ldp neighbor

Данная команда отображает информацию обо всех LDP-соседях.

Синтаксис

```
show mpls ldp neighbor [ { <ADDR> | interface { <IF> | <TUN> } } ]
```

Параметры

<ADDR> – IP-адрес LDP-соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show mpls ldp neighbor
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
State: Operational
TCP connection: 4.4.4.4:38759 - 1.1.1.1:646
Messages sent/received: 195/194
Uptime: 03:07:33
LDP discovery sources:
gigabitethernet 1/0/1
1.1.1.1 -> 4.4.4.4
```

targeted

Данная команда включает отправку targeted hello сообщений.

Использование отрицательной формы команды (no) отключает отправку targeted hello сообщений.

Синтаксис

```
[no] targeted
```

Параметры

Команда не имеет параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-NEIGH

Пример

```
wlc-30(config-ldp-neigh)# targeted
```

transport-address

С помощью данной команды определяется IP-адрес источника для LDP-сообщений, необходимых для установления сессии.

Использование отрицательной формы команды (no) удаляет сконфигурированный IP-адрес источника для LDP-сообщений.

Синтаксис

```
transport-address <ADDR>
no transport-address
```

Параметры

<ADDR> – задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-LDP-AF-IPV4

Пример

```
wlc-30(config-ldp-af-ipv4)# transport-address 1.1.1.1
```

Настройки MPLS L2VPN

autodiscovery bgp

Команда позволяет перейти в контекст настройки BGP auto-discovery and singnaling.

Использование отрицательной формы команды (no) удаляет параметр из конфигурации.

Синтаксис

```
[no] autodiscovery bgp
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# autodiscovery bgp
```

ignore encapsulation-mismatch

Данная команда разрешает установку псевдопроводного соединения при несовпадении типа инкапсуляции.

Использование отрицательной формы команды (no) включает проверку типа инкапсуляции перед установкой псевдопроводного соединения.

Синтаксис

```
[ no ] ignore encapsulation-mismatch
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# ignore encapsulation-mismatch
```

ignore mtu-mismatch

Данная команда разрешает установку псевдопроводного соединения при несовпадении значения MTU.

Использование отрицательной формы команды (no) включает проверку значения MTU перед псевдопроводного соединения.

Синтаксис

```
[no] ignore mtu-mismatch
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# ignore mtu-mismatch
```

mtu

Данная команда задает значение MTU для псевдопроводного соединения. Заданное значение передается в extended community.

Использование отрицательной формы команды (no) устанавливает значение MTU по умолчанию.

Синтаксис

```
mtu <VALUE>
no mtu
```

Параметры

<VALUE> – размер MTU, принимает значения в диапазоне [552..10000].

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# mtu 1510
```

rd

Установка значения Route Distinguisher для данного экземпляра VPLS.

Использование отрицательной формы команды (no) удаляет параметр из конфигурации.

Синтаксис

```
rd <RD>
no rd
```

Параметры

<RD> – значение Route distinguisher, задается в одном из следующем виде:

- <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535];
- <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535];
- <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# rd 65000:10001
```

route-target

Установка перечня значений route-target extended community.

Синтаксис

```
[no] route-target { import | export } <RT>
```

Параметры

import – команда определяет маршруты из таблицы L2VPN со значением <RT>, которые будут помещены в соответствующий экземпляр VPLS;

export – команда устанавливает значения <RT>, с которыми маршруты из данного экземпляра VPLS будут анонсированы в BGP;

<RT> – значение route-target, задается в одном из следующем виде:

- <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535];
- <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535];
- <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# route-target export 65000:10001
```

ve id

Данной командой задается идентификатор экземпляра VPLS.

Использование отрицательной формы команды (no) удаляет параметр из конфигурации.

Синтаксис

```
ve id <ID>
no ve id
```

Параметры

<ID> – идентификатор экземпляра VPLS, принимает значения в диапазоне [1..16384].

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# ve id 5
```

ve range

Данной командой настраивается диапазон идентификаторов пограничных устройств VPLS.

Использование отрицательной формы команды (no) устанавливает значение ve range по умолчанию.

Синтаксис

```
ve range <ID
no ve range
```

Параметры

<ID> – идентификатор пограничного устройства, принимает значения в диапазоне [8..100].

Необходимый уровень привилегий

10

Значение по умолчанию

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# ve range 20
```

vpn id

Данной командой задается идентификатор VPN-соединения.

Использование отрицательной формы команды (no) удаляет параметр из конфигурации.

Синтаксис

```
vpn id <ID
no vpn id
```

Параметры

<ID> – идентификатор VPN-соединения, принимает значения в диапазоне [1..4294967295].

Необходимый уровень привилегий

10

Командный режим

CONFIG-AUTODISCOVERY-BGP

Пример

```
wlc-30(config-autodiscovery-bgp)# vpn id 5
```

bridge-group

С помощью данной команды задается VSI (Virtual Switching Instance).

Использование отрицательной формы команды (no) удаляет параметр из конфигурации.

Синтаксис

```
bridge-group <INDEX>
no bridge-group
```

Параметры

<INDEX> – индекс bridge-group. Bridge с указанным индексом должен быть заранее добавлен в конфигурацию.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# bridge-group 25
```

description

Данной командой задаётся описание.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <LINE>
no description
```

Параметры

<LINE> – описание. Задается в виде строки длинной [1-255] символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-PW

CONFIG-L2VPN-PW-CLASS

Пример

```
wlc-30(config-l2vpn-pw)# description PW_FOR_VLAN398
```

enable

Данной командой активируется выбранный функционал.

Использование отрицательной формы команды (no) деактивирует выбранный функционал.

Синтаксис

```
[no] enable
```

Параметры

Команда не имеет параметров

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-PW

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-pw)# enable
```

encapsulation mpls mtu

Данной командой устанавливается значение MTU для pseudowire-интерфейсов входящих в данный pw-class.

Использование отрицательной формы команды (no) устанавливает значение MTU по умолчанию.

Синтаксис

```
encapsulation mpls mtu <MTU>
no encapsulation mpls mtu
```

Параметры

<MTU> – значение MTU, принимает значение в диапазоне [552..10000]

Значение по умолчанию

1500

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-PW-CLASS

Пример

```
wlc-30(config-l2vpn-pw-class)# encapsulation mpls mtu 1464
```

encapsulation mpls status-tlv disable

Данной командой отключается обмен status-tlv сообщениями.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] encapsulation mpls status-tlv disable
```

Параметры

Команда не имеет параметров.

Значение по умолчанию

status-tlv enable

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-PW-CLASS

Пример

```
wlc-30(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable
```

interface

С помощью данной команды задается Attached Circuit интерфейс.

Использование отрицательной формы команды (no) удаляет Attached Circuit интерфейс.

Синтаксис

```
interface { <IF> | <TUN> }
no interface
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# interface gigabitethernet 1/0/4.398
```

neighbor-address

С помощью данной команды указывается адрес контроллера, до которого будет установлен псевдопровод.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
neighbor-address <ADDR>
no neighbor-address
```

Параметры

<ADDR> – IP-адрес контроллера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Адрес соседа принимается равным LSR_ID

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# neighbor-address 192.168.24.78
```

p2p

С помощью данной команды создается L2VPN типа точка-точка (VPWS).

Использование отрицательной формы команды (no) удаляет указанный p2p.

Синтаксис

```
[no] p2p <NAME>
```

Параметры

<NAME> – имя p2p-сервиса, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN

Пример

```
wlc-30(config-l2vpn)# p2p VLAN_398
```

pw

С помощью данной команды создается псевдопровод.

Использование отрицательной формы команды (no) удаляет псевдопровод.

Синтаксис

```
pw <PW_ID> <LSR_ID>
no pw
```

Параметры

<PW_ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295];

<LSR_ID> – идентификатор LSR, до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# pw 398 1.1.1.1
```

pw-class

С помощью данной команды создается pw-class.

Использование отрицательной формы команды (no) удаляет pw-class из конфигурации.

Синтаксис

```
[no] pw-class <WORD>
```

Параметры

<WORD> – имя pw-class длинной [1..31] символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN

Пример

```
wlc-30(config-l2vpn)# pw-class Class1
```

pw-class

С помощью данной команды задается pw class для псевдопровода.

Использование отрицательной формы команды (no) убирает pw-class для данного псевдопровода.

Синтаксис

```
pw-class <WORD>
no pw-class
```

Параметры

<WORD> – имя pw-class, задается строкой длинной [1..31] символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-PW

Пример

```
wlc-30(config-l2vpn-pw)# pw-class Class1
```

transport-mode

Данная команда позволяет выбрать транспортный режим для данного псевдопровода.

Использование отрицательной формы команды (no) возвращает значение по умолчанию.

Синтаксис

```
transport-mode { ethenet | vlan }
no transport-mode
```

Параметры

ethernet – режим, при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тэг;

vlan – режим, при котором 802.1Q тэг может быть сохранен при передаче через pseudo-wire.

Значение по умолчанию

ethernet

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN-EOMPLS

Пример

```
wlc-30(config-l2vpn-eompls)# transport-mode vlan
```

vpls

С помощью данной команды создается L2VPN типа point-to-multipoint.

Использование отрицательной формы команды (no) удаляет указанный vpls.

Синтаксис

```
[no] vpls <NAME>
```

Параметры

<NAME> – имя vpls сервиса, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-L2VPN

Пример

```
wlc-30(config-l2vpn)# vpls Customer1
```

show mpls l2vpn bindings

Данная команда позволяет вывести информацию по параметрам псевдопровода.

Синтаксис

```
show mpls l2vpn binding [ { [ local <LABEL-ID> ] [ remote <LABEL ID> ] | neighbor <ADDR>
| pw <PW-ID> | ve-id <VE-ID> } ]
```

Параметры

<LABEL-ID> – MPLS-метка, задается в виде числа в диапазоне [0..104875];

<ADDR> – IP-адрес LDP-соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PW-ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295];

<VE-ID> – идентификатор PE-контроллера в домене VPLS [1.. 16384].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show mpls l2vpn bindings pw 100
Neighbor: 1.1.1.1, PW ID: 100
Local label: 19
Type: Eth Tagged
Group ID: 0
MTU: 1500
Remote label: 28
Type: Eth Tagged
Group ID: 0
MTU: 1500
```

show mpls l2vpn pseudowire

Данная команда позволяет вывести информацию по статусу псевдопровода.

Синтаксис

```
show mpls l2vpn pseudowire [ pw <PW-ID> ] [neighbor <ADDR> ]
```

Параметры

<PW-ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295];

<ADDR> – IP-адрес targeted LDP-соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show mpls l2vpn pseudowire
Neighbor                                                        PW ID                    Type
Status
---------------------------------------                        ----------
----------            --------
1.1.1.1                                                           100                 Eth
Tagged                Up
```

show mpls l2vpn p2p

Данная команда позволяет получить оперативную информацию по сервису VPWS.

Синтаксис

```
show mpls l2vpn p2p  [ name <WORD> ]
```

Параметры

<WORD> – имя сервиса, задается строкой длинной [1..31] символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh mpls l2vpn p2p
P2P: VPWS
    gigabitethernet 1/0/4.10:
        MTU:    1500
        Status: Up
    PW ID 100, Neighbor 10.10.0.2:
        MTU:         1500
        Status TLV:  Enable
        Last change: 00:05:35
        Status:      Up
```

show mpls l2vpn pw-class

Данная команда позволяет получить оперативную информацию по шаблону конфигурации, примененному к псевдопроводу.

Синтаксис

```
show mpls l2vpn pw-class  [ name <WORD> ]
```

Параметры

<WORD> – имя шаблона, задается строкой длинной [1..31] символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh mpls l2vpn pw-class
PW-class                        Neighbor   PW ID      Status Status-tlv MTU
------------------------------- ---------- ---------- ------ ---------- ------
PW_template                     10.10.0.2  100        UP   Enable     1500
```

show mpls l2vpn vpls

Данная команда позволяет получить оперативную информацию по сервису VPLS.

Синтаксис

```
show mpls l2vpn vpls [ name <WORD> ]
```

Параметры

<WORD> – имя сервиса, задается строкой длинной [1..31] символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh mpls l2vpn vpls
VPLS: VPLS
    bridge 100:
        MTU:    1500
        Status: UP
    PWs:
      PW ID 23, Neighbor 10.10.0.1:
        MTU:         1500
        Status TLV:  Enable
        Last change: 19:00:07
        Status:      UP
```

26 Резервирование

- Управление VRRP
- Управление IPv6 VRRP
- Настройка резервирования DHCP
- Настройка резервирования Firewall
- Настройка MultiWAN
- Настройка объектов отслеживания событий

Управление VRRP

- clear vrrp-state
- show vrrp
- vrrp
- vrrp authentication algorithm
- vrrp authentication key
- vrrp force-up
- vrrp group
- vrrp id
- vrrp ip
- vrrp preempt delay
- vrrp preempt disable
- vrrp priority
- vrrp source-ip
- vrrp timers advertise
- vrrp timers garp delay
- vrrp timers garp refresh
- vrrp timers garp refresh-repeat
- vrrp timers garp repeat
- vrrp track-ip
- vrrp track-ip interval
- vrrp track-ip packets
- vrrp version

clear vrrp-state

Данная команда останавливает выполнение протокола VRRP на время 3 * Advertisement_Interval +1. Это дает возможность контроллеру, находящемуся в состоянии backup, выполнить перехват мастерства.

Синтаксис

```
clear vrrp-state
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# clear vrrp-state
```

show vrrp

Данная команда выводит информации о протоколе VRRP.

Синтаксис

`show vrrp [ <ID> ] [ vrf <VRF> ]`

Параметры

<ID> – номер процесса, принимает значения [1..255];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show vrrp
Virtual router   Virtual IP         Priority   Preemption   State
--------------   ----------------   --------   ----------   ------
4                4.4.4.1            100        Enabled      Master
```

Пример 2

```
wlc-30# show vrrp 4
Interface                 bridge 50
State:                    Master
Virtual IP address:       4.4.4.1
Source IP address:        4.4.4.4
Virtual MAC address:      00:00:5e:00:01:04
Advertisement interval:   1
Preemption:               Enabled
Priority:                 100
Synchronization group ID: --
```

vrrp

Данная команда включает VRRP-процесс на IP-интерфейсе.

Использование отрицательной формы команды (no) выключает VRRP-процесс.

Синтаксис

```
[no] vrrp
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp
```

vrrp authentication algorithm

Данная команда определяет алгоритм аутентификации.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
vrrp authentication algorithm <ALGORITHM>
no vrrp authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации:

- cleartext – пароль, передается открытым текстом;
- md5 – пароль, хешируется по алгоритму md5.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp authentication algorithm cleartext
```

vrrp authentication key

Данная команда устанавливает пароль для аутентификации с соседом.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
vrrp authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no vrrp authentication key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;
<ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp authentication key ascii-text 123456789
wlc-30(config-if-gi)# vrrp authentication key ascii-text encrypted CDE65039E5591FA3F1
```

vrrp force-up

Данной командой устанавливается режим, когда виртуальный IP-интерфейс остается в состоянии UP вне зависимости от состояния самого интерфейса.

Использование отрицательной формы команды (no) устанавливает режим по умолчанию.

Синтаксис

```
[no] vrrp force-up
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp force-up
```

vrrp group

Данной командой устанавливается принадлежность VRRP-интерфейса к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произведется смена ролей.

Использование отрицательной формы команды (no) удаляет VRRP-контроллер из группы.

Синтаксис

```
vrrp group <GRID>
no vrrp group
```

Параметры

<GRID> – идентификатор группы VRRP-контроллера, принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp group 10
```

vrrp id

Данной командой устанавливается идентификатор VRRP контроллера.

Использование отрицательной формы команды (no) удаляет идентификатор виртуального контроллера.

Синтаксис

`vrrp id <VRID>`

`no vrrp id`

Параметры

<VRID> – идентификатор VRRP контроллера, принимает значения [1..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp id 125
```

vrrp ip

Данной командой устанавливается виртуальный IP-адрес VRRP-контроллера.

Использование отрицательной формы команды (no) удаляет виртуальный IP-адрес контроллера.

Синтаксис

```
vrrp ip <ADDR/LEN > [ secondary ]
no vrrp ip
```

Параметры

<ADDR/LEN> – виртуальный IP-адрес и длинна маски, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA–DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов на интерфейс;

secondary – ключ для установки дополнительного IP-адреса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# vrrp ip 115.0.0.1
```

vrrp preempt delay

Данной командой задается временной интервал, по истечении которого Backup-контроллер с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-контроллера с более низким приоритетом.

Использование отрицательной формы команды (no) восстанавливает настройки по умолчанию.

Синтаксис

```
[no] vrrp preempt delay <TIME>
no vrrp preempt delay
```

Параметры

<TIME> – время ожидания, определяется в секундах [0..1000].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp preempt delay 100
```

vrrp preempt disable

Данной командой определяется, будет ли Backup-контроллер с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-контроллера с более низким приоритетом.

Исключением является контроллер, у которого виртуальный IP-адрес совпадает с IP-адресом на интерфейсе, он всегда будет перехватывать на себя роль Master вне зависимости от данной настройки.

Использование отрицательной формы команды (no) восстанавливает настройки по умолчанию.

Синтаксис

```
[no] vrrp preempt disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Переключение включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp preempt disable
```

vrrp priority

Данной командой устанавливается приоритет VRRP-контроллера.

Использование отрицательной формы команды (no) устанавливает значение приоритета по умолчанию.

Синтаксис

`vrrp priority <PR>`

`no vrrp priority`

Параметры

<PR> – приоритет VRRP-контроллера, принимает значения [1..254].

Значение по умолчанию

100

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp priority 189
```

vrrp source-ip

Данной командой устанавливается IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес.

Синтаксис

```
vrrp source-ip <IP>
no vrrp source-ip
```

Параметры

<IP> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# vrrp source-ip 115.0.0.10
```

vrrp timers advertise

Данная команда определяет интервал между отправкой VRRP-сообщений.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
vrrp timers advertise <TIME>
no vrrp timers advertise
```

Параметры

<TIME> – время в секундах, принимает значения [1..40].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp timers advertise 4
```

vrrp timers garp delay

Данная команда определяет интервал, по истечении которого происходит отправка Gratuituous ARP сообщения (сообщений) при переходе контроллера в состояние Master.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

`vrrp timers garp delay <TIME>`

`no vrrp timers garp delay`

Параметры

<TIME> – время в секундах, принимает значения [1..60].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp timers garp delay 4
```

vrrp timers garp refresh

Данная команда определяет интервал, по истечении которого будет происходить периодическая отправка Gratuituous ARP-сообщения (сообщений), пока контроллер находится в состоянии Master.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

`vrrp timers garp refresh <TIME>`

`no vrrp timers garp refresh`

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

Периодическая отправка отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp timers garp refresh 4
```

vrrp timers garp refresh-repeat

Данная команда определяет количество Gratuituous ARP-сообщений, которые будут отправляться с периодом **garp refresh,** пока контроллер находится в состоянии Master.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
vrrp timers garp refresh-repeat <COUNT>
no vrrp timers garp refresh-repeat
```

Параметры

<COUNT> – количество сообщений, принимает значения [1..60].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp timers garp refresh-repeat 10
```

vrrp timers garp repeat

Данная команда определяет количество Gratuituous ARP сообщений, которые будут отправлены при переходе контроллера в состояние Master.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
vrrp timers garp repeat <COUNT>
no vrrp timers garp repeat
```

Параметры

<COUNT> – количество сообщений, принимает значения [1..60].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp timers garp repeat 10
```

vrrp track-ip

Данная команда активирует управление статусом vrrp на основе icmp-reply от определенного IP-адреса.

Использование отрицательной формы команды (no) отключает управление статусом vrrp на основе icmp-reply от определенного IP-адреса.

Синтаксис

```
[no] vrrp track-ip <ADDR>
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp track-ip 192.168.154.22
```

vrrp track-ip interval

Данная команда устанавливает интервал проверки при помощи icmp-request для управления статусом vrrp на основе icmp-reply от определенного IP-адреса.

Использование отрицательной формы команды (no) устанавливает значение интервала по умолчанию.

Синтаксис

```
vrrp track-ip interval <TIME>
no vrrp track-ip interval
```

Параметры

<TIME> – интервал отправки icmp-request в секундах [3..60].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp track-ip interval 20
```

vrrp track-ip packets

Данная команда устанавливает количество icmp-request при каждой проверке для управления статусом vrrp на основе icmp-reply от определенного IP-адреса.

Использование отрицательной формы команды (no) устанавливает значение количества пакетов по умолчанию.

Синтаксис

```
vrrp track-ip packets <COUNT>
no vrrp track-ip packets
```

Параметры

<COUNT> – интервал отправки icmp-request в секундах [1..5].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp track-ip packets 3
```

vrrp version

Данной командой задаётся версия VRRP-протокола.
Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
vrrp version <VERSION>
no vrrp version
```

Параметры

<VERSION> – версия VRRP-протокола: 2, 3.

Значение по умолчанию

2

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp version 3
```

Управление IPv6 VRRP

- ipv6 vrrp
- ipv6 vrrp group
- ipv6 vrrp id
- ipv6 vrrp ip
- ipv6 vrrp preempt delay
- ipv6 vrrp preempt disable
- ipv6 vrrp priority
- ipv6 vrrp source-ip
- ipv6 vrrp timers advertise
- ipv6 vrrp timers nd delay
- ipv6 vrrp timers nd refresh
- ipv6 vrrp timers nd refresh-repeat
- ipv6 vrrp timers nd repeat
- show ipv6 vrrp

ipv6 vrrp

Данная команда включает VRRP-процесс на IPv6-интерфейсе.

Использование отрицательной формы команды (no) выключает VRRP-процесс.

Синтаксис

```
[no] ipv6 vrrp
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp
```

ipv6 vrrp group

Данной командой устанавливается принадлежность VRRP-контроллера к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов. Так, если в одном из процессов произойдет смена мастера, то в другом процессе также произведется смена ролей.

Использование отрицательной формы команды (no) удаляет VRRP-контроллер из группы.

Синтаксис

```
ipv6 vrrp group <GRID>
no ipv6 vrrp group
```

Параметры

<GRID> – идентификатор группы VRRP-контроллера, принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp group 10
```

ipv6 vrrp id

Данной командой устанавливается идентификатор VRRP-контроллера.

Использование отрицательной формы команды (no) удаляет идентификатора виртуального контроллера.

Синтаксис

```
ipv6 vrrp id <VRID>
no ipv6 vrrp id
```

Параметры

<VRID> – идентификатора VRRP-контроллера, принимает значения [1..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp id 125
```

ipv6 vrrp ip

Данной командой устанавливается виртуальный IPv6-адрес VRRP-контроллера.

Использование отрицательной формы команды (no) удаляет виртуальный IPv6-адрес контроллера.

Синтаксис

```
ipv6 vrrp ip <IPV6-ADDR> [secondary]
no ipv6 vrrp ip
```

Параметры

<IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать несколько IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv6-адресов на интерфейс;

secondary – ключ для установки дополнительного IP-адреса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# ipv6 vrrp ip fc00::1
```

ipv6 vrrp preempt delay

Данной командой задается временной интервал, по истечении которого Backup-контроллер с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-контроллера с более низким приоритетом.

Использование отрицательной формы команды (no) восстанавливает настройки по умолчанию.

Синтаксис

`ipv6 vrrp preempt delay <TIME>`

`no ipv6 vrrp preempt delay`

Параметры

<TIME> – время ожидания, определяется в секундах [0..1000].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp preempt delay 100
```

ipv6 vrrp preempt disable

Данной командой определяется, будет ли Backup-контроллер с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-контроллера с более низким приоритетом.

Исключением является контроллер, у которого виртуальный IPv6-адрес совпадает с IPv6-адресом на интерфейсе – он всегда будет перехватывать на себя роль Master вне зависимости от данной настройки.

Использование отрицательной формы команды (no) восстанавливает настройки по умолчанию.

Синтаксис

```
[no] ipv6 vrrp preempt disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Переключение включено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp preempt disable
```

ipv6 vrrp priority

Данной командой устанавливается приоритет VRRP-контроллера.

Использование отрицательной формы команды (no) устанавливает значение приоритета по умолчанию.

Синтаксис

```
ipv6 vrrp priority <PR>
no ipv6 vrrp priority
```

Параметры

<PR> – приоритет VRRP-контроллера, принимает значения [1..254].

Значение по умолчанию

100

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp priority 189
```

ipv6 vrrp source-ip

Данной командой устанавливается IPv6-адрес, который будет использоваться в качестве IPv6-адреса отправителя для VRRP-сообщений.

Использование отрицательной формы команды (no) удаляет указанный IPv6-адрес.

Синтаксис

```
ipv6 vrrp source-ip <IPV6-ADDR>
no ipv6 vrrp source-ip
```

Параметры

<IPV6-ADDR> – IPv6-адрес отправителя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# ipv6 vrrp source-ip fc00::2
```

ipv6 vrrp timers advertise

Данная команда определяет интервал между отправкой VRRP-сообщений.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
ipv6 vrrp timers advertise <TIME>
no ipv6 vrrp timers advertise
```

Параметры

<TIME> – время в секундах, принимает значения [1..40].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp timers advertise 4
```

ipv6 vrrp timers nd delay

Данная команда определяет задержку между установлением IPv6 VRRP состояния MASTER и началом рассылки ND-сообщений.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
ipv6 vrrp timers nd delay <TIME>
```

```
no ipv6 vrrp timers nd delay
```

Параметры

<TIME> – время в секундах, принимает значения [1..60].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp timers nd delay 30
```

ipv6 vrrp timers nd refresh

Данная команда определяет период обновления информации протокола ND для IPv6 VRRP в состоянии MASTER.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
ipv6 vrrp timers nd refresh <TIME>
no ipv6 vrrp timers nd refresh
```

Параметры

<TIME> – время в секундах, принимает значения [1..65535].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp timers nd refresh 32768
```

ipv6 vrrp timers nd refresh-repeat

Данная команда определяет количество ND-сообщений, отправляемых за период обновления для IPv6 VRRP в состоянии MASTER.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

`ipv6 vrrp timers nd refresh-repeat <NUM>`

`no ipv6 vrrp timers nd refresh-repeat`

Параметры

<NUM> – количество, принимает значения [1..60].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp timers nd refresh-repeat 12
```

ipv6 vrrp timers nd repeat

Данная команда определяет количество отправок ND-пакетов после установки IPv6 VRRP в состояние MASTER.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
ipv6 vrrp timers nd repeat <NUM>
no ipv6 vrrp timers nd repeat
```

Параметры

<NUM> – количество, принимает значения [1..60].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 vrrp timers nd repeat 4
```

show ipv6 vrrp

Данная команда выводит информации о протоколе VRRP.

Синтаксис

```
show ipv6 vrrp [ <ID> ] [ vrf <VRF> ]
```

Параметры

<ID> – номер процесса, принимает значения [1..255];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример 1

```
wlc-30# show ipv6 vrrp
Virtual router   Virtual IP                                          Priority   Preemption
State
--------------   -------------------------------------------------   --------   ----------
------
2                fc00::3                                             100        Disabled
Master
```

Пример 2

```
wlc-30# show ipv6 vrrp 2
Interface                 gi1/0/1
State:                    Master
Source IP address:        fe80::aaf9:4bff:feaa:3a1
Virtual IP address:       fc00::3
Virtual MAC address:      00:00:5e:00:01:02
Advertisement interval:   1
Preemption:               Disabled
Priority:                 100
Synchronization group ID: --
```

Настройка резервирования DHCP

- auto-partner-down
- enable
- ip dhcp-server failover
- local-address
- maximum-client-lead-time
- remote-address
- role
- show ip dhcp server failover

auto-partner-down

Данной командой устанавливается время отработки DHCP-lease, при котором аренда может быть продлена одним из узлов отказоустойчивости, не связываясь с другим.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ip dhcp-server failover auto-partner-down <TIME>
no ip dhcp-server failover auto-partner-down
```

Параметры

<TIME> – время, определяется в секундах [1..86400].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-FAILOVER

Пример

```
wlc-30(config-dhcp-server-failover)# auto-partner-down 200
```

enable

Данной командой включается работа резервирования DHCP-сервера.

Использование отрицательной формы команды (no) выключает работа резервирования DHCP-сервера.

Синтаксис

```
[no] enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config-dhcp-server-failover)# enable
```

ip dhcp-server failover

Данной командой осуществляется переход в режим конфигурирования резервирования DHCP-сервера.

Использование отрицательной формы команды (no) удаляет настройки резервирования DHCP-сервера.

Синтаксис

```
[no] ip dhcp-server failover [ vrf <VRF> ] [ all ]
```

Параметры

<VRF> – имя VRF, задается строкой до 31 символа;

all – при использовании ключа при удалении, удаляется конфигурация резервирования DHCP-серверов во всех VRF и глобальной конфигурации.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-server failover
wlc-30(config-dhcp-server-failover)#
```

local-address

Данной командой устанавливается IP-адрес, порт (TCP 647), на котором DHCP-сервер принимает Failover-сообщения при работе в режиме резервирования.

Использование отрицательной формы команды (no) удаляет установленный IP-адрес.

Синтаксис

`local-address <ADDR>`

`no local-address`

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-FAILOVER

Пример

```
wlc-30(config-dhcp-server-failover)# local-address 192.168.1.1
```

maximum-client-lead-time

Данной командой устанавливается максимальное время, на которое DHCP-сервер может продлить время аренды IP-адреса.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`maximum-client-lead-time <TIME>`

`no maximum-client-lead-time`

Параметры

<TIME> – время, определяется в секундах [1..86400].

Значение по умолчанию

1800

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-FAILOVER

Пример

```
wlc-30(config-dhcp-server-failover)# maximum-client-lead-time 200
```

remote-address

Данной командой устанавливается IP-адрес резервного DHCP-сервера, на который отправляются Failover-сообщения при работе в режиме резервирования.

Использование отрицательной формы команды (no) удаляет IP-адрес резервного DHCP-сервера.

Синтаксис

```
remote-address <ADDR>
no remote-address
```

Параметры

<ADDR> – IP-адрес резервного DHCP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-FAILOVER

Пример

```
wlc-30(config-dhcp-server-failover)# remote-address 192.168.1.2
```

role

Данной командой определяется роль DHCP-сервера при работе в режиме резервирования.

Использование отрицательной формы команды (no) удаляет установленную роль DHCP-сервера при работе в режиме резервирования.

Синтаксис

```
role <ROLE>
role
```

Параметры

<ROLE> – роль DHCP-сервера при работе в режиме резервирования:

- primary – режим активного DHCP-сервера;
- secondary – режим резервного DHCP-сервера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-FAILOVER

Пример

```
wlc-30(config-dhcp-server-failover)# role primary
```

show ip dhcp server failover

Данная команда позволяет посмотреть состояние резервирования DHCP-сервера.

Синтаксис

```
show ip dhcp server failover [ vrf <VRF> | all ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip dhcp server failover

Status:                                     Disabled
```

Настройка резервирования Firewall

- ip firewall failover
- ip firewall failover source-address
- ip firewall failover destination-address
- ip firewall failover port
- ip firewall failover sync-type
- ip firewall failover multicast-address
- ip firewall failover multicast-group
- ip firewall failover vrrp-group
- show ip firewall failover
- show high-availability state

ip firewall failover

Данной командой включается резервирование сессий Firewall.

Использование отрицательной формы команды (no) выключает резервирование сессий Firewall.

Синтаксис

```
[no] ip firewall failover
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover
```

ip firewall failover source-address

Данной командой устанавливается IP-адрес сетевого интерфейса, с которого будут отправляться сообщения при работе Firewall в режиме резервирования сессий.

Использование отрицательной формы команды (no) удаляет IP-адрес исходящего интерфейса.

Синтаксис

```
ip firewall failover source-address <ADDR>
```

```
no ip firewall failover source-address
```

Параметры

<ADDR> – IP-адрес сетевого интерфейса, с которого будут отправляться сообщения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover source-address 192.168.1.1
```

ip firewall failover destination-address

Данной командой устанавливается IP-адрес соседа при работе резервирования сессий Firewall в unicast-режиме.

Использование отрицательной формы команды (no) удаляет IP-адрес соседа.

Синтаксис

```
ip firewall failover destination-address <ADDR>
no ip firewall failover destination-address
```

Параметры

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover destination-address 192.168.1.2
```

ip firewall failover port

Данной командой устанавливается номер UDP-порта службы резервирования сессий Firewall, через который происходит обмен информацией при работе в unicast-режиме.

Использование отрицательной формы команды (no) удаляет номер порта службы резервирования сессий Firewall.

Синтаксис

```
ip firewall failover port <PORT>
no ip firewall failover port
```

Параметры

<PORT> – номер порта службы резервирования сессий Firewall, указывается в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover port 3333
```

ip firewall failover sync-type

Данной командой определяется режим обмена информацией между основным и резервным контроллерами.

Использование отрицательной формы команды (no) удаляет режим работы резервирования Firewall.

Синтаксис

```
ip firewall failover sync-type <MODE>
no ip firewall failover sync-type
```

Параметры

<MODE> – режим обмена информацией:

- unicast – режим unicast;
- multicast – режим multicast.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover sync-type multicast
```

ip firewall failover multicast-address

Данной командой устанавливается многоадресный IP-адрес, который будет использоваться для обмена информации при работе резервирования сессий Firewall в multicast-режиме.

Использование отрицательной формы команды (no) удаляет многоадресный IP-адрес.

Синтаксис

```
ip firewall failover multicast-address <ADDR>
no ip firewall failover multicast-address
```

Параметры

<ADDR> – многоадресный IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover multicast-address 238.0.0.10
```

ip firewall failover multicast-group

Данной командой устанавливается идентификатор multicast-группы для обмена информацией при работе резервирования сессий Firewall в multicast-режиме.

Использование отрицательной формы команды (no) удаляет идентификатор группы.

Синтаксис

```
ip firewall failover multicast-group <GROUP>
no ip firewall failover multicast-group
```

Параметры

<GROUP> – multicast-группа, указывается в диапазоне [1000..9999].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall multicast-group 1028
```

ip firewall failover vrrp-group

Данной командой определяется VRRP-группа, на основе которой определяется состояние (основной/резервный) контроллера при резервировании сессий Firewall.

Использование отрицательной формы команды (no) удаляет идентификатор VRRP-группы.

Синтаксис

```
ip firewall failover vrrp-group <GRID>
no ip firewall failover vrrp-group
```

Параметры

<GRID> – идентификатор группы VRRP-контроллера, принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall failover vrrp-group 10
```

show ip firewall failover

Данная команда позволяет посмотреть состояние резервирования сессий Firewall.

Синтаксис

```
show ip firewall failover
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip firewall failover
Communication interface:                    br6
Status:                                     Running
Bytes sent:                                 6407688
Bytes received:                             6355040
Packets sent:                               430149
Packets received:                           429844
Send errors:                                0
Receive errors:                             0
```

show high-availability state

Данная команда позволяет посмотреть общее состояние систем резервирования и роль устройства.

Синтаксис

```
show high-availability state
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show high-availability state
VRRP role:                          Master
AP Tunnels:
    State:                          successful synchronization
    Last synchronization:           17:22:11 08.06.2015
DHCP server:
    State:                          successful synchronization
    Last state change:              17:49:42 03.06.2015
Firewall sessions:
    State:                          successful synchronization
    Last synchronization:           17:22:18 08.06.2015
```

Настройка MultiWAN

- description
- enable
- extended count
- extended jitter
- extended loss
- extended period
- extended rtt
- extended timeout
- failover
- ip address
- ipv6 address
- ipv6 wan load-balance enable
- ipv6 wan load-balance failure-count
- ipv6 wan load-balance nexthop
- ipv6 wan load-balance rule
- ipv6 wan load-balance source-address
- ipv6 wan load-balance success-count
- ipv6 wan load-balance target-list
- ipv6 wan load-balance target-list
- ipv6 wan load-balance target-list check-all
- mode
- outbound
- resp-time
- target
- wan load-balance enable
- wan load-balance failure-count
- wan load-balance nexthop
- wan load-balance rule
- wan load-balance source-address
- wan load-balance success-count
- wan load-balance target-list
- wan load-balance target-list
- wan load-balance target-list check-all
- show wan rules
- show wan cellular status modem
- show wan interfaces status
- show wan tunnels status
- show ipv6 wan rules
- show ipv6 wan interfaces status

description

Данной командой определяется описание правила.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-RULE

CONFIG-IPV6-WAN-RULE

CONFIG-WAN-TARGET

CONFIG-IPV6-WAN-TARGET

Пример

```
wlc-30(config-wan-rule)# description "tunnel to branch"
```

enable

Данной командой включается правило wan, проверка цели.

Использование отрицательной формы команды (no) выключает правило WAN, проверку цели.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-RULE

CONFIG-WAN-TARGET

CONFIG-IPV6-WAN-RULE

CONFIG-IPV6-WAN-TARGET

Пример

Проверка цели:

```
wlc-30(config-ipv6-wan-rule)# enable
```

extended count

Данной командой определяется количество одновременно отправленных ICMP-запросов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
extended count <NUM>
no extended count
```

Параметры

<NUM> – количество одновременно отправленных ICMP-запросов, принимает значение в диапазоне [10..100].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended count 75
```

extended jitter

Данная команда определяет пороговое значение джиттера, при превышении которого качество канала является неудовлетворительным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
extended jitter <TIME>
no extended jitter
```

Параметры

<TIME> – пороговое значение джиттера в миллисекундах, принимает значение в диапазоне [50-1000].

Значение по умолчанию

50

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended jitter 78500
```

extended loss

Данная команда определяет пороговое значение процента потерь, при превышении которого качество канала является неудовлетворительным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
extended loss <NUM>
no extended loss
```

Параметры

<NUM> – пороговое значение процента потерь [1..100].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended loss 80
```

extended period

Данная команда определяет период отправки ICMP-запросов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
extended period <TIME>
no extended period
```

Параметры

<TIME> – период отправки ICMP-запросов в секундах, принимает значение в диапазоне [10..600].

Значение по умолчанию

240

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended period 120
```

extended rtt

Данная команда определяет максимальное пороговое значение круговой задержки, при превышении которого качество канала является неудовлетворительным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
extended rtt <TIME>
no extended rtt
```

Параметры

<TIME> – максимальное пороговое значение RTT в миллисекундах, принимает значение в диапазоне [200..1000].

Значение по умолчанию

240

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended rtt 800
```

extended timeout

Данная команда определяет максимальное время ожидания ответа на ICMP-запрос.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`extended timeout <TIME>`

`no extended timeout`

Параметры

<TIME> – максимальное время ожидания ответа на ICMP-запрос в миллисекундах, принимает значение в диапазоне [500..10000].

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# extended timeout 5000
```

failover

Данной командой осуществляется переключение из режима балансировки в режим резервирования.

Использование отрицательной формы команды (no) возвращает режим балансировки.

Синтаксис

`[no] failover`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-RULE

CONFIG-IPV6-WAN-RULE

Пример

```
wlc-30(config-wan-rule)# failover
```

ip address

Данной командой указывается IP-адрес проверки.

Использование отрицательной формы команды (no) удаляет указанный адрес.

Синтаксис

`ip address <ADDR>`

`no ip address`

Параметры

<ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# ip address 18.168.1.25
```

ipv6 address

Данной командой указывается IPv6-адрес проверки.

Использование отрицательной формы команды (no) удаляет указанный адрес.

Синтаксис

```
ipv6 address <IPV6-ADDR>
no ipv6 address
```

Параметры

<IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-WAN-TARGET

Пример

```
wlc-30(config-ipv6-wan-target)# ipv6 address fc00::2
```

ipv6 wan load-balance enable

Данной командой включается WAN-режим на интерфейсе для IPv6-стека.

Использование отрицательной формы команды (no) выключает WAN-режим для IPv6-стека.

Синтаксис

```
[no] ipv6 wan load-balance enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 wan load-balance enable
```

ipv6 wan load-balance failure-count

Данной командой определяется количество неудачных попыток проверки соединения через IPv6-стек, после которых, при отсутствии ответа от встречной стороны, соединение считается неактивным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 wan load-balance failure-count <VALUE>
no ipv6 wan load-balance failure-count
```

Параметры

<VALUE> – количество попыток, определяется в диапазоне [1…10].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 wan load-balance failure-count 3
```

ipv6 wan load-balance nexthop

Данной командой определяется IPv6-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN.

Использование отрицательной формы команды (no) удаляет указанный IPv6-адрес соседа.

Синтаксис

```
ipv6 wan load-balance nexthop <IPV6-ADDR>
no ipv6 wan load-balance nexthop
```

Параметры

<IPV6-ADDR> – IPv6-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-gi)#ipv6 wan load-balance nexthop 220::71
```

ipv6 wan load-balance rule

Данной командой создается правило WAN и осуществляется переход в режим настройки параметров правила для протокола IPv6.

Использование отрицательной формы команды (no) удаляет созданное WAN-правило.

Синтаксис

```
ipv6 wan load-balance rule <ID>
no ipv6 wan load-balance rule { <ID> | all }
```

Параметры

<ID> – идентификатор создаваемого правила, принимает значения [1..50];

Значение «all» используется при удалении всех правил WAN для протокола IPv6.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 wan load-balance rule 1
```

ipv6 wan load-balance source-address

Данной командой определяется IPv6-адрес контроллера, который будет использоваться в качестве IPv6-адреса источника в отправляемых ICMPv6 пакетах для проверки целей.

Использование отрицательной формы команды (no) удаляет указанный IPv6-адрес источника.

Синтаксис

`ipv6 wan load-balance source-address <IPV6-ADDR>`

`no ipv6 wan load-balance source-address`

Параметры

<IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)#ipv6 wan load-balance source-address 220::71
```

ipv6 wan load-balance success-count

Данной командой определяется количество успешных попыток проверки соединения по протоколу IPv6, после которых, в случае успеха, соединение считается вновь активным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 wan load-balance success-count <VALUE>
no ipv6 wan load-balance success-count
```

Параметры

<VALUE> – количество попыток, определяется в диапазоне [1…10].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 wan load-balance success-count 3
```

ipv6 wan load-balance target-list

Данной командой создается список IPv6-адресов для проверки целостности соединения и осуществляется переход в режим настройки параметров списка.

Использование отрицательной формы команды (no) удаляет созданный список.

Синтаксис

```
ipv6 wan load-balance target-list <NAME>
no ipv6 wan load-balance target-list { <NAME> | all }
```

Параметры

<NAME> – название списка, задается строкой до 31 символа. Значение «all» используется при удалении всех списков IPv6-адресов для проверки целостности соединения.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 wan load-balance target-list ten1
```

ipv6 wan load-balance target-list

Данной командой производится привязка списка IPv6-адресов для проверки целостности соединения на сетевом интерфейсе.

Использование отрицательной формы команды (no) удаляет список с интерфейса.

Синтаксис

`ipv6 wan load-balance target-list <NAME>`

`no ipv6 wan load-balance target-list (удаление привязки списка в режиме конфигурирования сетевых интерфейсов)`

Параметры

<NAME> – название списка, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# ipv6 wan load-balance target-list ten1
```

ipv6 wan load-balance target-list check-all

Данной командой будут проверяться все IPv6-адреса из списка проверки целостности.

Использование отрицательной формы команды (no) отменяет проверку всех IPv6-адресов из списка проверки целостности. В случае недоступности одного из проверяемых узлов, шлюз будет считаться недоступным.

Синтаксис

```
[no] ipv6 wan load-balance target-list check-all
```

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LT

Пример

```
wlc-30(config-if-te)# ipv6 wan load-balance target-list check-all
```

mode

Данная команда определяет режим проверки доступности цели для проверки состояния канала.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
mode { basic | extended }
no mode
```

Параметры

basic – базовый, регулируется допустимым значением положительных ответов на ICMP-запросы;

extended – расширенный метод, в нем производится оценка уровня потерь, задержки, джиттер.

Значение по умолчанию

basic

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# mode extended
```

outbound

Данной командой определяются интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN. Количество шлюзов в маршруте зависит от режима работы MultiWAN:

- при балансировке в список nexthop-маршрута добавляются IP-адреса шлюзов (раздел wan load-balance nexthop) всех активных интерфейсов;
- при резервировании в качестве nexthop-маршрута выбирается IP-адрес шлюза (раздел wan load-balance nexthop) активного интерфейса с наибольшим весом.

Использование отрицательной формы команды (no) исключает указанный интерфейс или туннель из правила MultiWAN.

Синтаксис

```
[no] outbound { interface <IF> | tunnel <TUN> } [<WEIGHT> ]
```

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера (только для IPv4);

<WEIGHT> – вес туннеля или интерфейса, определяется в диапазоне [1..255]. Если установить значение 2, то по данному интерфейсу будет передаваться в 2 раза больше трафика, чем по интерфейсу с дефолтным значением. В режиме резервирования активным будет маршрут с наибольшим весом.

Значение по умолчанию

WEIGHT – 1

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-RULE

CONFIG-IPV6-WAN-RULE

Пример 1

```
wlc-30(config-wan-rule)# outbound interface gigabitethernet 1/0/15
```

Пример 2

```
wlc-30(config-ipv6-wan-rule)# outbound interface bridge 2
```

resp-time

Данной командой определяется время ожидания ответа на запрос по протоколу ICMP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`resp-time <TIME>`

`no resp-time`

Параметры

<TIME> – время ожидания, определяется в секундах [1..30].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET

CONFIG-IPV6-WAN-TARGET

Пример

```
wlc-30(config-wan-target)# resp-time 3
```

target

Данной командой создается цель проверки и осуществляется переход в режим настройки параметров цели.

Использование отрицательной формы команды (no) удаляет созданную цель.

Синтаксис

```
target <ID>
no target { <ID> | all }
```

Параметры

<ID> – идентификатор цели, задаётся в пределах [1..50]. Если при удалении используется значение параметра «all», то будут удалены все цели для конфигурируемого списка целей;

all – удалить все цели.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WAN-TARGET-LIST

CONFIG-IPV6-WAN-TARGET-LIST

Пример

```
wlc-30(config-wan-target-list)# target 1
```

wan load-balance enable

Данной командой включается WAN режим на интерфейсе для IPv4-стека.

Использование отрицательной формы команды (no) выключает WAN режим для IPv4-стека.

Синтаксис

```
[no] wan load-balance enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-if-gi)# wan load-balance enable
```

wan load-balance failure-count

Данной командой определяется количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение считается неактивным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wan load-balance failure-count <VALUE>
no wan load-balance failure-count
```

Параметры

<VALUE> – количество попыток, определяется в диапазоне [1…10].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-if-gi)# wan load-balance failure-count 3
```

wan load-balance nexthop

Данной командой определяется IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес соседа.

Синтаксис

```
wan load-balance nexthop { <ADDR> | dhcp enable | tunnel enable }
no wan load-balance nexthop
```

Параметры

<ADDR> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

dhcp enable – если на интерфейсе IP-адрес получен через DHCP-клиента, используется шлюз с DHCP-сервера;

tunnel enable – использовать в качестве nexthop – peer адрес. Применимо для подключаемых интерфейсов, работающих через PPP.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-if-gi)# wan load-balance nexthop 16.168.1.25
```

wan load-balance rule

Данной командой создается правило WAN и осуществляется переход в режим настройки параметров правила.

Использование отрицательной формы команды (no) удаляет созданное WAN-правило.

Синтаксис

```
wan load-balance rule <ID>
no wan load-balance rule { <ID> | all }
```

Параметры

<ID> – идентификатор создаваемого правила, принимает значения [1..50];

Значение «all» используется при удалении всех правил WAN для протокола IPv6.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# wan load-balance rule 1
```

wan load-balance source-address

Данной командой определяется IP-адрес контроллера, который будет использоваться в качестве IP-адреса источника в отправляемых ICMP пакетах для проверки целей.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

`wan load-balance source-address <ADDR>`

`no wan load-balance source-address`

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LT

Пример

```
wlc-30(config-if-gi)# wan load-balance source-address 16.168.1.25
```

wan load-balance success-count

Данной командой определяется количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
wan load-balance success-count <VALUE>
no wan load-balance success-count
```

Параметры

<VALUE> – количество попыток, определяется в диапазоне [1…10].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-if-gi)# wan load-balance success-count 3
```

wan load-balance target-list

Данной командой создается список IP-адресов для проверки целостности соединения и осуществляется переход в режим настройки параметров списка.

Использование отрицательной формы команды (no) удаляет созданный список.

Синтаксис

```
wan load-balance target-list <NAME>
no wan load-balance target-list { <NAME> | all }
```

Параметры

<NAME> – название списка, задается строкой до 31 символа. Значение «all» используется при удалении всех списков IP-адресов для проверки целостности соединения.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# wan load-balance target-list ten1
```

wan load-balance target-list

Данной командой производится привязка списка IP-адресов для проверки целостности соединения на сетевом интерфейсе.

Использование отрицательной формы команды (no) удаляет созданный список.

Синтаксис

```
wan load-balance target-list <NAME>
no wan load-balance target-list
```

Параметры

<NAME> – название списка, задается строкой до 31 символа. Значение «all» используется при удалении всех списков IP-адресов для проверки целостности соединения.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-if-gi)# wan load-balance target-list ten1
```

wan load-balance target-list check-all

Данной командой будут проверяться все IP-адреса из списка проверки целостности. В случае недоступности одного из проверяемых узлов шлюз будет считаться недоступным.

Использование отрицательной формы команды (no) отменяет проверку всех IP-адресов из списка проверки целостности.

Синтаксис

```
[no] wan load-balance target-list check-all
```

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-LT

CONFIG-CELLULAR-MODEM

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-PPPOE

CONFIG-PPTP

Пример

```
wlc-30(config-gre)# wan load-balance target-list check-all
```

show wan rules

Данная команда используется для просмотра оперативной информации по правилам WAN для протокола IPv4.

Синтаксис

```
show wan rules <ID>
```

Параметры

<ID> – номер правила WAN, принимает значения [1..50].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh wan rules 1
Rule 1 detailed information:
    Failover:     Enabled
    Network: 11.11.11.0/24 Metric: 50
        gi1/0/1 Weight: 2 Nexthop: 3.3.3.1 [Active]
```

show wan cellular status modem

Данная команда используется для просмотра оперативной информации о состоянии интерфейсов с включенным WAN режимом для IPv4-стека.

Синтаксис

```
show wan cellular status modem [ <MODEM-ID> ]
```

Параметры

<MODEM-ID> – идентификатор ранее созданного 2G/3G/4G-модема (только для IPv4).

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы с включенным WAN-режимом для IPv4-стека. Если задан конкретный интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны статусы всех системных интерфейсов с включенным WAN-режимом для IPv4-стека.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wan  interfaces status gigabitethernet 1/0/1
Interface 'gigabitethernet 1/0/1' detailed information:
    State:             Active
    Nexthop address:   3.3.3.1
    Last time success: 0 secs
    Last time failure: 1 hour, 48 minutes and 9 seconds
    Uptime:            --
    Targets:
        3.3.3.1 Test/Ping State: pass Attempts: 1/1
```

show wan interfaces status

Данная команда используется для просмотра оперативной информации о состоянии интерфейсов с включенным WAN режимом для IPv4-стека.

Синтаксис

```
show wan interfaces status [ <IF> ]
```

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы с включенным WAN-режимом для IPv4-стека. Если задан конкретный интерфейс, то будет отображена детальная информация по данному

интерфейсу. При выполнении команды без параметра будут показаны статусы всех системных интерфейсов с включенным WAN-режимом для IPv4-стека.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wan  interfaces status gigabitethernet 1/0/1
Interface 'gigabitethernet 1/0/1' detailed information:
    State:             Active
    Nexthop address:   3.3.3.1
    Last time success: 0 secs
    Last time failure: 1 hour, 48 minutes and 9 seconds
    Uptime:            --
    Targets:
        3.3.3.1 Test/Ping State: pass Attempts: 1/1
```

show wan tunnels status

Данная команда используется для просмотра оперативной информации о состоянии туннелей с включенным WAN-режимом для IPv4-стека.

Синтаксис

```
show wan tunnels status [ <TUN> ]
```

Параметры

<INDEX> – идентификатор туннеля, задается в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

В команде можно указать несколько туннелей. Если не указывать индексы туннелей, то будут отображены статусы заданной группы всех туннелей с включенным WAN-режимом для IPv4-стека. Если задан конкретный туннель, то будет отображена детальная информация по данному туннелю. При выполнении команды без параметра будут показаны статусы всех туннелей с включенным WAN-режимом для IPv4-стека.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show wan tunnels status gre 1
Tunnel 'gre 1' detailed information:
    State:             Active
    Nexthop address:   5.5.5.2
    Last time success: 0 secs
    Last time failure: 50 minutes and 2 seconds
    Uptime:            --
    Targets:
        5.5.5.2 Test/Ping State: pass Attempts: 1/1
```

show ipv6 wan rules

Данная команда используется для просмотра оперативной информации по правилам WAN для протокола IPv6.

Синтаксис

```
show ipv6 wan rules <ID>
```

Параметры

<ID> – номер правила WAN, принимает значения [1..50].

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 wan rules 1
Rule 1 detailed information:
    Failover:     Enabled
    Network: 2a14::/120 Metric: 0
        bridge 1 Weight: 1 Nexthop: 2a12::1 [Active]
```

show ipv6 wan interfaces status

Данная команда используется для просмотра оперативной информации о состоянии интерфейсов с включенным WAN-режимом для IPv6 стека.

Синтаксис

```
show ipv6 wan interfaces status [ <IF> ]
```

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

В команде можно указать несколько интерфейсов. Если не указывать индексы интерфейсов, то будут отображены статусы всех интерфейсов заданной группы интерфейсов с включенным WAN-режимом для стека IPv6. Если задан конкретный интерфейс, то будет отображена детальная информация по данному интерфейсу. При выполнении команды без параметра будут показаны статусы всех системных интерфейсов с включенным WAN-режимом для стека IPv6.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 wan interfaces status bridge 1
Interface 'bridge 1' detailed information:
    State:             Active
    Nexthop address:   2a12::1
    Source address:    fe80::aaf9:4bff:feaa:2dcf
    Last time success: 0 secs
    Last time failure: 19 minutes and 29 seconds
    Uptime:            --
    Targets:
        2a12::1 Test/Ping State: pass Attempts: 1/1
```

Настройка объектов отслеживания событий

- delay down
- delay up
- description
- enable
- mode
- shutdown track
- track
- track sla test
- track vrrp id
- vrrp priority track

delay down

Данной командой устанавливается задержка перед переходом Tracking-объекта в неактивное состояние.

Использование отрицательной формы команды (no) убирает задержку при переходе Tracking-объекта в неактивное состояние.

Синтаксис

```
delay down <TIME>
no delay down
```

Параметры

<TIME> – время задержки перехода Tracking-объекта в неактивное состояние, задаётся в секундах в диапазоне [1..300].

Значение по умолчанию

Задержка отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# delay down 2
```

delay up

Данной командой устанавливается задержка перед переходом Tracking-объекта в активное состояние.

Использование отрицательной формы команды (no) убирает задержку при переходе Tracking-объекта в активное состояние.

Синтаксис

```
delay up <TIME>
no delay up
```

Параметры

<TIME> – время задержки перехода Tracking-объекта в активное состояние, задаётся в секундах в диапазоне [1..300].

Значение по умолчанию

Задержка отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# delay up 5
```

description

Данной командой определяется описание объекта отслеживания событий.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание объекта отслеживания событий, задаётся строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# description "check uplink ip-connection"
```

enable

Данной командой включается Tracking-объект.

Использование отрицательной формы команды (no) отключает Tracking-объект.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Объект выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# enable
```

mode

Данной командой меняется условие перехода Tracking-объекта в активное состояние.

Использование отрицательной формы команды (no) устанавливает условие перехода Tracking-объекта в активное состоянии в дефолт.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – условие нахождения Tracking-объекта в активном состоянии, принимает значения:

- and – Tracking-объект будет находиться в активном состоянии, если все отслеживаемые условия будут в активном состоянии;
- or – Tracking-объект будет находиться в активном состоянии, если хотя бы одно отслеживаемое условие будет в активном состоянии.

Значение по умолчанию

and

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# mode and
```

shutdown track

Данной командой выполняется управление состоянием интерфейса в зависимости от состояния Tracking-объекта.

Использование отрицательной формы команды (no) отменяет управление состоянием интерфейса.

Синтаксис

```
shutdown track <ID>
no shutdown track
```

Параметры

<ID> – номер Tracking-объекта, принимает значения [1..100].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# shutdown track 20
```

track

Данной командой в систему добавляется Tracking-объект и осуществляется переход в режим настройки параметров Tracking-объекта. В объекте задаются события, которые необходимо отслеживать. При активации настроенных событий происходит воздействие на привязанные к объекту сущности.

Использование отрицательной формы команды (no) удаляет Tracking-объект из системы.

Синтаксис

```
[no] track <ID>
```

Параметры

<ID> – номер Tracking-объекта, принимает значения [1..100].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# track 20
wlc-30(config-track)#
```

track sla test

Данной командой устанавливается слежение за состоянием sla-теста.

Использование отрицательной формы команды (no) убирает слежение за sla-тестом.

Синтаксис

```
track sla test <ID> [mode <MODE> ]
[no] track sla test <ID>
```

Параметры

<ID> – номер sla-теста, принимает значение в диапазоне [1..10000];

<MODE> – режим слежения за sla-тестом, может принимать значения:

- state – отслеживается состояние sla-теста;
- reachability – отслеживаются состояние канала связи, которое предоставляет sla-тест.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# track sla test 1 mode reachability
```

track vrrp id

Данной командой задается правило слежения за состоянием VRRP-процесса.

При использовании команды «not» правило будет срабатывать для всех состояний VRRP-процесса кроме указанного. Использование отрицательной формы команды (no) отменяет установленное действие.

Синтаксис

```
track vrrp id <VRID> [not] state <STATE>{ master | backup | fault }
no vrrp <VRID>
```

Параметры

<VRID> – идентификатор отслеживаемого VRRP-контроллера, принимает значения [1..255];

<STATE> – состояние VRRP-процесса при котором Tracking-объект будет менять своё состояние, может принимать значения:

- master – master состояние VRRP-процесса;
- backup – backup состояние VRRP-процесса;
- fault – fault состояние VRRP-процесса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-TRACK

Пример

```
wlc-30(config-track)# track vrrp id 1 state master
```

vrrp priority track

Данной командой изменяется приоритет VRRP-процесса в зависимости от состояния Tracking-объекта.

Использование отрицательной формы команды (no) удаляет.

Синтаксис

```
vrrp priority track <ID> { <PRIO> | increment <INC> | decrement <DEC> }
no vrrp priority track
```

Параметры

<ID> – номер Tracking-объекта, принимает значения в диапазоне [1..100];

<PRIO> – приоритет VRRP-процесса, который выставится, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254];

<INC> – значение, на которое увеличится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии. Принимает значения в диапазоне [1..254];

<DEC> – значение, на которое уменьшится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии. Принимает значения в диапазоне [1..254].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# vrrp priority track 2 increment 2
```

27 Безопасность

- Управление списками контроля доступа (ACL)
- Управление Firewall
- Управление логированием и защитой от сетевых атак
- Управление фильтрацией
- Настройка системы предотвращения вторжений (IPS/IDS)
- Настройка системы "Антиспам"

Управление списками контроля доступа (ACL)

- action
- description
- enable
- ip access-list extended
- match cos
- match destination-address
- match destination-mac
- match destination-port
- match dscp
- match ip-precedence
- match protocol
- match source-address
- match source-mac
- match source-port
- match vlan
- rule
- service-acl input
- show ip access-list

action

Данная команда используется для указания действия, которое должно быть применено для трафика, удовлетворяющего заданным критериям.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
action <ACT>
no action
```

Параметры

<ACT> – назначаемое действие:

- permit – прохождение трафика разрешается;
- deny – прохождение трафика запрещается.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# action permit
```

description

Данная команда используется для изменения описания конфигурируемого списка контроля доступа.
Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

`description <DESCRIPTION>`

`no description`

Параметры

<DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL

Пример

```
wlc-30(config-acl)# description "Drop SSH traffic"
```

enable

Данная команда используется для активирования правила.
Использование отрицательной формы команды (no) деактивирует правило.

Синтаксис

`[no] enable`

Параметры

Команда не содержит параметров.

Значение по умолчанию

Правило выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# enable
```

ip access-list extended

Данная команда используется для создания списка контроля доступа и перехода в режим конфигурирования списка.

Использование отрицательной формы команды (no) удаляет заданный список контроля доступа.

Синтаксис

```
[no] ip access-list extended <NAME>
```

Параметры

<NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip access-list extended acl-ssh-drop
wlc-30(config-acl)#
```

match cos

Данной командой устанавливается значение 802.1p приоритета, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match cos <COS>
no match cos
```

Параметры

<COS> – значение 802.1p приоритета, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match cos 2
```

match destination-address

Данной командой устанавливаются IP-адреса получателя, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match destination-address { <ADDR> <MASK> | any }
no match destination-address
```

Параметры

<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске.

При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match destination-address 10.10.10.0 255.255.255.0
```

match destination-mac

Данной командой устанавливаются MAC-адреса получателя, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match destination-mac <ADDR> <WILDCARD>
no match destination-mac
```

Параметры

<ADDR> – MAC-адрес получателя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match destination-mac A8:F9:4B:AA:00:41 00:00:00:00:00:FF
```

match destination-port

Данной командой устанавливается номер TCP/UDP-порта получателя, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
match destination-port {<PORT> | any}
no match destination-port
```

Параметры

<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535]. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match destination-port 22
```

match dscp

Данной командой устанавливается значение кода DSCP, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match dscp <DSCP>
no match dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match dscp 55
```

match ip-precedence

Данной командой устанавливается значение кода IP Precedence, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match ip-precedence <IPP>
no match ip-precedence
```

Параметры

<IPP> – значение кода IP Precedence, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match ip-precedence 5
```

match protocol

Данной командой устанавливается имя IP-протокола, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match protocol <TYPE>
no match protocol
match protocol-id <ID>
no match protocol-id
```

Параметры

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов;

<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

При указании значения «any» правило будет срабатывать для любого протокола.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match protocol tcp
```

match source-address

Данной командой устанавливаются IP-адреса отправителя, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match source-address { <ADDR> <MASK> | any }
no match source-address
```

Параметры

<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске.

При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match source-address 10.100.100.0 255.255.255.0
```

match source-mac

Данной командой устанавливаются MAC-адреса отправителя, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match source-mac <ADDR> <WILDCARD>
no match source-mac
```

Параметры

<ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match source-mac A8:F9:4B:AA:00:40 00:00:00:FF:FF:FF
```

match source-port

Данной командой устанавливается номер TCP/UDP-порта отправителя, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match source-port { <PORT> | any }
no match source-port
```

Параметры

<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match source-port any
```

match vlan

Данной командой устанавливается значение идентификационного номера VLAN, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

`match vlan <VID>`

`no match vlan`

Параметры

<VID> – идентификационный номер VLAN, принимает значения [1…4094].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL-RULE

Пример

```
wlc-30(config-acl-rule)# match vlan 100
```

rule

Данная команда используется для создания правила и перехода в режим конфигурирования CONFIG-ACL-RULE. Правила обрабатываются устройством в порядке возрастания их номеров.

Использование отрицательной формы команды (no) удаляет указанное правило.

Синтаксис

`[no] rule <ORDER>`

Параметры

<ORDER> – номер правила, принимает значения [1..4094].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ACL

Пример

```
wlc-30(config-acl)# rule 10
wlc-30(config-acl-rule)#
```

service-acl input

Данная команда используется для привязки указанного списка контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.

Использование отрицательной формы команды (no) удаляет привязку списка контроля доступа к данному интерфейсу.

Синтаксис

```
service-acl input <NAME>
no service-acl input
```

Параметры

<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-PORT-CHANNEL

Пример

```
wlc-30(config-if-gi)# service-acl input acl-ssh-drop
```

show ip access-list

Данная команда используется для просмотра списков управления доступом.

Синтаксис

```
show ip access-list [ <NAME> [ <ORDER> ] ]
```

Параметры

<NAME> – имя списка управления доступом, задаётся строкой до 31 символа;

<ORDER> – номер правила, принимает значения [1..4096]. При указании номера правила будет показана информация только по данному правилу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip access-list
Name                              Description
--------------------------------  ------------------------------------------------
acl-telnet-drop                   --
acl-ssh-drop                      Drop SSH traffic
wlc-30# show ip access-list acl-ssh-drop
Index:                        1
Matching pattern:
    Protocol:                 TCP(6)
    Source MAC address:       any
    Source IP address:        any
    Source port:              any
    Destination MAC address:  any
    Destination IP address:   any
    Destination port:         22
Action:                       Deny
Status:                       Enabled
-------------------------------------------------------------------------------
```

```
Index:                        2
Matching pattern:
    Protocol:                 any
    Source MAC address:       any
    Source IP address:        any
    Destination MAC address:  any
    Destination IP address:   any
Action:                       Permit
Status:                       Enabled
-------------------------------------------------------------------------------
```

Управление Firewall

- action
- clear ip firewall counters
- clear ip firewall sessions
- clear ipv6 firewall counters
- clear ipv6 firewall sessions
- description
- enable
- ip firewall disable
- ip firewall mode
- ip firewall sessions counters
- ip firewall sessions allow-unknown
- ip firewall sessions generic-timeout
- ip firewall sessions icmp-timeout
- ip firewall sessions icmpv6-timeout
- ip firewall sessions max-expect
- ip firewall sessions max-tracking
- ip firewall sessions tcp-connect-timeout
- ip firewall sessions tcp-disconnect-timeout
- ip firewall sessions tcp-estabilished-timeout
- ip firewall sessions tcp-latecome-timeout
- ip firewall sessions tracking
- ip firewall sessions udp-assured-timeout
- ip firewall sessions udp-wait-timeout
- match application
- match destination-address
- match destination-address-port
- match destination-mac
- match destination-nat
- match destination-port
- match fragment
- match icmp
- match ip-option
- match protocol
- match source-address
- match source-address-port
- match source-mac
- match source-port
- ports firewall enable
- rate-limit pps
- rearrange
- renumber rule
- rule
- security zone
- security-zone
- security zone-pair
- show ip firewall counters
- show ip firewall sessions
- show ip firewall sessions tracking
- show ipv6 firewall counters
- show ipv6 firewall sessions
- show security zone
- show security zone-pair
- show security zone-pair configuration

action

Данная команда используется для указания действия, которое должно быть применено для трафика, удовлетворяющего заданным критериям.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
action <ACT> [log]
no action
```

Параметры

<ACT> – назначаемое действие:

- permit – прохождение трафика разрешается;
- deny – прохождение трафика запрещается;
- reject – прохождение трафика запрещается, а также посылается отправителю ответ об ошибке;
- netflow-sample – прохождение трафика разрешается и осуществляется экспорт статистики по протоколу Netflow;
- sflow-sample – прохождение трафика разрешается и осуществляется экспорт статистики по протоколу sFlow;
- log – ключ для активации логирования сессий, устанавливающимися согласно данному правилу.

Значение по умолчанию

Действие не настроено, логирование отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# action permit
```

clear ip firewall counters

Данной командой осуществляется сброс счетчиков правил Firewall.

Синтаксис

```
clear ip firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE>
[<ORDER>] ] ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут очищены счетчики правил в указанном VRF;

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будут очищены счетчики только по данному правилу.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip firewall counters trusted self
```

clear ip firewall sessions

Данной командой осуществляется удаление активных IP-сессий.

Синтаксис

```
clear ip firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address
<ADDR> ]
[ outiside-source-address <ADDR> ] [ inside-destination-address <ADDR> ] [ outside-
destination-address <ADDR> ]
[ inside-source-port <PORT> ] [ outside-source-port <PORT> ] [ inside-destination-port
<PORT> ] [ outside-destination-port <PORT> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут удалены активные сессии в указанном VRF;

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – TCP/UDP-порт, принимает значения [1..65535];

inside-source-address – ключ для указания IP-адреса источника, приходящих пакетов;

inside-destination-address – ключ для указания IP-адреса назначения, приходящих пакетов;

outiside-source-address – ключ для указания IP-адреса источника, отправляемых пакетов;

outside-destination-address – ключ для указания IP-адреса назначения отправляемых пакетов;

inside-source-port – ключ для указания TCP/UDP-порта отправителя в приходящих пакетах;

outside-source-port – ключ для указания TCP/UDP-порта отправителя в отправляемых пакетах;

inside-destination-port – ключ для указания TCP/UDP-порта назначения в приходящих пакетах;

outside-destination-port – ключ для указания TCP/UDP-порта назначения в отправляемых пакетах.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip firewall sessions vrf VRF1
```

clear ipv6 firewall counters

Данной командой осуществляется сброс счетчиков правил Firewall.

Синтаксис

```
clear ipv6 firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE>
[<ORDER>] ] ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут очищены счетчики правил в указанном VRF;

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будут очищены счетчики только по данному правилу.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ipv6 firewall counters trusted self
```

clear ipv6 firewall sessions

Данной командой осуществляется удаление активных IPv6-сессий.

Синтаксис

```
clear ipv6 firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address
<IPV6-ADDR> ] [ outiside-source-address <IPV6-ADDR> ]
[ inside-destination-address <IPV6-ADDR> ] [ outside-destination-address <IPV6-ADDR> ]
[ inside-source-port <PORT> ] [ outside-source-port <PORT> ]
[ inside-destination-port <PORT> ] [ outside-destination-port <PORT> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут удалены активные сессии в указанном VRF;

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<PORT> – TCP/UDP-порт, принимает значения [1..65535];

inside-source-address – команда для указания IPv6-адреса источника, приходящих пакетов;

inside-destination-address – команда для указания IPv6-адреса назначения, приходящих пакетов;

outiside-source-address – команда для указания IPv6-адреса источника, отправляемых пакетов;

outside-destination-address – команда для указания IPv6-адреса назначения отправляемых пакетов;

inside-source-port – ключ для указания TCP/UDP-порта отправителя в приходящих пакетах;

outside-source-port – ключ для указания TCP/UDP-порта отправителя в отправляемых пакетах;

inside-destination-port – ключ для указания TCP/UDP-порта назначения в приходящих пакетах;

outside-destination-port – ключ для указания TCP/UDP-порта назначения в отправляемых пакетах.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ipv6 firewall sessions vrf VRF1
```

description

Данная команда используется для изменения описания конфигурируемой зоны или пары зон безопасности. Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание зоны безопасности, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE

CONFIG-ZONE-PAIR

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone)# description "Trusted interfaces"
```

enable

Данная команда используется для активирования правила.

Использование отрицательной формы команды (no) деактивирует правило.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# enable
```

ip firewall disable

Данная команда используется для отключения функции Firewall на сетевом интерфейсе.

Использование отрицательной формы команды (no) включает функцию Firewall на сетевом интерфейсе.

Синтаксис

```
[no] ip firewall disable
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-CELLULAR-MODEM

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-L2TP

CONFIG-LT

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-OPENVPN

Пример

```
wlc-30(config-if-gi)# ip firewall disable
```

ip firewall mode

Данная команда используется для выбора режима работы межсетевого экрана.

Использование отрицательной формы команды (no) устанавливает режим работы межсетевого экрана по умолчанию.

Синтаксис

```
ip firewall mode <MODE>
no ip firewall mode
```

Параметры

<MODE> – режим работы межсетевого экрана, может принимать значения:

- stateful – режим, при котором контроллер отслеживает сессии. Первые пакеты сессии проходят полный цикл проверки согласно правил межсетевого экрана, а последующие пакеты сессии маршрутизируются без дополнительных проверок. Данное правило не распространяется на работу механизма DPI;
- stateless – режим, при котором контроллер не отслеживает сессии. Каждый пакет проходит полный цикл проверки согласно правил межсетевого экрана, что существенно снижает производительность оборудования. Использование данного режима допустимо только в условиях крайней необходимости.

Значение по умолчанию

stateful

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall mode stateless
```

ip firewall sessions counters

Командой выполняется включение счетчиков сессий для NAT и Firewall. Счетчики увеличиваются только тогда, когда устанавливается новая сессия. Для установленных сессий увеличения значений счетчиков не происходит при прохождении пакетов. Включение счетчиков снижает производительность контроллера.

Команды для просмотра счетчиков и сессий описаны в разделах show ip firewall counters, show ip firewall sessions, show ipv6 firewall counters и show ipv6 firewall sessions.

Использование отрицательной формы команды (no) отключает счетчики сессий.

Синтаксис

```
[no] ip firewall sessions counters
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions counters
```

ip firewall sessions allow-unknown

Данной командой отключается фильтрация пакетов, для которых не удалось определить принадлежность к какому-либо известному соединению и которые не являются началом нового соединения.

Использование отрицательной формы команды (no) включает фильтрацию.

Синтаксис

```
[no] ip firewall sessions allow-unknown
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Включено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions allow-unknown
```

ip firewall sessions generic-timeout

Данной командой определяется время жизни сессии для неподдерживаемых протоколов, по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions generic-timeout <TIME>
no ip firewall sessions generic-timeout
```

Параметры

<TIME> – время жизни сессии для неподдерживаемых протоколов, принимает значения в секундах [1..8553600].

Значение по умолчанию

60 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions generic-timeout 60
```

ip firewall sessions icmp-timeout

Данной командой определяется время жизни ICMP-сессии, по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions icmp-timeout <TIME>
no ip firewall sessions icmp-timeout
```

Параметры

<TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600].

Значение по умолчанию

30 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions icmp-timeout 60
```

ip firewall sessions icmpv6-timeout

Данной командой определяется время жизни ICMPv6-сессии, по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions icmpv6-timeout <TIME>
no ip firewall sessions icmpv6-timeout
```

Параметры

<TIME> – время жизни ICMPv6-сессии, принимает значения в секундах [1..8553600].

Значение по умолчанию

30 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions icmpv6-timeout 60
```

ip firewall sessions max-expect

Данной командой определяется размер таблицы сессий ожидающих обработки.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions max-expect <COUNT>
no ip firewall sessions max-expect
```

Параметры

<COUNT> – размер таблицы, принимает значения [1..8553600].

Значение по умолчанию

256

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions max-expect 512
```

ip firewall sessions max-tracking

Данной командой определяется размер таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions max-tracking <COUNT>
no ip firewall sessions max- tracking
```

Параметры

<COUNT> – размер таблицы, принимает значения [1..8553600].

Значение по умолчанию

512000

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions max-tracking 256000
```

ip firewall sessions tcp-connect-timeout

Данной командой определяется время жизни TCP-сессии в состоянии «соединение устанавливается», по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions tcp-connect-timeout <TIME>
no ip firewall sessions tcp-connect-timeout
```

Параметры

<TIME> – время жизни TCP-сессии в состоянии "соединение устанавливается", принимает значения в секундах [1..8553600].

Значение по умолчанию

60 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions tcp-connect-timeout 120
```

ip firewall sessions tcp-disconnect-timeout

Данной командой определяется время жизни TCP-сессии в состоянии "соединение закрывается", по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions tcp-disconnect-timeout <TIME>
no ip firewall sessions tcp-disconnect-timeout
```

Параметры

<TIME> – время жизни TCP-сессии в состоянии "соединение закрывается", принимает значения в секундах [1..8553600].

Значение по умолчанию

30 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions tcp-disconnect-timeout 10
```

ip firewall sessions tcp-estabilished-timeout

Данной командой определяется время жизни TCP-сессии в состоянии "соединение установлено", по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions tcp-estabilished-timeout <TIME>
no ip firewall sessions tcp-estabilished-timeout
```

Параметры

<TIME> – время жизни TCP-сессии в состоянии "соединение установлено", принимает значения в секундах [1..8553600].

Значение по умолчанию

120 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions tcp-estabilished-timeout 3600
```

ip firewall sessions tcp-latecome-timeout

Данной командой определяется время ожидания, по истечении которого происходит фактическое удаление закрытой TCP-сессии из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions tcp-latecome-timeout <TIME>
no ip firewall sessions tcp-latecome-timeout
```

Параметры

<TIME> – время ожидания, принимает значения в секундах [1..8553600].

Значение по умолчанию

120 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions tcp-latecome-timeout 10
```

ip firewall sessions tracking

Данной командой включается функция отслеживания сессий уровня приложений для отдельных протоколов.

Использование отрицательной формы команды (no) отключает функцию отслеживания сессий уровня приложений для отдельных протоколов.

Синтаксис

```
ip firewall sessions tracking { <PROTOCOL> |  sip [ port <OBJECT-GROUP-SERVICE> ] }
no ip firewall sessions tracking { <PROTOCOL> |  sip [ port <OBJECT-GROUP-SERVICE> ] |
all }
```

Параметры

<PROTOCOL> – протокол уровня приложений, сессии которого должны отслеживаться, принимает значения [ftp, h323, pptp, netbios-ns];

<OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.

Вместо имени отдельного протокола можно использовать ключ "all", который включает функцию отслеживания сессий уровня приложений для всех доступных протоколов.

Значение по умолчанию

Отключено для всех протоколов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions tracking ftp
```

ip firewall sessions udp-assured-timeout

Данной командой определяется время жизни UDP-сессии в состоянии "соединение подтверждено", по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions udp-assured-timeout <TIME>
no ip firewall sessions udp-assured-timeout
```

Параметры

<TIME> – время жизни UDP-сессии в состоянии "соединение подтверждено ", принимает значения в секундах [1..8553600].

Значение по умолчанию

180 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions udp-assured-timeout 3600
```

ip firewall sessions udp-wait-timeout

Данной командой определяется время жизни UDP-сессии в состоянии «соединение не подтверждено», по истечении которого она считается устаревшей и удаляется из таблицы отслеживаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip firewall sessions udp-wait-timeout <TIME>
no ip firewall sessions udp-wait-timeout
```

Параметры

<TIME> – время жизни UDP-сессии в состоянии «соединение не подтверждено», принимает значения в секундах [1..8553600].

Значение по умолчанию

30 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions udp-wait-timeout 60
```

match application

Данной командой устанавливается профиль приложений, для которых должно срабатывать правило. Данная функция используется для фильтрации по приложениям (механизм DPI)

При использовании параметра «not» правило будет срабатывать для приложений, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] application <OBJ-GROUP-APPLICATION>
no match application
```

Параметры

<OBJ-GROUP-APPLICATION> – имя профиля приложений, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match application APP_DENY
```

match destination-address

Данной командой устанавливается профиль IP-адресов получателя, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для IP-адресов получателя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] destination-address <OBJ-GROUP-NETWORK-NAME>
no match destination-address
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match destination-address local
```

match destination-address-port

Данной командой устанавливается профиль связок IP-адресов и TCP/UDP-портов получателя, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для связок IP-адресов и TCP/UDP-портов получателя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] destination-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
```

```
no match destination-address
```

Параметры

<OBJ-GROUP-ADDRESS-PORT-NAME> – имя профиля связок IP-адресов и TCP/UDP-портов, задаётся строкой до 31 символа. При указании значения «any» правило не будет учитывать данный способ фильтрации.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match destination-address local
```

match destination-mac

Данной командой устанавливается MAC-адрес получателя, для которого должно срабатывать правило.

При использовании параметра «not» (match not) правило будет срабатывать для MAC-адресов получателя, отличных от указанного.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] destination-mac <ADDR>
no match destination-mac <ADDR>
```

Параметры

<ADDR> – MAC-адрес получателя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match destination-mac A8:F9:4B:AA:00:40
```

match destination-nat

Данной командой устанавливается ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя.

При использовании параметра «not» правило будет срабатывать для трафика, не измененного сервисом трансляции IP-адресов и портов получателя. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] destination-nat
no match destination-nat
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match destination-nat
```

match destination-port

Данной командой устанавливается профиль TCP/UDP-портов получателя, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для TCP/UDP-портов получателя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
match [not] destination-port <PORT-SET-NAME>
no match destination-port
```

Параметры

<PORT-SET-NAME> – имя профиля TCP/UDP-портов, задаётся строка до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match destination-port ssh
```

match fragment

Данной командой определяются фрагментированные пакеты, направленные на устройство. Команда применима только в правилах между зонами any self. Под действие правила попадают второй и последующие фрагменты пакета. Обработка пакетов этим правилом происходит до трансляции адресов DNAT.

При использовании параметра «not» правило будет срабатывать для нефрагментированных пакетов.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] fragment
no match fragmen
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match fragment
```

match icmp

Данная команда используется для настройки параметров протокола ICMP, если он выбран командой «match protocol». Данной командой устанавливается тип и код сообщений протокола ICMP, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для всех типов и кодов сообщений протокола ICMP, кроме указанных.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] icmp { <ICMP_TYPE> <ICMP_CODE> | <OPTION> }
no match icmp
```

Параметры

<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255];

<ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP;

<OPTION> – стандартные типы ICMP-сообщений, могут принимать значения:

- administratively-prohibited;
- alternate-address;
- conversion-error;
- dod-host-prohibited;
- dod-network-prohibited;
- echo;
- echo-reply;
- host-isolated;
- host-precedence;
- host-redirect;
- host-tos-redirect;
- host-tos-unreachable;
- host-unknown;
- host-unreachable;
- information-reply;
- information-request;
- mask-reply;
- mask-request;
- network-redirect;
- network-tos-redirect;
- network-tos-unreachable;
- network-unknown;
- network-unreachable;
- option-missing;
- packet-too-big;
- parameter-problem;
- port-unreachable;
- precedence;
- protocol-unreachable;
- reassembly-timeout;
- router-advertisement;
- router-solicitation;
- source-quench;

- source-route-failed;
- time-exceeded;
- timestamp-reply;
- timestamp-request;
- traceroute.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match icmp 2 any
```

match ip-option

Данной командой определяются пакеты, содержащие опции в IP-заголовках. Команда применима только в правилах между зонами any self.

При использовании параметра «not» правило будет срабатывать для пакетов, не содержащих опций в IP-заголовках.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] ip-option
no match ip-option
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match ip-options
```

match protocol

Данной командой устанавливается имя или номер IP-протокола, для которого должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для всех протоколов, кроме указанного.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] protocol <TYPE>
no match protocol
match [not] protocol-id <ID>
no match protocol-id
```

Параметры

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

При указании значения «any» правило будет срабатывать для любых протоколов.

<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match protocol udp
```

match source-address

Данной командой устанавливается профиль IP-адресов отправителя, для которых должно срабатывать правило.

При использовании параметра «not» (match not) правило будет срабатывать для IP-адресов отправителя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] source-address <OBJ-GROUP-NETWORK-NAME>
no match source-address <OBJ-GROUP-NETWORK-NAME>
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match source-address remote
```

match source-address-port

Данной командой устанавливается профиль связок IP-адресов и TCP/UDP-портов отправителя, для которых должно срабатывать правило.

При использовании параметра «not» (match not) правило будет срабатывать для связок IP-адресов и TCP/UDP-портов отправителя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
no match source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
```

Параметры

<OBJ-GROUP-ADDRESS-PORT-NAME> – имя профиля связок IP-адресов и TCP/UDP-портов, задаётся строкой до 31 символа. При указании значения «any» правило не будет учитывать данный способ фильтрации.

Значение по умолчанию

any

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match source-address-port admin
```

match source-mac

Данной командой устанавливается MAC-адрес отправителя, для которого должно срабатывать правило.

При использовании параметра «not» (match not) правило будет срабатывать для MAC-адресов отправителя, отличных от указанного.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] source-mac <ADDR>
no match source-mac <ADDR>
```

Параметры

<ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match source-mac A8:F9:4B:AA:00:40
```

match source-port

Данной командой устанавливается профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило.

При использовании параметра «not» правило будет срабатывать для TCP/UDP-портов отправителя, которые не входят в указанный профиль.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
match [not] source-port <PORT-SET-NAME>
no match source-port
```

Параметры

<PORT-SET-NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# match source-port telnet
```

ports firewall enable

Данная команда активирует фильтрацию и режим отслеживания сессий при прохождении пакетов между членами Bridge-интерфейса.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
[no] ports firewall enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-BRIDGE

Пример

```
wlc-30(config-bridge)# ports firewall enable
```

rate-limit pps

Данная команда ограничивает количество обрабатываемых правилом пакетов в секунду. Команда применима только в правилах между зонами any self и при условии действия action permit в этом правиле.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
rate-limit pps <RATE>
no rate-limit
```

Параметры

<PPS> – количество пакетов в секунду, принимает значения [1..10000].

Значение по умолчанию

Не ограничено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ZONE-PAIR-RULE

Пример

```
wlc-30(config-zone-pair-rule)# rate-limit pps 200
```

rearrange

Данная команда меняет шаг между созданными правилами.

Синтаксис

```
rearrange <VALUE>
```

Параметры

<VALUE> – шаг между правилами, принимает значения [1..50].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR

Пример

```
wlc-30(config-zone-pair)# rearrange 10
```

renumber rule

Данная команда меняет номер правила.

Синтаксис

```
renumber rule <CUR_ORDER> <NEW_ORDER>
```

Параметры

<CUR_ORDER> – текущий номер правила, принимает значения [1..10000];

<NEW_ORDER> – новый номер правила, принимает значения [1..10000].

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR

Пример

```
wlc-30(config-zone-pair)# renumber rule 13 100
```

rule

Данная команда используется для создания правила и перехода в командный режим SECURITY ZONE PAIR RULE. Правила обрабатываются устройством в порядке возрастания их номеров.

Использование отрицательной формы команды (no) удаляет указанное правило.

Синтаксис

```
[no] rule <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1..10000]. Если при удалении используется значение параметра "all", то будут удалены все правила для конфигурируемой пары зон безопасности.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZONE-PAIR

Пример

```
wlc-30(config-zone-pair)# rule 10
wlc-30(config-zone-rule)#
```

security zone

Данная команда используется для создания зон безопасности и перехода в режим конфигурирования зоны.

Использование отрицательной формы команды (no) удаляет заданную зону безопасности.

Синтаксис

```
[no] security zone [ <NAME> | all ]
```

Параметры

<NAME> – имя создаваемой зоны безопасности, задаётся строкой до 12 символов. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все зоны безопасности.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security zone trusted
wlc-30(config-zone)#
```

security-zone

Данная команда используется для добавления выбранного сетевого интерфейса в зону безопасности. Использование отрицательной формы команды (no) удаляет интерфейс из зоны.

Синтаксис

```
security-zone <NAME>
no security-zone
```

Параметры

<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-BRIDGE
CONFIG-CELLULAR-MODEM
CONFIG-E1
CONFIG-MULTILINK
CONFIG-VTI
CONFIG-GRE
CONFIG-IP4IP4
CONFIG-LT
CONFIG-PPPOE
CONFIG-PPTP
CONFIG-L2TP
CONFIG-OPENVPN
CONFIG-L2TP-SERVER
CONFIG-OPENVPN-SERVER
CONFIG-PPTP-SERVER

Пример

```
wlc-30(config-if-gi)# security-zone trusted
```

security zone-pair

Данная команда используется для создания группы правил для пары зон безопасности.

Использование отрицательной формы команды (no) удаляет указанную группу правил.

Синтаксис

```
[no] security zone-pair <SOURCE-ZONE> <DESTINATION-ZONE>
```

Параметры

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик. На контроллере всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам контроллер, то есть трафик не является транзитным, то в качестве параметра указывается зона «self». Если при удалении используется значение параметра «all», то будут удалены все конфигурируемые пары зон безопасности.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# security zone-pair trusted self
```

show ip firewall counters

Данная команда используется для просмотра статистики по пакетам, проходящим между зонами, для которых не установлена сессия.

Синтаксис

```
show ip firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE>
[ <ORDER> ] ] ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены счетчики правил в указанном VRF;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик;

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будет показана информация только по данному правилу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip firewall counters trusted self
Zone-pair                       Rule         Action            Pkts         Bytes
------------------------------  -----------  ----------------  -----------  -----------
any/any                         default      deny              0            0
trusted/self                    1            permit            0            0
trusted/trusted                 1            permit            0            0
```

show ip firewall sessions

Данная команда используется для просмотра активных IP-сессий.

Синтаксис

```
show ip firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address
<ADDR>] [ outside-source-address <ADDR> ]
[ inside-destination-address <ADDR> ] [ outside-destination-address <ADDR> ] [ inside-
source-port <PORT> ]
[ outside-source-port <PORT> ] [ inside-destination-port <PORT> ] [ outside-destination-
port <PORT> ] [ summary ] [ configuration ] [ expected ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сессии в указанном VRF;

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – TCP/UDP-порт, принимает значения [1..65535];

inside-source-address – команда для указания IP-адреса источника, приходящих пакетов;

inside-destination-address – команда для указания IP-адреса назначения, приходящих пакетов;

outiside-source-address – команда для указания IP-адреса источника, отправляемых пакетов;

outside-destination-address – команда для указания IP-адреса назначения отправляемых пакетов;

inside-source-port – ключ для указания TCP/UDP-порта отправителя в приходящих пакетах;

outside-source-port – ключ для указания TCP/UDP-порта отправителя в отправляемых пакетах;

inside-destination-port – ключ для указания TCP/UDP-порта назначения в приходящих пакетах;

outside-destination-port – ключ для указания TCP/UDP-порта назначения в отправляемых пакетах;

summary – выводит суммарную статистику по IP-сессиям;

configuration – выводит настройку таймаутов и объема таблиц IP-сессий;

expected – команда для отображения сессий, ожидающих обработки других сессий.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip firewall sessions
Prot Inside source  Inside destination  Outside source Outside destination Pkts Bytes
---  ------------  -----------------    -------------   -----------------  -----  ----
vrrp   4.4.4.4      224.0.0.18              4.4.4.4       224.0.0.18       --     --
```

show ip firewall sessions tracking

Данной командой отображается настройка функционала отслеживания сессий уровня приложений.

Синтаксис

```
show ip firewall sessions tracking
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip firewall sessions tracking
Tracking Status:
    FTP:         Enabled
    H.323:       Enabled
    GRE:         Enabled
    PPTP:        Enabled
    NETBIOS-NS: Enabled
    SIP:         Enabled
```

show ipv6 firewall counters

Данная команда используется для просмотра статистики по пакетам, проходящим между зонами, для которых не установлена сессия.

Синтаксис

```
show ipv6 firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE>
[ <ORDER> ] ] ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены счетчики правил в указанном VRF;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик;

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будет показана информация только по данному правилу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 firewall counters trusted self
Zone-pair                       Rule         Action            Pkts         Bytes
------------------------------  -----------  ----------------  -----------  -----------
any/any                         default      deny              0            0
trusted/self                    1            permit            0            0
trusted/trusted                 1            permit            0            0
```

show ipv6 firewall sessions

Данная команда используется для просмотра активных IPv6-сессий.

Синтаксис

```
show ipv6 firewall sessions [ vrf <VRF> ] [summary] [ protocol <TYPE> ] [ inside-source-address <IPV6-ADDR>] [ outiside-source-address <IPV6-ADDR> ]
[ inside-destination-address <IPV6-ADDR> ] [ outside-destination-address <IPV6-ADDR> ]
[ inside-source-port <PORT> ] [ outside-source-port <PORT> ]
[ inside-destination-port <PORT> ] [ outside-destination-port <PORT> ] [ expected ]
[ summary ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сессии в указанном VRF;

<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<PORT> – TCP/UDP-порт, принимает значения [1..65535];

inside-source-address – команда для указания IPv6-адреса источника, приходящих пакетов;

inside-destination-address – команда для указания IPv6-адреса назначения, приходящих пакетов;

outiside-source-address – команда для указания IPv6-адреса источника, отправляемых пакетов;
outside-destination-address – команда для указания IPv6-адреса назначения отправляемых пакетов;
inside-source-port – ключ для указания TCP/UDP-порта отправителя в приходящих пакетах;
outside-source-port – ключ для указания TCP/UDP-порта отправителя в отправляемых пакетах;
inside-destination-port – ключ для указания TCP/UDP-порта назначения в приходящих пакетах;
outside-destination-port – ключ для указания TCP/UDP-порта назначения в отправляемых пакетах;
expected – команда для отображения сессий, ожидающих обработки других сессий;
summary – выводит суммарную статистику по IPv6-сессиям.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 firewall sessions
Prot  Inside source  Inside destination  Outside source Outside destination  Pkts  Bytes
----- -------------- ------------------- -------------- -------------------- ----- -----
icmp6 fc00::2         fc00::2            fc00::2        fc00::2               --     --
icmp6 fc00::2         fc00::1            fc00::2        fc00::1               --     --
```

show security zone

Данная команда используется для просмотра интерфейсов, входящих в зону безопасности.

Синтаксис

```
show security zone [<NAME>]
```

Параметры

<NAME> – имя зоны, задаётся строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show security zone
Zone name       Interfaces
-------------   ----------------------------------------
trusted         gi1/0/2-6, gi1/0/8-24, bridge 1
untrusted       gi1/0/1, te1/0/1-2, bridge 2
```

show security zone-pair

Данная команда используется для просмотра списка пар зон.

Синтаксис

```
show security zone-pair
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show security zone-pair
From zone       To zone
-------------   -------------
trusted         untrusted
trusted         trusted
trusted         self
untrusted       self
```

show security zone-pair configuration

Данная команда используется для просмотра правил для пары зон безопасности.

Синтаксис

```
show security zone-pair configuration <SOURCE-ZONE> <DESTINATION-ZONE> [<ORDER>]
```

Параметры

<SOURCE-ZONE> – зона безопасности, из которой поступает трафик;

<DESTINATION-ZONE> – зона безопасности, в которую поступает трафик;

<ORDER> – номер правила, принимает значения [1..10000]. При указании номера правила будет показана информация только по данному правилу.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show security zone-pair configuration trusted self
Order:              1
Description:        --
Matching pattern:
    Protocol:       tcp(6)
    Src-addr:       any
    src-port:       any
    Dest-addr:      any
    dest-port:      23
0            0
```

Управление логированием и защитой от сетевых атак

- Управление защитой от сетевых атак
  - ip firewall screen dos-defense icmp-threshold
  - ip firewall screen dos-defense land
  - ip firewall screen dos-defense limit-session-destination
  - ip firewall screen dos-defense limit-session-source
  - ip firewall screen dos-defense syn-flood
  - ip firewall screen dos-defense udp-threshold
  - ip firewall screen dos-defense winnuke
  - ip firewall screen spy-blocking fin-no-ack
  - ip firewall screen spy-blocking icmp-type destination-unreachable
  - ip firewall screen spy-blocking icmp-type echo-request
  - ip firewall screen spy-blocking icmp-type reserved
  - ip firewall screen spy-blocking icmp-type source-quench
  - ip firewall screen spy-blocking icmp-type time-exceeded
  - ip firewall screen spy-blocking ip-sweep
  - ip firewall screen spy-blocking port-scan
  - ip firewall screen spy-blocking spoofing
  - ip firewall screen spy-blocking syn-fin
  - ip firewall screen spy-blocking tcp-all-flags
  - ip firewall screen spy-blocking tcp-no-flag
  - ip firewall screen suspicious-packets icmp-fragment
  - ip firewall screen suspicious-packets ip-fragment
  - ip firewall screen suspicious-packets large-icmp
  - ip firewall screen suspicious-packets syn-fragment
  - ip firewall screen suspicious-packets udp-fragment
  - ip firewall screen suspicious-packets unknown-protocols
- Управление оповещением о сетевых атаках
  - ip firewall logging interval
  - logging firewall screen detailed
  - logging firewall screen dos-defense
  - logging firewall screen spy-blocking
  - logging firewall screen suspicious-packets
  - show ip firewall screens counters

Управление защитой от сетевых атак

ip firewall screen dos-defense icmp-threshold

Данная команда включает защиту от ICMP flood атак. При включенной защите ограничивается количество icmp-пакетов всех типов в секунду для одного адреса назначения.

Использование отрицательной формы команды (no) отключает защиту от ICMP flood атак.

Синтаксис

```
ip firewall screen dos-defense icmp-threshold <NUM>
no ip firewall screen dos-defense icmp-threshold
```

Параметры

<NUM> – количество icmp-пакетов в секунду задается в диапазоне [1..10000].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense icmp-threshold 2000
```

ip firewall screen dos-defense land

Данная команда включает защиту от land-атак. При включенной защите блокируются пакеты с одинаковыми source и destination ip, и флагом SYN в заголовке TCP.

Использование отрицательной формы команды (no) отключает защиту от land-атак.

Синтаксис

```
[no] ip firewall screen dos-defense land
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense land
```

ip firewall screen dos-defense limit-session-destination

Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду на один адреса назначения, которое смягчает DoS-атаки.

Использование отрицательной формы команды (no) снимает это ограничение.

Синтаксис

```
ip firewall screen dos-defense limit-session-destination <NUM>
no ip firewall screen dos-defense limit-session-destination
```

Параметры

<NUM> – ограничение количества ip-пакетов в секунду задается в диапазоне [1..10000].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense limit-session-destination 1000
```

ip firewall screen dos-defense limit-session-source

Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду с одного адреса источника, которое смягчает DoS-атаки.

Использование отрицательной формы команды (no) снимает это ограничение.

Синтаксис

```
ip firewall screen dos-defense limit-session-source <NUM>
no ip firewall screen dos-defense limit-session-source
```

Параметры

<NUM> – ограничение количества ip-пакетов в секунду задается в диапазоне [1..10000].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense limit-session-source 1000
```

ip firewall screen dos-defense syn-flood

Данная команда включает защиту от SYN flood атак. При включенной защите ограничивается количество TCP пакетов с установленным флагом SYN в секунду для одного адреса назначения.

Использование отрицательной формы команды (no) отключает защиту от SYN flood атак.

Синтаксис

```
ip firewall screen dos-defense syn-flood <NUM> [src-dst]
no ip firewall screen dos-defense syn-flood
```

Параметры

<NUM> – максимальное количество TCP-пакетов с установленным флагом SYN в секунду задается в диапазоне [1..10000];

src-dst – ограничение количества TCP-пакетов с установленным флагом SYN на основании адреса источника и адреса назначения.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense syn-flood 100 src-dsr
```

ip firewall screen dos-defense udp-threshold

Данная команда включает защиту от UDP flood атак. При включенной защите ограничивается количество UDP-пакетов в секунду для одного адреса назначения.

Использование отрицательной формы команды (no) отключает защиту от UDP flood.

Синтаксис

```
ip firewall screen dos-defense udp-threshold <NUM>
no ip firewall screen dos-defense udp-threshold
```

Параметры

<NUM> – максимальное количество UDP-пакетов в секунду задается в диапазоне [1..10000].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense udp-threshold
```

ip firewall screen dos-defense winnuke

Данная команда включает защиту от winnuke-атак. При включенной защите блокируются TCP-пакеты с установленным флагом URG и 139 портом назначения.

Использование отрицательной формы команды (no) отключает защиту от winnuke-атак.

Синтаксис

```
[no] ip firewall screen dos-defense winnuke
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen dos-defense winnuke
```

ip firewall screen spy-blocking fin-no-ack

Данная команда включает блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK.

Использование отрицательной формы команды (no) отключает блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK.

Синтаксис

```
[no] ip firewall screen spy-blocking fin-no-ack
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking fin-no-ack
```

ip firewall screen spy-blocking icmp-type destination-unreachable

Данная команда включает блокировку всех ICMP-пакетов 3 типа (destination-unreachable), включая пакеты, сгенерированные самим контроллером.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов 3 типа.

Синтаксис

```
[no] ip firewall screen spy-blocking icmp-type destination-unreachable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking icmp-type destination-unreachable
```

ip firewall screen spy-blocking icmp-type echo-request

Данная команда включает блокировку всех ICMP пакетов 8 типа (echo-request), включая пакеты, сгенерированные самим контроллером.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов 8 типа.

Синтаксис

```
[no] ip firewall screen spy-blocking icmp-type echo-request
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking icmp-type echo-request
```

ip firewall screen spy-blocking icmp-type reserved

Данная команда включает блокировку всех ICMP-пакетов 2 и 7 типов (reserved), включая пакеты, сгенерированные самим контроллером.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов 2 и 7 типов.

Синтаксис

```
[no] ip firewall screen spy-blocking icmp-type reserved
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking icmp-type reserved
```

ip firewall screen spy-blocking icmp-type source-quench

Данная команда включает блокировку всех ICMP-пакетов 4 типа (source quench), включая пакеты, сгенерированные самим контроллером.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов 4 типа.

Синтаксис

```
[no] ip firewall screen spy-blocking icmp-type source-quench
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking icmp-type source-quench
```

ip firewall screen spy-blocking icmp-type time-exceeded

Данная команда включает блокировку всех ICMP-пакетов 11 типа (time exceeded), включая пакеты, сгенерированные самим контроллером.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов 11 типа.

Синтаксис

```
[no] ip firewall screen spy-blocking icmp-type time-exceeded
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking icmp-type time-exceeded
```

ip firewall screen spy-blocking ip-sweep

Данная команда включает защиту от IP-sweep атак. При включенной защите, если в течение заданного в параметрах интервала приходит более 10 ICMP-запросов от одного источника, первые 10 запросов пропускаются контроллером, а 11 и последующие отбрасываются на оставшееся время интервала.

Использование отрицательной формы команды (no) отключает защиту от ip-sweep атак.

Синтаксис

`ip firewall screen spy-blocking ip-sweep <THRESHOLD> [ <TIME> ]`

`no ip firewall screen spy-blocking ip-sweep`

Параметры

<THRESHOLD> – количество пакетов ip sweep атаки в секунду, задается в диапазоне [1..10000];

<TIME> – время блокировки в миллисекундах [1..1000000].

Значение по умолчанию

Отключено.

Без указания времени блокировки при включении, устанавливается значение 10000.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking ip-sweep 1000
```

ip firewall screen spy-blocking port-scan

Данная команда включает защиту от port scan атак. Если в течение первого заданного интервала времени (<threshold>) на один источник приходит более 10 TCP-пакетов с флагом SYN на разные TCP-порты или более 10 UDP-пакетов на разные UDP-порты, то такое поведение фиксируется как port scan

атака и все последующие пакеты такого рода от источника блокируются на второй заданный интервал времени (<TIME>).

Использование отрицательной формы команды (no) отключает защиту от port scan атак.

Синтаксис

```
ip firewall screen spy-blocking port-scan <THRESHOLD> [ <TIME> ]
no ip firewall screen spy-blocking port-scan
```

Параметры

<THRESHOLD> – количество пакетов port scan атаки в секунду, указывается в диапазоне [1..10000];

<TIME> – время блокировки в миллисекундах [1..1000000].

Значение по умолчанию

Отключено.

Без указания времени блокировки при включении устанавливается значение 10000.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking port-scan 100 1000
```

ip firewall screen spy-blocking spoofing

Данная команда включает защиту от IP spoofing атак. При включенной защите контроллер проверяет пакеты на соответствие адреса источника и записей в таблице маршрутизации и в случае несоответствия пакет отбрасывается. Например, если пакет с адресом источника 10.0.0.1/24 приходит на интерфейс Gi1/0/1, а в таблице маршрутизации данная подсеть располагается за интерфейсом Gi1/0/2, то считается, что адрес источника был подменен.

Использование отрицательной формы команды (no) отключает защиту от ip spoofing атак.

Синтаксис

```
[no] ip firewall screen spy-blocking spoofing
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking spoofing
```

ip firewall screen spy-blocking syn-fin

Данная команда включает блокировку TCP-пакетов, с установленными флагами SYN и FIN.

Использование отрицательной формы команды (no) отключает блокировку TCP-пакетов, с установленными флагами SYN и FIN.

Синтаксис

```
[no] ip firewall screen spy-blocking syn-fin
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking syn-fin
```

ip firewall screen spy-blocking tcp-all-flags

Данная команда включает блокировку TCP-пакетов, со всеми флагами или с набором флагов: FIN, PSH, URG. Обеспечивается защита от атаки XMAS.

Использование отрицательной формы команды (no) отключает блокировку TCP-пакетов со всеми флагами или с набором флагов: FIN, PSH, URG.

Синтаксис

```
[no] ip firewall screen spy-blocking tcp-all-flag
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking tcp-all-flag
```

ip firewall screen spy-blocking tcp-no-flag

Данная команда включает блокировку TCP-пакетов, с нулевым полем flags.

Использование отрицательной формы команды (no) отключает блокировку TCP-пакетов, с нулевым полем flags.

Синтаксис

```
[no] ip firewall screen spy-blocking tcp-no-flag
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen spy-blocking tcp-no-flag
```

ip firewall screen suspicious-packets icmp-fragment

Данная команда включает блокировку фрагментированных ICMP-пакетов.

Использование отрицательной формы команды (no) отключает блокировку фрагментированных ICMP-пакетов.

Синтаксис

```
[no] ip firewall screen suspicious-packets icmp-fragment
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets icmp-fragment
```

ip firewall screen suspicious-packets ip-fragment

Данная команда включает блокировку фрагментированных IP-пакетов.

Использование отрицательной формы команды (no) отключает блокировку фрагментированных пакетов.

Синтаксис

```
[no] ip firewall screen suspicious-packets ip-fragment
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets ip-fragment
```

ip firewall screen suspicious-packets large-icmp

Данная команда включает блокировку ICMP-пакетов длиной более 1024 байт.

Использование отрицательной формы команды (no) отключает блокировку ICMP-пакетов длиной более 1024 байт.

Синтаксис

```
[no] ip firewall screen suspicious-packets large-icmp
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets large-icmp
```

ip firewall screen suspicious-packets syn-fragment

Данная команда включает блокировку фрагментированных TCP-пакетов, с флагом SYN.

Использование отрицательной формы команды (no) отключает блокировку фрагментированных TCP-пакетов, с флагом SYN.

Синтаксис

```
[no] ip firewall screen suspicious-packets syn-fragment
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets syn-fragment
```

ip firewall screen suspicious-packets udp-fragment

Данная команда включает блокировку фрагментированных UDP-пакетов.

Использование отрицательной формы команды (no) отключает блокировку фрагментированных UDP-пакетов.

Синтаксис

```
[no] ip firewall screen suspicious-packets udp-fragment
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets udp-fragment
```

ip firewall screen suspicious-packets unknown-protocols

Данная команда включает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.

Использование отрицательной формы команды (no) отключает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.

Синтаксис

```
[no] ip firewall screen suspicious-packets unknown-protocols
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall screen suspicious-packets unknown-protocols
```

Управление оповещением о сетевых атаках

ip firewall logging interval

Данной командой устанавливается частота оповещения (по SNMP, syslog и в CLI) об обнаруженных и отраженных сетевых атаках. При детектировании атаки сообщение логируется мгновенно, но следующие оповещения о данной конкретной атаке будут логироваться через заданный интервал времени, если атака будет носить продолжительный характер.

Использование отрицательной формы команды (no) возвращает таймер к значению по умолчанию.

Синтаксис

`ip firewall logging interval <NUM>`

`no ip firewall logging interval`

Параметры

<NUM> – интервал времени в секундах [30 .. 2147483647].

Значение по умолчанию

30

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall logging interval 60
```

logging firewall screen detailed

Данной командой включается более детальный вывод сообщений по обнаруженным и отраженным сетевым атакам в CLI.

В детальном выводе, кроме имени интерфейса, с которого пришёл пакет, отображается IP-адрес источника и IP-адрес назначения этого пакета, а также MAC-адрес источника, отправившего этот пакет.

Использование отрицательной формы команды (no) отключает детальный вывод сообщений.

Синтаксис

```
[no] logging firewall screen detailed
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging firewall screen detailed
```

logging firewall screen dos-defense

Данной командой включается механизм обнаружения и логирования DoS-атак через CLI, syslog и по SNMP. В связке с включенной защитой от атак будет производиться оповещение об отраженных DoS-атаках.

Использование отрицательной формы команды (no) отключает механизм обнаружения и логирования обнаруженных и отраженных DoS-атак.

Синтаксис

```
[no] logging firewall screen dos-defense <ATACK_TYPE>
```

Параметры

<ATACK_TYPE> – тип DoS-атаки, принимает значения:

- icmp-threshold;
- land;

- limit-session-destination;
- limit-session-source;
- syn-flood;
- udp-threshold;
- winnuke.

Подробное описание DoS-атак приведено в разделе Управление защитой от сетевых атак.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging firewall screen dos-defense land
```

logging firewall screen spy-blocking

Данной командой включается механизм обнаружения и логирования шпионской активности через CLI, syslog и по SNMP. В связке с включенной защитой от шпионской активности будет производиться оповещение о блокированной шпионской активности.

Использование отрицательной формы команды (no) отключает механизм обнаружения и логирования обнаруженной и блокированной шпионской активности.

Синтаксис

```
[no] logging firewall screen spy-blocking { <ATACK_TYPE> | icmp-type <ICMP_TYPE> }
```

Параметры

<ATACK_TYPE> – тип шпионской активности, принимает значения:

- fin-no-ack;
- ip-sweep;
- port-scan;
- spoofing;
- syn-fin;
- tcp-all-flag;
- tcp-no-flag.

<ICMP_TYPE> – тип icmp, принимает значения:

- destination-unreachable;
- echo-request;
- reserved;
- source-quench;
- time-exceeded.

Подробное описание шпионских активностей приведено в разделе Управление защитой от сетевых атак.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging firewall screen spy-blocking icmp-type echo-request
```

logging firewall screen suspicious-packets

Данной командой включается механизм обнаружения нестандартных пакетов и логирования через CLI, syslog и по SNMP. В связке с включенной защитой от нестандартных пакетов будет производиться также оповещение о блокировке нестандартных пакетов.

Использование отрицательной формы команды (no) отключает механизм обнаружения и логирования обнаруженных и блокированных нестандартных пакетов.

Синтаксис

```
[no] logging firewall screen suspicious-packets <PACKET_TYPE>
```

Параметры

< PACKET_TYPE> – тип нестандартных пакетов, принимает значения:

- icmp-fragment;
- ip-fragment;
- large-icmp;
- syn-fragment;
- udp-fragment;
- unknown-protocols.

Подробное описание защиты от нестандартных пакетов приведено в разделе Управление защитой от сетевых атак.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging firewall screen suspicious-packets icmp-fragment
```

show ip firewall screens counters

Данная команда позволяет просматривать статистику по обнаруженным сетевым атакам.

Синтаксис

```
show ip firewall screens counters
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show ip firewall screens counters
DDoS:
    Destination limit screen:  --
    Source limit screen:       --
    ICMP threshold screen:     1
    UDP threshold screen:      --
    SYN flood screen:          0
    Land attack screen:        1
    Winnuke attack screen:     --
Suspicious packets:
    ICMP fragmented screen:    --
    UDP fragmented screen:     --
    Large ICMP screen:         4
    Fragmented SYN screen:     --
    Unknown protocol screen:   --
    Fragmented IP screen:      --
Spying:
    Port scanning screen:      --
    IP sweep secreen:          --
    SYN-FIN screen:            --
    TCP all flags screen:      --
    FIN no ACK screen:         --
    TCP no flags screen:       --
    Spoofing screen:           --
ICMP types:
    ICMP reserved screen:      --
    ICMP quench screen:        --
    ICMP echo request screen:  --
    ICMP time exceeded screen: --
    ICMP unreachable screen:   --
```

Управление фильтрацией

- default action
- description
- filter
- log enable
- ip http profile
- ip http proxy
- ip http proxy aaa das-profile
- ip http proxy listen-ports
- ip http proxy redirect-port
- ip http proxy server-url
- ip https proxy
- ip https proxy listen-ports
- ip https proxy redirect-port
- urls local
- urls remote

default action

Данной командой устанавливается действие для обработки трафика неавторизованных пользователей.

Использование отрицательной формы команды (no) удаляет действие для обработки трафика неавторизованных пользователей.

Синтаксис

```
default action <ACTION> { redirect-url <REDIRECT-URL>}
```

```
no default action
```

Параметры

<ACTION> – действие, которое будет происходить для трафика никак не описанного в профиле. Возможные значения:

- permit – пропускать http-запросы;
- deny – блокировать http-запросы;
- redirect – перенаправлять запросы на определенный url-адрес.

<REDIRECT-URL> – url-адрес для перенаправления http-запросов. Указывается только в режиме redirect.

Значение по умолчанию

Не задано.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROXY-PROFILE

Пример

```
wlc-30(config-proxy-profile)# default action deny
```

description

Данной командой задаётся описание профиля фильтрации.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-PROXY-PROFILE

Пример

```
wlc-30(config-proxy-profile)# description "deny any"
```

filter

Данной командой включается режим фильтрации данных.

Использование отрицательной формы команды (no) режим фильтрации данных отключается.

Синтаксис

```
[no] filter <DATA-TYPE>
```

Параметры

<DATA-TYPE> тип данных подлежащих фильтрации. Может принимать значения:

- activex
- cookie
- js

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROXY-PROFILE

Пример

```
wlc-30(config-proxy-profile)# filter cookie
```

log enable

Данной командой включается ведение журнала профиля прокси-сервера.

Использование отрицательной формы команды (no) ведение журнала отключается.

Синтаксис

```
[no] log enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROXY-PROFILE

Пример

```
wlc-30(config-proxy-profile)# log enable
```

ip http profile

Данной командой создается профиль фильтрации HTTP-трафика и производится переход в режим конфигурирования созданного профиля.

Использование отрицательной формы команды (no) удаляет профиль фильтрации HTTP-трафика.

Синтаксис

```
[no] ip http profile <NAME>
```

Параметры

<NAME> – имя профиля фильтрации HTTP-трафика, задается строкой длинной [1..31] символ.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip http profile HTTP-BLOCKED
```

ip http proxy

Данной командой на интерфейс или туннель назначается профиль фильтрации http-запросов.

Использование отрицательной формы команды (no) профиль фильтрации http-запросов удаляется.

Синтаксис

```
ip http proxy <NAME>
no ip http proxy
```

Параметры

<NAME> – имя профиля. Задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-VTI

CONFIG-LT

CONFIG-PPPOE

Пример

```
wlc-30(config-cellular-modem)# ip http proxy HTTP-BLOCKED
```

ip http proxy aaa das-profile

Данная команда используется для выбора профиля серверов динамической авторизации (DAS), на которые будут приходить CoA запросы от PCRF об изменении списков URL.

Использование отрицательной формы команды (no) удаляет профиль динамической авторизации.

Синтаксис

```
ip http proxy aaa das-profile <NAME>
no ip http proxy aaa das-profile
```

Параметры

<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.

Значение по умолчанию

Профиль не задан.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip http proxy aaa das-profile my_server
```

ip http proxy listen-ports

Данной командой устанавливается список дополнительных tcp-портов для фильтрации http-запросов (в дополнение к стандартным 80 и 8080).

Использование отрицательной формы команды (no) удаляет ранее созданный список.

Синтаксис

```
[no] ip http proxy listen-ports <SERVICE_OBJ_GROUP_NAME>
```

Параметры

<SERVICE_OBJ_GROUP_NAME> – профиль портов (object-group service). Задается строкой до 31 символа.

Значение по умолчанию

80, 8080

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip http proxy listen-ports HTTP-ADD
```

ip http proxy redirect-port

Данной командой определяется базовый порт HTTP Proxy-сервера на контроллере. Количество используемых портов соответствует числу ядер процессора.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip http proxy redirect-port <PORT>
no ip http proxy redirect-port
```

Параметры

<PORT> – номер порта, указывается в диапазоне [1..65535].

Значение по умолчанию

3128

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip proxy http redirect-port 3001
```

ip http proxy server-url

Данной командой задается URL-адрес сервера, с которого будет загружаться список фильтрации.

Использование отрицательной формы команды (no) удаляет URL-адрес сервера.

Синтаксис

```
[no] ip http proxy server-url <URL>
```

Параметры

<URL> – URL-адрес ресурса, откуда необходимо скачивать файл со списком фильтрации. Задается строкой до [8..255] символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip http proxy server-url http://domain.example
```

ip https proxy

Данной командой на интерфейс или туннель назначается профиль фильтрации https-запросов.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip https proxy <NAME>
no ip https proxy
```

Параметры

<NAME> – имя профиля. Задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-VTI

CONFIG-LT

CONFIG-PPPOE

Пример

```
wlc-30(config-cellular-modem)# ip https proxy HTTPS-BLOCKED
```

ip https proxy listen-ports

Данной командой устанавливается список дополнительных tcp-портов для фильтрации https-запросов (в дополнение к стандартному 433).

Использование отрицательной формы команды (no) удаляет ранее созданный список.

Синтаксис

```
[no] ip https proxy listen-ports <SERVICE_OBJ_GROUP_NAME>
```

Параметры

<SERVICE_OBJ_GROUP_NAME> – профиль портов (object-group service). Задается строкой до 31 символа.

Значение по умолчанию

433

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip https proxy listen-ports HTTPS-ADD
```

ip https proxy redirect-port

Данной командой определяется базовый порт HTTPS Proxy-сервера на контроллере. Количество используемых портов соответствует числу ядер процессора.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip https proxy redirect-port <PORT>
```

```
no ip https proxy redirect-port
```

Параметры

<PORT> – номер порта, указывается в диапазоне [1..65535].

Значение по умолчанию

3129

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip proxy https redirect-port 3001
```

urls local

Данной командой в профиль фильтрации добавляется локальный список URL-адресов и действий для данного списка.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
urls local <URL_OBJ_GROUP_NAME> action { deny | permit | redirect redirect-url <REDIRECT-URL> }
```

```
no urls local
```

Параметры

<URL_OBJ_GROUP_NAME> – список URL, для которых будет применяться действие;

permit – пропускать http-запросы на адреса, описанные в указанном списке URL;

deny – блокировать http-запросы на адреса, описанные в указанном списке URL;

redirect – перенаправлять запросы на адреса, описанные в указанном списке URL на определенный URL-адрес;

<REDIRECT-URL> – URL-адрес для перенаправления http-запросов. Указывается только в режиме redirect.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROFILE

Пример

```
wlc-30(config-profile)# urls local OGU_DENY action deny
```

urls remote

Данной командой в профиль фильтрации добавляется ссылка на удаленный список url-адресов и действий для данного списка.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
urls remote <FILE-NAME> action { deny | permit | redirect redirect-url <REDIRECT-URL> }
no urls remote
```

Параметры

<FILE-NAME> – имя файла, содержащее список URL и расположенного на сервере прописанном в команде ip http proxy server-url (см. раздел ip http proxy server-url). Имя файла задается строкой до 31 символов;

permit – пропускать http-запросы на адреса, описанные в файле с указанным именем;

deny – блокировать http-запросы на адреса, описанные в файле с указанным именем;

redirect – перенаправлять запросы на адреса, описанные в файле с указанным именем на определенный URL-адрес.

<REDIRECT-URL> – URL-адрес для перенаправления http-запросов. Указывается только в режиме redirect.

Необходимый уровень привилегий

15

Командный режим

CONFIG-PROFILE

Пример

```
wlc-30(config-profile)# urls remote http-deny action deny
```

Настройка системы предотвращения вторжений (IPS/IDS)

- Общие команды IPS/IDS
  - description
  - enable
  - show security ips content-provider
  - show security ips content-provider rules-info
  - show security ips counters
  - show security ips status
  - show security ips user-server
  - update security ips content-provider rules
  - update security ips content-provider rules-info
  - update security ips user-server rules
- Настройка политики IPS/IDS
  - category
  - external network-group
  - protect network-group
  - rules action
  - rules count
  - security ips policy
  - vendor
- Настройка IPS
  - logging ips severity
  - logging remote-server
  - logging update-interval
  - security ips
  - performance max
  - policy
  - service-ips enable
- Настройка автообновления правил IPS/IDS, распространяемых по коммерческой лицензии
  - content-provider
  - host address
  - host port
  - location
  - reboot
  - storage-path
  - system-name
  - upgrade interval
- Настройка автообновления правил IPS/IDS из внешних источников
  - auto-upgrade
  - upgrade interval
  - url
  - user-server
- Настройка пользовательских правил IPS/IDS
  - action
  - destination-address
  - destination-port
  - direction
  - ip dscp
  - ip ftp command
  - ip ftp-data command
  - ip http
  - ip http content-filter
  - ip http method
  - ip icmp code

    - ip icmp code comparison-operator
    - ip icmp id
    - ip icmp sequence-id
    - ip icmp type
    - ip icmp type comparison-operator
    - ip protocol-id
    - ip tcp acknowledgment-number
    - ip tcp sequence-id
    - ip tcp window-size
    - ip ttl
    - ip ttl comparison-operator
    - meta classification-type
    - meta log-message
    - payload content
    - payload data-size
    - payload data-size comparison-operator
    - payload depth
    - payload no-case
    - payload offset
    - protocol
    - rule
    - security ips-category user-defined
    - source-address
    - source-port
    - threshold count
    - threshold second
    - threshold track
    - threshold type
- Настройка расширенных пользовательских правил
    - rule-advanced
    - rule-text

Общие команды IPS/IDS

description

Данной командой выполняется изменение описания.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPS-CATEGORY

CONFIG-IPS-CATEGORY-RULE

CONFIG-IPS-POLICY

CONFIG-IPS-UPGRADE-USER-SERVER

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-ips-upgrade-user-server)# description "Etnetera aggressive IP blacklist"
```

enable

Данной командой активируется сервис IPS/IDS и его правила.

Использование отрицательной формы команды (no) деактивирует сервис IPS/IDS.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

IPS/IDS-сервис не активирован.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

CONFIG-IPS-CATEGORY-RULE

CONFIG-CONTENT-PROVIDER

CONFIG-IPS-UPGRADE-USER-SERVER

Пример

```
wlc-30(config-ips)# enable
```

show security ips content-provider

Данной командой выполняется просмотр информации об обновлении правил IPS/IDS, распространяемых по коммерческой лицензии.

Синтаксис

```
show security ips content-provider
```

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ips content-provider
 Server: content-provider
        Last MD5 of received files:        93633ab9a73248ea50d58c25b1ac806c
        Next update: 06 October 2020 12:27:40
```

show security ips content-provider rules-info

Данной командой выполняется просмотр информации о категориях правил IPS/IDS, доступных по текущей коммерческой лицензии. При отсутствии действующей лицензии список будет пуст.

Синтаксис

```
show security ips content-provider rules-info
```

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ips content-provider rules-info
Vendor : kaspersky
    Category : IoTURLsDF
        Count of rules : 8000
        Description : Kasperksy Lab IoTURLsDF feed
              IoTURLsDF URL feed - a set of URLs with context covering malware that infects IoT
(Internet of Things) devices
    Category : MaliciousHashDF
        Count of rules : 1
        Description : Kasperksy Lab MaliciousHashDF feed
              Malicious Hash feed - a set of hashes of malicious objects
    Category : PhishingURLsDF
        Count of rules : 11167
        Description : Kasperksy Lab PhishingURLsDF feed
              Phishing URL feed - a set of URLs with context that cover phishing websites and
web pages
```

show security ips counters

Данной командой выполняется просмотр счетчиков работы правил сервиса IPS/IDS.

Синтаксис

```
show security ips counters
```

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ips counters
TCP flows processed : 34687
Alerts generated : 456
Blocked by ips engine : 78
Accepted by ips engine : 1356436
```

show security ips status

Данной командой выполняется просмотр числа правил, используемых в текущий момент системой IPS/IDS.

Синтаксис

```
show security ips status [detailed]
```

Параметры

detailed – показывает расширенную информацию об используемых правилах.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show security ips status

Rule files processed:         3
Rules successfully loaded:    21724
Rules failed:                 0


wlc-30# show security ips status detailed
Rule files processed:         3
Rules successfully loaded:    21724
Rules failed:                 0
Rules processed:              21727
IP-only inspecting:           1
Payload inspecting:           3980
Application layer inspecting: 18951
Decoder event:                0
```

show security ips user-server

Данной командой выполняется просмотр информации об обновлении правил IPS/IDS с пользовательских серверов обновлений.

Синтаксис

show security ips user-server [<WORD>]

Параметры

<WORD> – имя сервера задается строкой от 1 до 64 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# sh security ips user-server
Server name                      Files MD5                         Next update
---------------------------------   ---------------------------------
---------------------------------
content-provider                 93633ab9a73248ea50d58c25b1ac806c   06 October 2020 12:27:40
TH                               919f51bdf44052bfc0953362aef11c0d   06 October 2020 12:36:40
Traffic-ID                       e5e2f6472a397227c0d96f5df430a207   06 October 2020 12:36:40
Aggressive                       cfc3547b50f3f9fec366ba5a1e51cd1f   06 October 2020 12:36:40
JA3-Fingerprint                  439aa6e57c66826b92337672937d505b   05 October 2020 16:51:40
C2-Botnet                        39e118bd3884b3dc1df4ca3a03c05df1   05 October 2020 16:51:40
SSL-BlackList                    1d9c969f25791b9ee8c8c0ab8449d849   05 October 2020 16:51:40
ET-Open                          d53d92248a1f7cdc040d669a76cf27bc   06 October 2020 12:36:40
```

update security ips content-provider rules

Данной командой инициируется принудительное обновление правил IPS/IDS, распространяемых по коммерческой лицензии.

Фактическое начало процедуры обновления правил происходит с некоторой задержкой после введения команды. Максимальная величина задержки составляет 5 минут.

Синтаксис

```
update security ips content-provider rules
```

Необходимый уровень привилегий

15

Командный режимupdate security ips content-provider rules

ROOT

Пример

```
wlc-30# update security ips content-provider rules
```

update security ips content-provider rules-info

Данной командой инициируется принудительный запрос информации о категориях правил IPS/IDS, доступных по текущей коммерческой лицензии.

Фактическое начало процедуры обновления правил происходит с некоторой задержкой после введения команды. Максимальная величина задержки составляет 5 минут.

Синтаксис

```
update security ips content-provider rules-info
```

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# update security ips content-provider rules-info
```

update security ips user-server rules

Данной командой инициируется принудительное обновление правил IPS/IDS с пользовательского сервера обновлений.

Фактическое начало процедуры обновления правил происходит с некоторой задержкой после введения команды. Максимальная величина задержки составляет 5 минут.

Синтаксис

```
update security ips user-server rules <WORD>
```

Параметры

<WORD> – имя сервера задается строкой от 1 до 64 символа.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# update security ips user-server rules ET-Open
```

Настройка политики IPS/IDS

category

Данной командой определяется категория правил IPS/IDS определённого вендора, распространяемых по коммерческой лицензии, и осуществляется переход в режим настройки данной категории

Использование отрицательной формы команды (no) удаляет сконфигурированную категорию из настроек сервиса IPS/IDS.

Синтаксис

```
category <CATEGORY>
no category { <CATEGORY> | all }
```

Параметры

<CATEGORY> – категория правил.

Список доступных категорий можно посмотреть в контекстной подсказке или командой:

```
show security ips content-provider rules-info
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-VENDOR

Пример

```
wlc-30(config-ips-vendor)# category MobileBotnetCAndCDF
```

external network-group

Данной командой устанавливается профиль IP-адресов, которые сервис IPS/IDS будет считать ненадежными.

Сам профиль IP-адресов должен быть предварительно создан.

Использование отрицательной формы команды (no) удаляет сконфигурированный профиль из настроек сервиса IPS/IDS.

Синтаксис

```
external network-group <OBJ-GROUP-NETWORK-NAME>
no external network-group
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-POLICY

Пример

```
wlc-30(config-ips-policy)# external network-group WAN
```

protect network-group

Данной командой устанавливается профиль IP-адресов, которые будет защищать сервис IPS/IDS.

Сам профиль IP-адресов должен быть предварительно создан.

Использование отрицательной формы команды (no) удаляет сконфигурированный профиль из настроек сервиса IPS/IDS.

Синтаксис

```
protect network-group <OBJ-GROUP-NETWORK-NAME>
no protect network-group
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-POLICY

Пример

```
wlc-30(config-ips-policy)# protect network-group LAN
```

rules action

Данная команда используется для указания действия, которое должно быть применено для трафика, удовлетворяющего правилам данной категории.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Команда применима только для правил, распространяемых по коммерческой лицензии.

Синтаксис

```
rules action { alert | reject | pass | drop }
no rules action
```

Параметры:

- alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение;
- reject – прохождение трафика запрещается. Если это TCP-трафик отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение;
- pass – прохождение трафика разрешается;
- drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-VENDOR-CATEGORY

Пример

```
wlc-30(config-ips-vendor-category)# rules action drop
```

rules count

Данной командой указывается действующее число правил данной категории, с которым будет работать система IPS/IDS.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Команда применима только для правил, распространяемых по коммерческой лицензии.

Синтаксис

```
rules count <COUNT>
no rules count
```

Параметры:

<COUNT> – число правил. Минимальное значение 1, максимальное значение зависит от категории правил.

Максимальное число правил по категориям можно посмотреть в контекстной подсказке или командой:

```
show security ips content-provider rules-info
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-VENDOR-CATEGORY

Пример

```
wlc-30(config-ips-vendor-category)# rules count 8000
```

security ips policy

Данной командой создается политика настроек сервиса IPS/IDS с определенным именем и осуществляется переход в режим конфигурирования политики.

Использование отрицательной формы команды (no) удаляет сконфигурированную политику настроек сервиса IPS/IDS.

Синтаксис

```
[no] security ips policy <POLICY_NAME>
```

Параметры

<POLICY_NAME> – имя политики сервиса IPS/IDS, задаётся строкой до 31 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ips policy OFFICE
```

vendor

Данной командой определяется вендор правил IPS/IDS, распространяемых по коммерческой лицензии, и осуществляется переход в режим настройки данного вендора.

Использование отрицательной формы команды (no) удаляет сконфигурированного вендора из настроек сервиса IPS/IDS.

Синтаксис

```
vendor <VENDOR>
no vendor <CATEGORY>
```

Параметры

<VENDOR> – вендор правил.

Список доступных вендоров можно посмотреть в контекстной подсказке или командой:

```
show security ips content-provider rules-info
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-POLICY

Пример

```
wlc-30(config-ips-policy)# vendor kaspersky
```

Настройка IPS

logging ips severity

Данной командой устанавливается уровень важности сообщения для логирования событий IPS/IDS. Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
logging ips severity <SEVERITY>
no logging ips severity
```

Параметры

<SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности):

- emerg – в системе произошла критическая ошибка, система неработоспособна;
- alert – сигналы тревоги, необходимо немедленное вмешательство персонала;
- crit – критическое состояние системы, сообщение о событии;
- error – сообщения об ошибках;
- warning – предупреждения, неаварийные сообщения;
- notice – сообщения о важных системных событиях;
- info – информационные сообщения системы;
- debug – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы;
- none – отключает вывод syslog-сообщений.

Значение по умолчанию

info

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging ips severity error
```

logging remote-server

Данной командой задаются параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch).

Использование отрицательной формы команды (no) останавливает отправку статистики.

Синтаксис

```
logging remote-server { <ADDR> | <IPV6-ADDR> } [ <TRANSPORT> ] [ <PORT> ] [ source-address { <SRC-ADDR> | <IPV6-SRC-ADDR> } ]
```

```
no logging remote-server
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<TRANSPORT> – протокол передачи данных, по умолчанию – UDP, принимает значения:

- TCP – передача данных осуществляется по протоколу TCP;
- UDP – передача данных осуществляется по протоколу UDP.

<PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514;

<SRC-ADDR> – IPv4-адрес контроллера, который будет использоваться в качестве IP-адреса источника в отправляемых syslog пакетах, по умолчанию – ipv4-адрес интерфейса с которого отправляются пакеты;

<IPV6-SRC-ADDR> – IPv6-адрес контроллера, который будет использоваться в качестве IPv6-адреса источника в отправляемых syslog пакетах, по умолчанию – ipv6-адрес интерфейса с которого отправляются пакеты.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

Пример

```
wlc-30(config-ips)# logging remote-server 192.168.0.101
```

logging update-interval

Данной командой устанавливается интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
logging update-interval <INTERVAL>
no logging update-interval
```

Параметры

<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.

Значение по умолчанию

10 минут

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

Пример

```
wlc-30(config-ips)# logging update-interval 10
```

security ips

Команда используется для создания профиля сервиса IPS/IDS и перехода в режим его конфигурирования.

Синтаксис

```
security ips
```

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ips
```

performance max

Данная команда позволяет сервису IPS/IDS использовать все ресурсы устройства для достижения максимальной производительности. Рекомендуется применять, когда устройство используется исключительно в качестве IPS/IDS. Не рекомендуется применять, когда помимо IPS/IDS устройство выполняет другие функции (маршрутизация, BRAS и т.д.).

Использование отрицательной формы команды (no) освобождает часть ресурсов устройства для использования другими сервисами.

Синтаксис

```
[no] performance max
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

Пример

```
wlc-30(config-ips)# perfomance max
```

policy

Данной командой назначается созданная ранее политика настроек сервиса IPS/IDS.

Использование отрицательной формы команды (no) снимает назначенную ранее политику настроек сервиса IPS/IDS.

Синтаксис

```
policy <POLICY_NAME>
no policy
```

Параметры

<POLICY_NAME> – имя политики сервиса IPS, задаётся строкой до 32 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

Пример

```
wlc-30(config-ips)# policy OFFICE
```

service-ips enable

Данная команда используется для включение сервиса IPS/IDS на сетевом интерфейсе.

Использование отрицательной формы команды (no) выключает сервис IPS/IDS на сетевом интерфейсе.

Синтаксис

```
[no] service-ips enable
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# service-ips enable
```

Настройка автообновления правил IPS/IDS, распространяемых по коммерческой лицензии

content-provider

Данной командой осуществляется переход в режим конфигурирования источника обновлений правил, распространяемых по коммерческой лицензии.

Синтаксис

```
content-provider
```

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# content-provider
```

host address

Данной командой задаётся адрес сервера обновлений правил, распространяемых по коммерческой лицензии.

Синтаксис

```
host address { <ADDR> | <IPV6-ADDR> | <HOSTNAME> }
```

Параметры

<ADDR> – IP-адрес устройства, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес устройства, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<HOSTNAME> – DNS-имя устройства, задаётся строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# host address edm.eltex-co.ru
```

host port

Данной командой задаётся номер TCP-порта сервера обновлений правил, распространяемых по коммерческой лицензии.

Использование отрицательной формы команды (no) удаляет номер TCP-порта сервера обновлений правил, распространяемых по коммерческой лицензии.

Синтаксис

```
host port <PORT>
no host port
```

Параметры

<PORT> – номер TCP-порта, принимает значения [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# host port 8098
```

location

Данной командой задаётся текстовое описание, которое передаётся на сервер EDM-Issue.

Использование отрицательной формы команды (no) удаляет это описание.

Синтаксис

```
location <WORD>
no location
```

Параметры

<WORD> – описание, задаётся строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# location "Server room in Novokuznetsk office"
```

reboot

Данной командой задаётся время перезагрузки устройства при получении системной лицензии. Устройство перезагружается при первом подключении к серверу обновлений правил, распространяемых по коммерческой лицензии.

При наличии функциональной лицензии IPS/IDS перезагрузки не происходит.

Синтаксис

```
reboot { immediately | time <TIME> }
```

Параметры

immediately – перезагружаться сразу после получения лицензии;

time <TIME> – перезагружаться в указанное время <TIME>;

<TIME> – время перезагрузки в формате HH:MM:SS.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# reboot time 05:00:00
```

storage-path

Данной командой задается путь на внешнем носителе, по которому будут сохраняться правила IPS/IDS в шифрованном виде, распространяемые по коммерческой лицензии.

Использование отрицательной формы команды (no) останавливает сохранение правил.

Синтаксис

```
storage-path { usb://<USB-NAME>:/<PATH> | mmc://<MMC-NAME>:/<PATH> }
no storage-device
```

Параметры

<USB-NAME> – имя подключенного USB-носителя. Имя можно узнать в выводе команды show storage-devices usb;

<MMC-NAME> – имя подключенного MMC-носителя. Имя можно узнать в выводе команды show storage-devices mmc;

<PATH> – путь и имя файла на внешнем носителе.

Необходимый уровень привилегий config-ips-upgrade-user-server

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# storage-device usb://DATA/IPS
```

system-name

Данной командой задаётся текстовое имя устройства, которое передаётся на сервер EDM-Issue.

Использование отрицательной формы команды (no) присваивает этому имени значение по умолчанию.

Синтаксис

```
system-name <WORD>
no system-name
```

Параметры

<WORD> – имя, задаётся строкой до 255 символов.

Значение по умолчанию

По умолчанию значение system-name совпадает с hostname

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# system-name main-office
```

upgrade interval

Команда задаёт частоту, с которой устройство будет проверять обновления правил IPS/IDS, распространяемых по коммерческой лицензии.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
upgrade interval <HOURS>
no upgrade interval
```

Параметры

<HOURS> – интервал обновлений в часах, от 1 до 240.

Значение по умолчанию

24

Необходимый уровень привилегий

15

Командный режим

CONFIG-CONTENT-PROVIDER

Пример

```
wlc-30(config-content-provider)# upgrade interval 36
```

Настройка автообновления правил IPS/IDS из внешних источников

auto-upgrade

Данной командой осуществляется переход в режим конфигурирования источников обновлений правил для сервиса.

Синтаксис

```
auto-upgrade
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS

Пример

```
wlc-30(config-ips)# auto-upgrade
```

upgrade interval

Команда задаёт частоту, с которой устройство будет проверять обновления правил IPS/IDS и/или файла классификатора IPD/IDS для данного URL.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
upgrade interval <HOURS>
no upgrade interval
```

Параметры

<HOURS> – интервал обновлений в часах, от 1 до 240.

Значение по умолчанию

24

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-UPGRADE-USER-SERVER

Пример

```
wlc-30(config-ips-upgrade-user-server)# upgrade interval 36
```

url

Команда используется для задания URL-ссылки.

Использование отрицательной формы команды (no) удаляет ссылку из конфигурации источника обновлений правил IPS/IDS.

Синтаксис

```
url <URL>
no url
```

Параметры

<URL> – текстовое поле, содержащее URL-ссылку длинной от 8 до 255 символов.

В качестве URL-ссылки может быть указан:

- файл правил с расширение .rule;
- файл классификатора правил с именем classification.config;
- каталог на сервере содержащий файлы правил и/или файл классификатора правил.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-UPGRADE-USER-SERVER

Пример

```
wlc-30(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/
suricata-4.0/rules/
```

user-server

Данной командой задаётся имя пользовательского сервера обновлений правил IPS/IDS и осуществляется переход в режим конфигурирования параметров пользовательского сервера обновлений.

Использование отрицательной формы команды (no) удаляет пользовательский сервер обновлений правил IPS/IDS и все правила полученные с этого сервера.

Синтаксис

```
user-server <WORD>
no user-server { <WORD> | all }
```

Параметры

<WORD> имя сервера задается строкой от 1 до 64 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-AUTO-UPGRADE

Пример

```
wlc-30(config-ips-auto-upgrade)# user-server ET-Open
```

Настройка пользовательских правил IPS/IDS

action

Данная команда используется для указания действия, которое должно быть применено для трафика, удовлетворяющего заданным критериям.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
action { alert | reject | pass | drop }
no action
```

Параметры:

- alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение;
- reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение;
- pass – прохождение трафика разрешается;
- drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# action reject
```

destination-address

Данной командой устанавливаются IP-адреса получателя, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
destination-address { ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> |
policy-object-group { protect | external } | any }
no destination-address
```

Параметры

<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];

<OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса назначения, задаётся строкой до 31 символа;

destination-address policy-object-group protect устанавливает в качестве адресов назначения protect-адреса, определенные в политике IPS/IDS;

destination-address policy-object-group external устанавливает в качестве адресов назначения external-адреса, определенные в политике IPS/IDS;

При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# destination-address ip 10.10.10.1
```

destination-port

Данной командой устанавливается номер TCP/UDP-порта получателя, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
destination-port { any | <PORT> | object-group <OBJ-GR-NAME> }
no destination-port
```

Параметры

<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535];

<OBJ_GR_NAME> – имя профиля TCP/UDP-портов получателя, задаётся строкой до 31 символа.

При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# destination-port 22
```

direction

Данной командой устанавливается направление потока трафика, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
direction { one-way | round-trip }
no direction
```

Параметры

- one-way – трафик передаётся в одну сторону;
- round-trip – трафик передаётся в обе стороны.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# direction one-way
```

ip dscp

Данной командой устанавливается значение кода DSCP, трафик которого будет обрабатываться в данном правиле.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip dscp <DSCP>
[no] ip dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip dscp 8
```

ip ftp command

Данной командой устанавливаются значения ключевых слов протокола FTP, для которых должно срабатывать правило.

Данная команда применима только для значения protocol ftp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip ftp command <COMMAND>
[no] ip ftp command
```

Параметры

<COMMAND> – может принимать следующие значения:

- <retr> – скачать файл;
- <stor> – залить файл;
- <mkd> – создать директорию;
- <rmd> – удалить директорию;
- <appe> – добавить в конец файла (с созданием);
- <dele> – удалить файл.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# protocol ftp
wlc-30(config-ips-category-rule)# ip ftp command allo
```

ip ftp-data command

Данной командой устанавливаются значения ключевых слов протокола FTP-DATA, для которых должно срабатывать правило.

Данная команда применима только для значения protocol ftp-data.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip ftp-data command <COMMAND>
```

```
[no] ip ftp-data command
```

Параметры

<COMMAND> – может принимать следующие значения:

- <retr> – скачать файл;
- <stor> – залить файл;
- <appe> – добавить в конец файла (с созданием).

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# protocol ftp-data
wlc-30(config-ips-category-rule)# ip ftp-data command stor
```

ip http

Данной командой устанавливаются значения ключевых слов протокола HTTP, для которых должно срабатывать правило.

Данная команда применима только для значения protocol http.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip http <COMMAND>
```

```
[no] ip http
```

Параметры

<COMMAND> – может принимать следующие значения:

- accept;
- accept-enc;
- accept-lang;
- client-body;
- connection;
- content-len;
- content-type;
- cookie;
- file-data;
- header;
- header-names;
- host;
- protocol;
- referer;

- request-line;
- response-line;
- server-body;
- start;
- stat-code;
- stat-msg;
- uri;
- urilen <VALUE>;
- urilen comparison-operator { greater-than | less-than};
- user-agent.

Значения и применение ключевых слов протокола HTTP подробно описаны в документации SNORT 2.X / Suricata 4.X.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload content «HTTP/1.0»
wlc-30(config-ips-category-rule)# ip http protocol
```

ip http content-filter

Данной командой назначается профиль категорий контентной фильтрации. Текущее правило будет срабатывать для http-сайтов, которые относятся к категориям заданным в этом профиле.

Сам профиль контентной фильтрации должен быть предварительно создан.

Данная команда применима только для значения protocol http.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip http content-filter <NAME>
[no] ip http content-filter
```

Параметры

<NAME> – имя профиля контентной фильтрации задаётся строкой до 31 символа;

any – правило будет срабатывать для http-сайтов любой категории.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip http content-filter Black-List
```

ip http method

Данной командой устанавливаются значения метода доступа по протоколу http, для которых должно срабатывать правило.

Данная команда применима только для значения protocol http.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip http method <COMMAND>
[no] ip http method
```

Параметры

<COMMAND> – может принимать следующие значения:

- <GET> – запрашивает представление ресурса. Запросы с использованием этого метода могут только извлекать данные;
- <HEAD> – запрашивает ресурс так же, как и метод GET, но без тела ответа;
- <POST> – используется для отправки сущностей к определённому ресурсу;
- <PUT> – заменяет все текущие представления ресурса данными запроса;
- <DELETE> – удаляет указанный ресурс;
- <CONNECT> – устанавливает "туннель" к серверу, определённому по ресурсу;
- <OPTIONS> – используется для описания параметров соединения с ресурсом;
- <TRACE> – выполняет вызов возвращаемого тестового сообщения с ресурса;
- <PATCH> – используется для частичного изменения ресурса.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip http method get
```

ip icmp code

Данной командой устанавливается значение ICMP CODE, при котором сработает правило.

Данная команда применима только для значения protocol icmp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip icmp code <CODE>
```

```
[no] ip icmp code
```

Параметры

<CODE> – значение CODE протокола ICMP, принимает значение в диапазоне [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp code 5
```

ip icmp code comparison-operator

Оператор сравнения для команды ip icmp code. Применим только совместно с этой командой.

Использование отрицательной формы команды (no) отменяет сравнение.

Синтаксис

```
ip icmp code comparison-operator { greater-than | less-than }
[no] ip icmp code comparison-operator
```

Параметры

- greater-than – больше чем;
- less-than – меньше чем.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp code 5
wlc-30(config-ips-category-rule)# ip icmp code comparison-operator less-than
```

ip icmp id

Данной командой устанавливается значение ICMP ID, при котором сработает правило.

Данная команда применима только для значения protocol icmp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip icmp id <ID>
[no] ip icmp id
```

Параметры

<ID> – значение ID протокола ICMP, принимает значение в диапазоне [0..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp id 65000
```

ip icmp sequence-id

Данной командой устанавливается значение ICMP sequence-ID, при котором сработает правило.
Данная команда применима только для значения protocol icmp.
Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip icmp sequence-id <SEQ-ID>
[no] ip icmp sequence-id
```

Параметры

<SEQ-ID> – значение Sequence-ID протокола ICMP, принимает значение в диапазоне [0..4294967295].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp sequence-id 8388608
```

ip icmp type

Данной командой устанавливается значение ICMP TYPE, при котором сработает правило.
Данная команда применима только для значения protocol icmp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip icmp type <TYPE>
[no] ip icmp type
```

Параметры

<TYPE> – значение TYPE протокола ICMP, принимает значение в диапазоне [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp type 12
```

ip icmp type comparison-operator

Оператор сравнения для команды ip icmp type. Применим только совместно с этой командой.

Использование отрицательной формы команды (no) отменяет сравнение.

Синтаксис

```
ip icmp type comparison-operator { greater-than | less-than }
[no] ip icmp type comparison-operator
```

Параметры

- greater-than – больше чем;
- less-than – меньше чем.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip icmp type 14
wlc-30(config-ips-category-rule)# ip icmp code comparison-operator greater-than
```

ip protocol-id

Данной командой устанавливается идентификационный номер IP-протокола, трафик которого будет обрабатываться в данном правиле.

Данная команда применима только для значения protocol any.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip protocol-id <ID>
[no] ip protocol-id
```

Параметры

<ID> – идентификационный номер IP-протокола [1..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip protocol-id 250
```

ip tcp acknowledgment-number

Данной командой устанавливается значение TCP Acknowledgment-Number, при котором сработает правило.

Данная команда применима только для значения protocol tcp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip tcp acknowledgment-number <ACK-NUM>
[no] ip tcp acknowledgment-number
```

Параметры

<ACK-NUM> – значение Acknowledgment-Number протокола TCP, принимает значение в диапазоне [0..4294967295].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip tcp acknowledgment-number 32
```

ip tcp sequence-id

Данной командой устанавливается значение TCP Sequence-ID, при котором сработает правило.

Данная команда применима только для значения protocol tcp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip tcp sequence-id <SEQ-ID>
[no] ip tcp sequence-id
```

Параметры

<SEQ-ID> – значение Sequence-ID протокола TCP, принимает значение в диапазоне [0..4294967295].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip tcp sequence-id 2542
```

ip tcp window-size

Данной командой устанавливается значение TCP Window Size, при котором сработает правило.

Данная команда применима только для значения protocol tcp.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip tcp window-size <SIZE>
[no] ip tcp window-size
```

Параметры

<SIZE> – значение Window-Size протокола TCP, принимает значение в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip tcp window-size 50
```

ip ttl

Данной командой устанавливается значение времени жизни IP-пакета, трафик которого будет обрабатываться в данном правиле.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
ip ttl <TTL>
[no] ip ttl
```

Параметры

<TTL> – время жизни IP-пакета, принимает значения [1..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip ttl 8
```

ip ttl comparison-operator

Оператор сравнения для команды ip ttl. Применим только совместно с этой командой.

Использование отрицательной формы команды (no) отменяет сравнение.

Синтаксис

```
ip ttl comparison-operator { greater-than | less-than }
[no] ip ttl comparison-operator
```

Параметры

- greater-than – больше чем;
- less-than – меньше чем.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# ip ttl 5
wlc-30(config-ips-category-rule)# ip ttl comparison-operator less-than
```

meta classification-type

Данная команда определяет классификацию события, которое сгенерирует сервис IPS/IDS, когда сработает правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
meta classification-type { not-suspicious | unknown | bad-unknown | attempted-recon |
successful-recon-limited | successful-recon-largescale | attempted-dos | successful-dos |
attempted-user | unsuccessful-user |
successful-user | attempted-admin | successful-admin | rpc-portmap-decode | shellcode-
detect | string-detect | suspicious-filename-detect | suspicious-login | system-call-
detect | tcp-connection | trojan-activity |
unusual-client-port-connection | network-scan | denial-of-service | non-standard-protocol
| protocol-command-decode | web-application-activity | web-application-attack | misc-
activity | misc-attack | icmp-event |
inappropriate-content | policy-violation | default-login-attempt }

[no] meta classification-type
```

Параметры

- not-suspicious – не подозрительный трафик;
- unknown – неизвестный трафик;
- bad-unknown – потенциально плохой трафик;
- attempted-recon – попытка утечки информации;
- successful-recon-limited – утечка информации;
- successful-recon-largescale – масштабная утечка информации;
- attempted-dos – попытка отказа в обслуживании;
- successful-dos – отказ в обслуживании;
- attempted-user – попытка получения привилегий пользователя;
- unsuccessful-user – безуспешная попытка получения привилегий пользователя;
- successful-user – успешная попытка получения привилегий пользователя;
- attempted-admin – попытка получения привилегий администратора;
- successful-admin – успешная попытка получения привилегий администратора;
- rpc-portmap-decode – декодирование запроса RPC;
- shellcode-detect – обнаружен исполняемый код;
- string-detect – обнаружена подозрительная строка;
- suspicious-filename-detect – было обнаружено подозрительное имя файла;
- suspicious-login – была обнаружена попытка входа с использованием подозрительного имени пользователя;
- system-call-detect – обнаружен системный вызов;
- tcp-connection – обнаружено TCP-соединение;
- trojan-activity – был обнаружен сетевой троян;
- unusual-client-port-connection – клиент использовал необычный порт;
- network-scan – обнаружение сетевого сканирования;

- denial-of-service – обнаружение атаки отказа в обслуживании;
- non-standard-protocol – обнаружение нестандартного протокола или события;
- protocol-command-decode – обнаружена попытка шифрования;
- web-application-activity – доступ к потенциально уязвимому веб-приложению;
- web-application-attack – атака на веб-приложение;
- misc-activity – прочая активность;
- misc-attack – прочие атаки;
- icmp-event – общее событие ICMP;
- inappropriate-content – обнаружено неприемлемое содержание;
- policy-violation – потенциальное нарушение корпоративной конфиденциальности;
- default-login-attempt – попытка входа с помощью стандартного логина/пароля.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# meta classification-type misc-attack
```

meta log-message

Данная команда определяет текстовое сообщение, которое сгенерирует сервис IPS/IDS, когда сработает правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
meta log-message <MESSAGE>
[no] mera log-message
```

Параметры

<MESSAGE> – текстовое сообщение, задаётся строкой до 128 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# meta log-message «Possible SlowLorys attack»
```

payload content

Данной командой можно указать содержимое IP-пакетов, при совпадении с которым будет срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
payload content <CONTENT>
[no] payload content <CONTENT>
```

Параметры

<CONTENT> – текстовое сообщение, задаётся строкой до 1024 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload content «virus»
```

payload data-size

Данной командой устанавливается размер содержимого пакетов, при котором сработает правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
payload data-size <SIZE>
[no] payload data-size
```

Параметры

<SIZE> – размер содержимого пакетов, принимает значение в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload data-size 1024
```

payload data-size comparison-operator

Оператор сравнения для команды ip icmp type. Применим только совместно с этой командой.

Использование отрицательной формы команды (no) отменяет сравнение.

Синтаксис

```
payload data-size comparison-operator { greater-than | less-than }
[no] payload data-size comparison-operator
```

Параметры

- greater-than – больше чем;
- less-than – меньше чем.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload data-size 1024
wlc-30(config-ips-category-rule)# payload data-size comparison-operator less-than
```

payload depth

Данная команда указывает сколько байтов с начала содержимого пакета будет проверять это правило. Команда используется только совместно с командой payload content. Может применяться совместно с командой payload offset.

Использование отрицательной формы команды (no) означает что будет проверяться все содержимое пакета на точное соответствие.

Синтаксис

```
payload depth <DEPTH>
[no] payload content depth
```

Параметры

<DEPTH> – число байт с начала содержимого пакета, принимает значение в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload content «abc»
wlc-30(config-ips-category-rule)# payload depth 3
```

Под действие правила попадут пакеты с содержимым «abcdef», «abc123», «abcabcabc» и т.д.

payload no-case

Данная команда указывает не различать прописные и заглавные буквы в описании содержимого пакетов. Команда используется только совместно с командой payload content.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
payload no-case
[no] payload content no-case
```

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload content «virus»
wlc-30(config-ips-category-rule)# payload no-case
```

Под действие правила попадут пакеты с содержимым «virus», «VIRUS», «ViRuS» и т.д.

payload offset

Данная команда указывает число байт смещения от начала содержимого пакета, с которого начнется проверка. Команда используется только совместно с командой payload content. Может применяться совместно с командой payload depth.

Использование отрицательной формы команды (no) означает, что будет проверяться все содержимое пакета на точное соответствие.

Синтаксис

```
payload offset <OFFSET>
[no] payload content offset
```

Параметры

<OFFSET> – число байт смещения от начала содержимого пакета, принимает значение в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# payload content «abc»
wlc-30(config-ips-category-rule)# payload depth 6
wlc-30(config-ips-category-rule)# payload offset 3
```

Под действие правила попадут пакеты с содержимым «123abcdef», «defabc», «abcabcabc» и т.д.

protocol

Данной командой устанавливается имя IP-протокола, для которого должно срабатывать правило. Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
protocol { any | ip | icmp | http | tcp | udp }
[no] protocol
```

Параметры

- any – правило будет срабатывать для любых протоколов;
- ip – правило сработает для протокола ip. В правиле можно настроить дополнительную фильтрацию командой ip protocol-id;
- icmp – правило сработает для протокола icmp. При выборе этого параметра значения source-port и destination-port должны быть any. В правиле можно настроить дополнительную фильтрацию командами ip icmp;
- http – правило сработает для протокола http. В правиле можно настроить дополнительную фильтрацию командами ip http;
- tcp – правило сработает для протокола tcp. В правиле можно настроить дополнительную фильтрацию командами ip tcp;
- udp – правило сработает для протокола tcp. В правиле можно настроить дополнительную фильтрацию командами ip udp;
- ftp – правило сработает для протокола ftp. В правиле можно настроить дополнительную фильтрацию командами ip ftp;
- ftp-data – правило сработает для поля data протокола ftp. В правиле можно настроить дополнительную фильтрацию командами ip ftp-data.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# protocol udp
```

rule

Данная команда используется для создания правила и перехода в режим конфигурирования CONFIG-IPS-CATEGORY-RULE. Правила обрабатываются устройством в порядке возрастания их номеров.

Использование отрицательной формы команды (no) удаляет указанное правило.

Синтаксис

```
[no] rule <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1..512].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY

Пример

```
wlc-30(config-ips-category)# rule 10
wlc-30(config-ips-category-rule)#
```

security ips-category user-defined

Данной командой создается набор пользовательских правил сервиса IPS/IDS с определенным именем и осуществляется переход в режим конфигурирования этого набора.

Использование отрицательной формы команды (no) удаляет сконфигурированную политику настроек сервиса IPS.

Синтаксис

```
[no] security ips-category user-defined <CATEGORY_NAME>
```

Параметры

<CATEGORY_NAME> – имя набора пользовательских правил сервиса IPS/IDS, задаётся строкой до 31 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# security ips-category user-defined PROTOCOL
wlc-30(config-ips-category)#
```

source-address

Данной командой устанавливаются IP-адреса отправителей, для которых должно срабатывать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }
```

```
no source-address
```

Параметры

<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32];

<OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса отправителя, задаётся строкой до 31 символа;

destination-address policy-object-group protect устанавливает в качестве адресов отправителя, protect адреса определенные в политике IPS/IDS;

destination-address policy-object-group external устанавливает в качестве адресов отправителя, external адреса определенные в политике IPS/IDS.

При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# source-address ip-prefix 192.168.0.0/16
```

source-port

Данной командой устанавливается номер TCP/UDP-порта отправителя, для которого должно срабатывать правило.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
source-port { any | <PORT> | object-group <OBJ-GR-NAME> }
no source-port
```

Параметры

<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535];

<OBJ_GR_NAME> – имя профиля TCP/UDP портов отправителя, задаётся строкой до 31 символа.

При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# source-port 22
```

threshold count

Данной командой устанавливается пороговое значение количества пакетов, при котором сработает правило.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
threshold count <COUNT>
[no] threshold count
```

Параметры

<COUNT> – число пакетов, принимает значение в диапазоне [1..65535]

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# threshold count 1024
```

threshold second

Данной командой устанавливается интервал времени, для которого считается пороговое значение. пакетов, при котором сработает правило. Команда используется только совместно с командой threshold count.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
threshold second <SECOND>
[no] threshold second
```

Параметры

<SECOND> – интервал времени в секундах, принимает значение в диапазоне [1..65535].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# threshold second 1
```

threshold track

Данной командой устанавливается по адресу отправителя или получателя будут считаться пакеты, для которых устанавливаются пороговые значения. Команда используется только совместно с командой threshold count.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
threshold track { by-src | by-dst }
[no] threshold track
```

Параметры

- by-src – считать пороговое значение для пакетов с одинаковым IP-отправителя;
- by-dst – считать пороговое значение для пакетов с одинаковым IP-получателя.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# threshold track by-src
```

threshold type

Данной командой устанавливается метод обработки пороговых значений. Команда используется только совместно с командой threshold count.

Использование отрицательной формы команды (no) удаляет назначение.

Синтаксис

```
threshold type { treshhold | limit | both }
[no] threshold type
```

Параметры

- threshold – выдавать сообщение каждый раз по достижении порога;
- limit – выдавать сообщение не чаще <COUNT> раз за интервал времени <SECOND>;
- both – комбинация threshold и limit. Сообщение будет генерироваться, если в течении интервала времени <SECOND> было <COUNT> или более пакетов, подходящих под условия правила, и сообщение будет отправлено только один раз в течении интервала времени.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# threshold count 1024
wlc-30(config-ips-category-rule)# threshold second 1
wlc-30(config-ips-category-rule)# threshold track by-src
wlc-30(config-ips-category-rule)# threshold type treshold
```

Сообщение будет генерироваться на каждый X*1025 пакет, приходящий за 1 секунду с одного IP-адреса.

Настройка расширенных пользовательских правил

rule-advanced

Данная команда используется для создания правила и перехода в режим конфигурирования CONFIG-IPS-CATEGORY-RULE. Правила обрабатываются устройством в порядке возрастания их номеров.

Использование отрицательной формы команды (no) удаляет указанное правило.

Синтаксис

```
[no] rule-advanced <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1..4294967295].

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY

Пример

```
wlc-30(config-ips-category)# rule-advanced 10
wlc-30(config-ips-category-rule)#
```

rule-text

Данная команда описывает правило обработки трафика в формате SNORT 2.X / Suricata 4.X

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

`rule-text <LINE>`

`[no] rule-text`

Параметры

<LINE> – текстовое сообщение в формате SNORT 2.X / Suricata 4.X, задаётся строкой до 1024 символов.

При написании правил символ " требуется заменить на символ '.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IPS-CATEGORY-RULE

Пример

```
wlc-30(config-ips-category-rule)# rule-text «alert tcp any any -> $HOME_NET any (msg: 'ATTACK
[PTsecurity] Attempt to crash named using malformed RNDC packet'; flow: established, to_server;
content:'_auth'; depth: 20; fast_pattern; content: !'|02 00 00 00|'; within: 4; content:
'_ctrl'; content: '_ser'; content: '_tim'; content: '_exp'; reference: cve, 2016-1285;
classtype: attempted-dos; reference: url, github.com/ptresearch/AttackDetection; metadata: Open
Ptsecurity.com ruleset; sid: 10000005; rev: 3; )»
```

Настройка системы "Антиспам"

- action
- description
- domain
- enable
- enable
- headers max-size
- mail domain
- mail max-size
- mail server ip
- mailserver
- mailserver domain
- mark-type
- profile antispam
- rule
- security antispam profile
- sender email
- sender ip
- smtp helo-required
- smtp vrfy-enable
- tls enable
- tls keyfile

action

Данная команда используется для указания действия, которое должно быть применено к электронному письму, на котором сработало правило.

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
action <ACTION>
[no] action
```

Параметры

<ACTION> – назначаемое действие:

- reject – дальнейшая доставка письма запрещена, отправителю письма высылается ответ об ошибке.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE-RULE

Пример

```
wlc-30(config-antispam-profile-rule)# action reject
```

description

Данная команда используется для изменения описания настраиваемого профиля сервиса «Антиспам», правила внутри профиля сервиса «Антиспам» или почтового домена.

Использование отрицательной формы команды (no) удаляет установленное описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

< DESCRIPTION > – описание настраиваемого почтового домена, задаётся строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ANTISPAM-PROFILE

CONFIG-ANTISPAM-PROFILE-RULE

CONFIG-MAILSERVER-DOMAIN

Пример

```
wlc-30(config-mailserver-domain)# description "Test Mail Domain"
```

domain

Данная команда используется для указания почтового домена.

Использование отрицательной формы команды (no) удаляет указанный почтовый домен.

Синтаксис

```
domain <DOMAIN-NAME>
no domain
```

Параметры

<DOMAIN-NAME> – имя почтового домена, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# domain test_domain
```

enable

Данная команда используется для активации правила в профиля сервиса «Антиспам».

Использование отрицательной формы команды (no) деактивирует правило.

Синтаксис

```
[no] enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE-RULE

Пример

```
wlc-30(config-antispam-profile)# enable
```

enable

Данная команда используется для активации почтового сервера, на базе которого работает сервис «Антиспам» или почтового домена.

Использование отрицательной формы команды (no) деактивирует почтовый сервер или почтовый домен.

Синтаксис

```
[no] enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

CONFIG-MAILSERVER-DOMAIN

Пример

```
wlc-30(config-mailserver-domain)# enable
```

headers max-size

Данная команда используется для указания максимального размера заголовка электронного письма. Если размер заголовка обрабатываемого письма превысит указанное значение, то лишние записи в заголовке будут отброшены и не будут учтены при обработке письма.

Использование отрицательной формы команды (no) устанавливает максимальный размер заголовка электронного письма по умолчанию.

Синтаксис

```
headers max-size <SIZE>
no headers max-size
```

Параметры

<SIZE> – максимальный размер заголовка электронного письма в КБ, принимает значения в диапазоне от [50..200].

Значение по умолчанию

100.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# headers max-size 115
```

mail domain

Данная команда используется для указания имени почтового домена, для которого сервис «Антиспам» будет принимать, анализировать и доставлять почту согласно настроек почтового домена. Письма, пришедшие не из указанного домена или не для указанного домена, будут отброшены.

Использование отрицательной формы команды (no) удаляет указанное имя почтового домена.

Синтаксис

```
mail domain <NAME>
[no] mail domain
```

Параметры

<NAME> – имя почтового домена, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-MAILSERVER-DOMAIN

Пример

```
wlc-30(config-mailserver-domain)# mail domain eltex-co.ru
```

mail max-size

Данная команда используется для указания максимального размера электронного письма. Если размер обрабатываемого письма превысит указанное значение, письмо будет отброшено, а отправитель письма получит соответствующее уведомление.

Использование отрицательной формы команды (no) устанавливает максимальный размер электронного письма по умолчанию.

Синтаксис

```
mail max-size <SIZE>
no mail max-size
```

Параметры

<SIZE> – максимальный размер электронного письма в КБ. Принимает значения в диапазоне [5120..51200].

Значение по умолчанию

15360.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# mail max-size 10000
```

mail server ip

Данная команда используется для указания IP-адреса почтового сервера, для которого сервис «Антиспам» будет перенаправлять электронную почту согласно настройкам почтового домена. Письма, пришедшие из домена, прописанного в команде "mail domain", но не с указанного IP-адреса будут отброшены.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес почтового сервера.

Синтаксис

```
mail server ip <ADDR>
[no] mail server ip
```

Параметры

<ADDR> – IP-адрес почтового сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-MAILSERVER-DOMAIN

Пример

```
wlc-30(config-mailserver-domain)# mail server ip 192.168.1.1
```

mailserver

Данная команда используется для перехода в режим конфигурирования почтового сервера, на базе которого работает сервис «Антиспам».

Использование отрицательной формы команды (no) удаляет почтовый сервер из конфигурации.

Синтаксис

```
[no] mailserver
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# mailserver
```

mailserver domain

Данная команда используется для создания почтового домена, который используется при работе почтового сервера.

Использование отрицательной формы команды (no) удаляет указанный почтовый домен.

Синтаксис

```
[no] mailserver domain <DOMAIN-NAME>
```

Параметры

<DOMAIN-NAME> – имя почтового домена, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# mailserver domain local_domain
```

mark-type

Данная команда используется для указания типа маркировки электронных писем, которые сервис «Антиспам» отнес к категории «Спам».

Использование отрицательной формы команды (no) удаляет тип маркировки письма, отнесенного сервисом «Антиспам» к категории «Спам».

Синтаксис

```
mark-type <MARK-TYPE>
no mark-type
```

Параметры

<MARK-TYPE> – тип маркировки письма, отнесенного к категории «Спам». Принимает значения:

- header – добавить X-Spam заголовок к заголовкам электронного письма;
- subject – добавить тег [SPAM] перед темой электронного письма.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE

Пример

```
wlc-30(config-antispam-profile)# mark-type header
```

profile antispam

Данная команда используется для указания используемого профиля сервиса «Антиспам» в конфигурации почтового домена.

Использование отрицательной формы команды (no) удаляет указанный профиль из конфигурации почтового домена.

Синтаксис

```
profile antispam <ANTISPAM-PROFILE-NAME>
no profile antispam
```

Параметры

<ANTISPAM-PROFILE-NAME> – имя профиля сервиса «Антиспам», задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-MAILSERVER-DOMAIN

Пример

```
wlc-30(config-mailserver-domain)# profile antispam main_domain_protection
```

rule

Данная команда используется для создания правила в профиле сервиса «Антиспам» и перехода в режим конфигурирования. Правила обрабатываются устройством в порядке возрастания их номеров.

Использование отрицательной формы команды (no) удаляет указанное правило.

Синтаксис

```
[no] rule <ORDER>
```

Параметры

<ORDER> – номер правила, принимает значения [1..100].

Значение по умолчанию

Правило не создано.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE

Пример

```
wlc-30(config-antispam-profile)# rule 10
```

security antispam profile

Данная команда используется для создания профиля сервиса «Антиспам» и перехода в режим конфигурирования профиля сервиса «Антиспам».

Использование отрицательной формы команды (no) удаляет указанный профиля сервиса «Антиспам».

Синтаксис

```
[no] security antispam profile <NAME>
```

Параметры

<NAME> – имя профиля сервиса «Антиспам», задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# security antispam profile TEST
```

sender email

Данная команда используется для указания группы доменов или почтовых ящиков, с которых отправляются письма, для которых должно сработать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
sender email <OBJ-GROUP-MAIL-NAME>
[no] sender email
```

Параметры

<OBJ-GROUP-MAIL-NAME> – имя группы доменов или почтовых ящиков, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE-RULE

Пример

```
wlc-30(config-antispam-profile-rule)# sender email mail_blacklist
```

sender ip

Данная команда используется для указания группы IP-адресов почтовых серверов или клиентов, для которых должно сработать правило.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
sender ip <OBJ-GROUP-NETWORK-NAME>
[no] sender ip
```

Параметры

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ANTISPAM-PROFILE-RULE

Пример

```
wlc-30(config-antispam-profile-rule)# sender ip ip_blacklist
```

smtp helo-required

Данная команда используется для включения обязательного требования SMTP-команды HELO/EHLO от SMTP-клиента, который пытается подключиться к wlc-30 по протоколу SMTP. Отсутствие HELO/EHLO-команды во во время установления SMTP-сессии приведет к разрыву соединения.

Использование отрицательной формы команды (no) отключает обязательное требование HELO/EHLO-команды.

Синтаксис

```
[no] smtp helo-required
```

Параметры

Отсутствуют.

Значение по умолчанию

Команда HELO/EHLO во время установления SMTP-сессии не требуется.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# smtp helo-required
```

smtp vrfy-enable

Данная команда используется для разрешения использования SMTP-команды VRFY, которая позволяет проверить наличие пользователя с таким именем в списке пользователей, обслуживаемых данным почтовым сервером. В целях обеспечения защиты от сканирования базы пользователей на почтовом сервере данная команда по умолчанию отключена.

Использование отрицательной формы команды (no) отключает возможность использования SMTP-команды VRFY.

Синтаксис

```
[no] smtp vrfy-enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Команда VRFY отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# smtp vrfy-enable
```

tls enable

Данная команда используется для включения TLS-протокола для поддержки установления защищенных соединений с другими почтовыми серверами и почтовыми клиентами. Если при включенном на wlc-30 TLS вторая сторона не сообщает о поддержке TLS – вся SMTP-сессия будет проходить в формате plaintext (т.е. в открытом виде).

Использование отрицательной формы команды (no) отключает поддержку TLS.

Синтаксис

```
[no] tls enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Поддержка TLS отключена.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# tls enable
```

tls keyfile

Данная команда используется для указания сертификатов и ключей для работы протокола TLS при установлении SMTP-сессий.

Использование отрицательной формы команды (no) удаляет указанный тип сертификата или ключа.

Синтаксис

```
tls keyfile <TYPE> <NAME>
[no] tls keyfile
```

Параметры

<TYPE> – тип файла сертификата или ключа, принимает значения:

- ca – сертификат удостоверяющего центра;
- server-key – приватный ключ сервера;
- server-crt – публичный сертификат сервера;
- dh – ключ Диффи-Хеллмана.

<NAME> – имя файла сертификата, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# tls keyfile server-crt server.crt
```

28 Управление QoS

- class
- class-map
- compression header ip tcp
- description
- fair-queue
- ip firewall sessions classification enable
- match access-group
- match application
- match dscp
- match url
- mode
- policy-map
- priority class
- priority level
- priority-queue out
- priority-queue out num-of-queues
- qos dscp-mutation
- qos enable
- qos map cos-queue
- qos map dscp-mutation
- qos map dscp-queue
- qos queue default
- qos trust
- qos wrr-queue
- queue-limit
- random-detect
- random-detect queue
- random-detect queue default
- rate-limit
- service-policy
- service-policy
- set class-default cos
- set class-default dscp
- set class-default ip-precedence
- set cos
- set dscp
- set ip-precedence
- shape auto-distribution
- shape average
- shape peak
- show qos interface shapers
- show qos map cos-queue
- show qos map dscp-mutation
- show qos map dscp-queue
- show qos policy binding
- show qos policy configuration
- show qos policy statistics
- show qos statistics
- show qos tunnel shapers
- traffic-shape

class

Данная команда используется для привязки указанного QoS-класса к политике и осуществляется переход в режим настройки параметров класса.

Использование отрицательной формы команды (no) удаляет привязку класса к политике.

Синтаксис

```
[no] class <NAME>
```

Параметры

<NAME> – имя привязываемого класса, задается строкой до 31 символа. При указании значения «class-default» в данный класс попадает трафик, неклассифицированный на входе.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-policy-map)# class telnet_traffic
wlc-30(config-policy-map-class)#
```

class-map

Данной командой создается класс QoS и осуществляется переход в режим настройки параметров класса.

Использование отрицательной формы команды (no) удаляет созданный класс.

Синтаксис

```
[no] class-map <NAME>
```

Параметры

<NAME> – имя создаваемого класса, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# class-map telnet_traffic
```

compression header ip tcp

Данной командой включается протокол компрессии tcp-заголовков для трафика отдельного класса.

Использование отрицательной формы команды (no) отменяет использование протокола компрессии tcp-заголовков для трафика отдельного класса.

Синтаксис

```
[no] compression header ip tcp
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# compression header ip tcp
```

description

Данной командой определяется описание классификатора QoS.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание классификатора, задаётся строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-CLASS-MAP

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-class-map)# description "test"
```

fair-queue

Данной командой определяется предельное количество виртуальных очередей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
fair-queue <QUEUE-LIMIT>
no fair-queue
```

Параметры

<QUEUE-LIMIT> – предельное количество виртуальных очередей, принимает значения в диапазоне [16..4096].

Значение по умолчанию

16

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# fair-queue 200
```

ip firewall sessions classification enable

Командой выполняется включение классифицирования сессий на основе политики QoS.

Использование отрицательной формы команды (no) отключает классифицирование сессий.

Синтаксис

```
[no] ip firewall sessions classification enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip firewall sessions classification enable
```

match access-group

Команда используется для привязки списка контроля доступа (ACL), по которому будет определяться отношение входящего трафика к конфигурируемому классу.

Использование отрицательной формы команды (no) удаляет привязку списка контроля доступа к данному классу.

Синтаксис

```
[no] match access-group {<NAME> | all }
```

Параметры

<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

При удалении возможно использование ключа "all" для удаления всех заданных списков доступа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# match access-group acl-ssh-traffic
```

match application

Команда используется для привязки списка приложений, по которому будет определяться отношение входящего трафика к конфигурируемому классу.

Использование отрицательной формы команды (no) удаляет привязку списка приложений к данному классу.

> Классификация QoS по спискам приложений работает, только если firewall настроен на работы в StateLess-режиме.

Синтаксис

```
[no] match application { <NAME> | all }
```

Параметры

<NAME> – имя списка приложений, задаётся строкой до 31 символа.

При удалении возможно использование ключа "all" для удаления всех заданных списков доступа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# match application APP-PERMIT
```

match dscp

Данной командой устанавливается значение кода DSCP, трафик которого будет обрабатываться в данном class-map.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
[no] match dscp <DSCP>
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

При удалении возможно использование ключа "all" для удаления всех заданных dscp.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# match dscp 55
```

match url

Команда используется для привязки списка url, по которому будет определяться отношение входящего трафика к конфигурируемому классу.

Использование отрицательной формы команды (no) удаляет привязку списка url.

> Классификация QoS по спискам url работает, только если firewall настроен на работы в StateLess-режиме.

Синтаксис

```
[no] match url { <NAME> | all }
```

Параметры

<NAME> – имя списка url, задаётся строкой до 31 символа.

При удалении возможно использование ключа "all" для удаления всех заданных списков доступа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# match url URL-PERMIT
```

mode

Данной командой определяется режим работы класса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
mode <MODE>
no mode
```

Параметры

<MODE> – режим класса:

- fifo – режим FIFO (First In, First Out);
- gred – режим GRED (Generalized RED);
- red – режим RED (Random Early Detection);
- sfq – режим SFQ (очередь SFQ распределяет передачу пакетов на базе потоков).

Значение по умолчанию

FIFO

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# mode red
```

policy-map

Данной командой создается политика QoS и осуществляется переход в режим настройки параметров политики.

Использование отрицательной формы команды (no) удаляет созданную политику.

Синтаксис

```
[no] policy-map <NAME>
```

Параметры

<NAME> – имя создаваемой политики, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# policy-map input_policy
```

priority class

Данной командой задается приоритет класса в WRR-процессе. Классы с наибольшим приоритетом обрабатываются в первую очередь.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
priority class <PRIORITY>
no priority
```

Параметры

<PRIORITY> – приоритет класса в WRR-процессе, принимает значения [1..8].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# priority class 5
```

priority level

Данной командой класс переводится в режим Strict Priority и задается приоритет класса. Классы с наибольшим приоритетом обрабатываются в первую очередь.

Использование отрицательной формы команды (no) переводит класс в режим WRR.

Синтаксис

```
priority level <PRIORITY>
no priority
```

Параметры

<PRIORITY> – приоритет класса в Strict Priority-процессе, принимает значения [1..8].

Значение по умолчанию

Класс работает в режиме WRR, приоритет не задан.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# priority level 5
```

priority-queue out

Данная команда задаёт предельное количество пакетов в очереди.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
priority-queue out <QUEUE> limit <LIMIT>
no priority-queue out <QUEUE> limit
```

Параметры

<QUEUE> – идентификатор очереди, принимает значение [1..8];

<LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [100-1000].

Значение по умолчанию

500

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-SUBIF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-L2TPV3

Пример

```
wlc-30(config-if-gi)# priority-queue out 1 limit 800
```

priority-queue out num-of-queues

Данная команда задает количество приоритетных очередей от восьмой к первой. Оставшиеся очереди являются взвешенными.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
priority-queue out num-of-queues <VALUE>
no priority-queue out num-of-queues
```

Параметры

<VALUE> – количество очередей, принимает значение [1..8], где:

- 0 – все очереди участвуют в WRR (WRR – механизм обработки очередей на основе веса);
- 8 – все очереди обслуживаются как «strict priority» (strict priority – приоритетная очередь обслуживается сразу, как только появляются пакеты).

Значение по умолчанию

8

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# priority-queue out num-of-queues 5
```

qos dscp-mutation

Данной командой включается применение изменений кодов DSCP в соответствии с таблицей DSCP-Mutation. Коды DSCP изменяются только для входящего трафика доверенных портов в режиме QoS Basic.

Использование отрицательной формы команды (no) отключает изменение кодов DSCP.

Синтаксис

```
[no] qos dscp-mutation
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos wrr-queue 3 bandwidth 130
```

qos enable

Данной командой включается сервис QoS на интерфейсе. Если к интерфейсу не привязана политика QoS (привязка политик описана в разделе service-policy), то интерфейс работает в режиме Basic QoS, иначе Policy-based QoS.

Basic QoS – классификация трафика выполняется на основе кодов DSCP и/или 802.1p в зависимости от выбранного режима доверия (команда описана в разделе qos trust). Трафик направляется в очереди в соответствии с таблицами DSCP-Queue и/или CoS-Queue.

Policy-based QoS – классификация и направление трафика в очереди выполняется на основе QoS политик. В каждой политике определяется набор классов, на которые необходимо разделить трафик. Отношение трафика к определенному классу политики определяется на входе в контроллер правилами ACL (привязка ACL описана в разделе match access-group), для этого назначается QoS-политика на входящее направление. Для ограничения полосы ранее классифицированного трафика и других функций QoS-политика назначается на исходящее направление.

Использование отрицательной формы команды (no) выключает сервис QoS на интерфейсе.

Синтаксис

```
[no] qos enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-SUBTUNNEL

CONFIG-VTI

CONFIG-L2TPV3

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

CONFIG-OPENVPN

Пример

```
wlc-30(config-if-gi)# qos enable
```

qos map cos-queue

Данная команда устанавливает соответствие между значениями кодов 802.1p входящих пакетов и исходящими очередями.

Использование отрицательной формы команды (no) устанавливает соответствие по умолчанию.

Синтаксис

```
qos map cos-queue <COS> to <QUEUE>
no qos map dscp-queue <COS>
```

Параметры

<COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7];

<QUEUE> – идентификатор очереди, принимает значения [1..8].

Значения по умолчанию:

CoS: (0), очередь 1

CoS: (1), очередь 2

CoS: (2), очередь 3

CoS: (3), очередь 4

CoS: (4), очередь 5

CoS: (5), очередь 6

CoS: (6), очередь 7

CoS: (7), очередь 8

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos map cos-queue 7 to 5
```

qos map dscp-mutation

Данная команда устанавливает соответствие между значениями кодов DSCP входящих пакетов и кодов DSCP на выходе из устройства.

Использование отрицательной формы команды (no) устанавливает соответствие по умолчанию.

Синтаксис

```
qos map dscp-mutation <DSCP> to <DSCP>
no qos map dscp-mutation <DSCP>
```

Параметры

<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63].

Значения по умолчанию:

Значения кодов DSCP входящих пакетов и кодов DSCP на выходе из устройства совпадают.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos map dscp-mutation 10 to 40
```

qos map dscp-queue

Данная команда устанавливает соответствие между значениями кодов DSCP входящих пакетов и исходящими очередями.

Использование отрицательной формы команды (no) устанавливает соответствие по умолчанию.

Синтаксис

```
qos map dscp-queue <DSCP> to <QUEUE>
no qos map dscp-queue <DSCP>
```

Параметры

<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63];

<QUEUE> – внутренняя очередь, в которую необходимо отправлять пакеты с ранее описанным DSCP, принимает значение [1..8].

Значения по умолчанию:

DSCP: (0-7), очередь 1

DSCP: (8-15), очередь 2

DSCP: (16-23), очередь 3

DSCP: (24-31), очередь 4

DSCP: (32-39), очередь 5

DSCP: (40-47), очередь 6

DSCP: (48-55), очередь 7

DSCP: (56-63), очередь 8

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos map dscp-queue 42 to 5
```

qos queue default

Данная команда устанавливает номер очереди по умолчанию, в которую попадает весь трафик, кроме IP, в режиме доверия DSCP-приоритетам в случае с Basic QoS, а также неклассифицированный трафик в случае с Policy-based QoS.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
qos queue default <QUEUE>
no qos queue default
```

Параметры

<QUEUE> – идентификатор очереди, принимает значения [1..8].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos queue default 3
```

qos trust

Данной командой устанавливается режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах для Basic QoS-режима работы интерфейса.

Использование отрицательной формы команды (no) устанавливает соответствие по умолчанию.

Синтаксис

```
qos trust <MODE>
no qos trust
```

Параметры

<MODE> – режим доверия к значениям кодов 802.1p и DSCP, принимает одно из следующих значений:

- dscp – режим доверия значениям кодов DSCP в IP-заголовке. Не IP-пакеты будут направлены в очередь по умолчанию (команда описана в разделе qos queue default);
- cos – режим доверия значениям кодов 802.1p в теге 802.1q. Нетегированные пакеты будут направлены в очередь по умолчанию (команда описана в разделе qos queue default);

- cos-dscp – режим доверия значениям кодов DSCP для IP-пакетов и значениям кодов 802.1p для остальных пакетов.

Значения по умолчанию

Режим доверия значениям кодов DSCP (dscp).

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos trust cos-dscp
```

qos wrr-queue

Данной командой определятся веса для соответствующих взвешенных очередей.

Использование отрицательной формы команды (no) устанавливает значение веса для указанной очереди по умолчанию.

Синтаксис

```
qos wrr-queue <QUEUE> bandwidth <WEIGHT>
no qos wrr-queue <QUEUE>
```

Параметры

<QUEUE> – идентификатор очереди, принимает значение [1..8];

<WEIGHT> – значение веса, принимает значение [1..255].

Значение по умолчанию

1

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# qos wrr-queue 3 bandwidth 130
```

queue-limit

Данной командой определяется предельное количество пакетов для виртуальной очереди.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
queue-limit <QUEUE-LIMIT>
no queue-limit
```

Параметры

<QUEUE-LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [2..4096].

Значение по умолчанию

127

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# queue-limit 200
```

random-detect

Данной командой определяются параметры RED.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
random-detect <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>
no random-detect
```

Параметры

<LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<APS> – средний размер пакета в байтах, принимает значение в диапазоне [1..10000000];

<APS-NUM> – количество пакетов среднего размера разрешенных для кратковременного пропускания, принимает значение в диапазоне [0..10000000];

<PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].

При указании значений должны выполняться следующие правила:

<MAX> > 2 * <MIN> <LIMIT> >3 * <MAX>

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# random-detect 9000 1500 3000 10
```

random-detect queue

Данной командой определяются параметры GRED.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
random-detect queue <QUEUE-NUM> [ dscp <DSCP> | precedence <IPP> ] <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>
```

```
no random-detect queue <PRECEDENCE>
```

Параметры

<QUEUE-NUM> – номер очереди [1..16];

<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63];

<IPP> – значение кода IP Precedence, принимает значения [0..7];

<PRECEDENCE> – значение IP Precendence [0..7];

<LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

<APS> – средний размер пакета в байтах, принимает значение в диапазоне [1..10000000];

<APS-NUM> – количество пакетов среднего размера разрешенных для кратковременного пропускания, принимает значение в диапазоне [0..10000000];

<PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].

При указании значений должны выполняться следующие правила:

<MAX> > 2 * <MIN>

<LIMIT> > 3 * <MAX>

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# random-detect precedence 2 9000 1500 3000 10
```

random-detect queue default

Данной командой определяется очередь по умолчанию для механизма GRED.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
random-detect queue default <QUEUE-NUM>
no random-detect queue default <QUEUE-NUM>
```

Параметры

<QUEUE-NUM> – номер очереди [1..16].

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# random-detect queue default
```

rate-limit

Данная команда устанавливает ограничение скорости входящего трафика. Команда актуальна только для Basic QoS режима интерфейса.

Использование отрицательной формы команды (no) снимает ограничение.

Синтаксис

```
rate-limit <BANDWIDTH> [BURST]
no rate-limit
```

Параметры

<BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [1..10000000] для TengigabitEthernet интерфейсов и [1..1000000] для прочих интерфейсов и туннелей;

<BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-L2TPV3

CONFIG-L2TP

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-OPENVPN

Пример

```
wlc-30(config-if-gi)# rate-limit 1670000
```

service-policy

Данная команда используется для привязки указанной QoS-политики к конфигурируемому интерфейсу для классификации входящего (input) или приоритизации исходящего (output) трафика.

Использование отрицательной формы команды (no) удаляет привязку политики к данному интерфейсу.

Синтаксис

```
service-policy { input | output } <NAME>
service-policy dynamic { upstream | downstream | all }
no service-policy { input | output }
```

Параметры

<NAME> – имя QoS-политики, задаётся строкой до 31 символа;

dynamic – привязка динамической QoS-политики к конфигурируемому интерфейсу для приоритизации восходящего (upstream), нисходящего (downstream) или всего (all) трафика. Политика наполняется данными, полученными от RADIUS-сервера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-L2TPV3

CONFIG-SUBTUNNEL (Только с ключом "input")

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

CONFIG-OPENVPN

Пример

```
wlc-30(config-if-gi)# service-policy input input_policy
```

service-policy

Данной командой привязывается политика QoS к классу для создания иерархического QoS.

Использование отрицательной формы команды (no) удаляет привязку политики к классу.

Синтаксис

```
[no] service-policy <NAME>
```

Параметры

<NAME> – имя политики, задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# service-policy input_policy
```

set class-default cos

Данной командой задается значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих классу по умолчанию (class-default).

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set class-default cos <COS>
no set class-default cos
```

Параметры

<COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-policy-map)# set class-default cos 5
```

set class-default dscp

Данной командой задается значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих классу по умолчанию (class-default).

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set class-default dscp <DSCP>
no set class-default dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-policy-map)# set class-default dscp 16
```

set class-default ip-precedence

Данной командой задается значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих классу по умолчанию (class-default).

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set class-default ip-precedence <IPP>
no set class-default ip-precedence
```

Параметры

<IPP> – значение кода IP Precedence, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-policy-map)# set class-default ip-precedence 5
```

set cos

Данной командой задается значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигурируемому классу.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set cos <COS>
no set cos
```

Параметры

<COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# set cos 5
```

set dscp

Данной командой задается значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set dscp <DSCP>
no set dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# set dscp 16
```

set ip-precedence

Данной командой задается значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу.

Использование отрицательной формы команды (no) отменяет назначение.

Синтаксис

```
set ip-precedence <IPP>
no set ip-precedence
```

Параметры

<IPP> – значение кода IP Precedence, принимает значения [0..7].

Необходимый уровень привилегий

10

Командный режим

CONFIG-CLASS-MAP

Пример

```
wlc-30(config-class-map)# set ip-precedence 5
```

shape auto-distribution

Данной командой включается автоматическое распределение полосы пропускания между классами, в которых нет настройки полосы пропускания, включая класс по умолчанию.

Использование отрицательной формы команды (no) отключает автоматическое распределение полосы.

Синтаксис

```
[no] shape auto-distribution
```

Параметры

Команда не имеет параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

Пример

```
wlc-30(config-policy-map)# shape auto-distribution
```

shape average

Данной командой устанавливается гарантированная полоса исходящего трафика для определенного класса или политики в целом.

Использование отрицательной формы команды (no) снимает ограничение.

Синтаксис

```
shape average { <BANDWIDTH> | percent <BANDWIDTH_PERCENT> } [<BURST>]
no shape average
```

Параметры

<BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [1..10000000];

<BURST> – размер сдерживающего порога в байтах, принимает значение [128..16000000];

<BANDWIDTH_PERCENT> – гарантированная полоса трафика в %, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению):

- значения shape average корневой политики;
- значения traffic-shape на сетевом интерфейсе, bridge, туннеле;
- значения speed сетевого интерфейса.

Принимает значение [1..100].

Значения по умолчанию:

<BANDWIDTH> – отсутствует

<BURST> – 128000

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map)# shape average 100000 2000
```

shape peak

Устанавливается разделяемая полоса исходящего трафика для определенного класса. Данную полосу класс может занять, если другие классы не заняли свою гарантированную полосу. Конфигурация актуальна только для классов работающих во взвешенном режиме (WRR).

Использование отрицательной формы команды (no) снимает ограничение.

Синтаксис

```
shape peak { <BANDWIDTH> | percent <PERCENT> } [<BURST>]
no shape peak
```

Параметры

<BANDWIDTH> – разделяемая полоса трафика в Кбит/с, принимает значение [1..10000000];

<BURST> – размер сдерживающего порога в байт, принимает значение [128..16000000];

<BANDWIDTH_PERCENT> – общая для priority class полоса трафика в %, конкуренция происходит на основании приоритета класса, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению):

- значения shape average корневой политики;
- значения traffic-shape на сетевом интерфейсе, bridge, туннеле;
- значения speed сетевого интерфейса.

Принимает значение [1..100].

Значения по умолчанию:

<BANDWIDTH> – отсутствует

<BURST> – 128000

Необходимый уровень привилегий

10

Командный режим

CONFIG-POLICY-MAP-CLASS

Пример

```
wlc-30(config-policy-map-class)# shape average 100000 2000
```

show qos interface shapers

Данная команда показывает параметры QoS сетевых интерфейсов.

Синтаксис

```
show qos interface shapers <IF>
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos interface shapers gigabitethernet 1/0/2
gigabitethernet 1/0/2
Committed rate:  100000 Kbps
Committed burst: 1600 KBytes
```

show qos map cos-queue

Данная команда показывает информацию о соответствии кодов 802.1p в пакетах и выходных очередей, используемых в QoS.

Синтаксис

```
show qos map cos-queue
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos map dscp-queue
d1 : d2   0  1  2  3  4  5  6  7
-------   ------------------------
0         01 02 03 04 05 06 07 08
```

show qos map dscp-mutation

Данная команда показывает информацию о соответствии кодов DSCP в пакетах и кодов DSCP после изменений.

Синтаксис

```
show qos map dscp-mutation
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos map dscp-mutation
d1 : d2   0  1  2  3  4  5  6  7  8  9
-------   --------------------------------
0         00 01 02 03 04 05 06 07 08 09
1         10 11 12 13 14 15 16 17 18 19
2         20 21 22 23 24 25 26 27 28 29
3         30 31 32 33 34 35 36 37 38 39
4         40 41 42 43 44 45 46 47 48 49
5         50 51 52 53 54 55 56 57 58 59
6         60 61 62 63
```

show qos map dscp-queue

Данная команда показывает информацию о соответствии кодов DSCP в пакетах и выходных очередей, используемых в QoS.

Синтаксис

```
show qos map dscp-queue
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos map dscp-queue
d1 : d2   0  1  2  3  4  5  6  7  8  9
-------   ------------------------------
0         01 01 01 01 01 01 01 01 02 02
1         02 02 02 02 02 02 03 03 03 03
2         03 03 03 03 04 04 04 04 04 04
3         04 04 05 05 05 05 05 05 05 05
4         06 06 06 06 06 06 06 06 07 07
5         07 07 07 07 07 07 08 08 08 08
6         08 08 08 08
```

show qos policy binding

Данная команда используется для просмотра привязанной QoS-политики к заданному интерфейсу для классификации входящего (input) или приоритизации исходящего (output) трафика.

Синтаксис

```
show qos policy binding [ <IF> | <TUN> ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos policy binding gi1/0/1
gigabitethernet 1/0/1
Output: parent
    Class: class1
        Policy: child1
            Class: class3
    Class: class2
        Policy: child2
```

show qos policy configuration

Данная команда выводит конфигурацию заданной политики QoS.

Синтаксис

```
show qos policy configuration <NAME>
```

Параметры

<NAME> – имя политики, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos policy configuration parent
Policy-map: parent
    Shape average:
        Bandwidth:          --
        Burst:              128
    Class: class1
        Set:
            COS:            --
            DSCP:           --
            IP-Precedence:  --
            Queue:          --
        Match access group: --
        Shape average:
            Bandwidth:      --
            Burst:          128
        Shape peak:
            Bandwidth:      --
            Burst:          128
        Mode:               FIFO
        Priority class:     8
        Queue limit:        127
        Service policy:     child1
    Class: class2
        Set:
            COS:            --
            DSCP:           --
            IP-Precedence:  --
            Queue:          --
        Match access group: --
        Shape average:
            Bandwidth:      --
            Burst:          128
        Shape peak:
            Bandwidth:      --
            Burst:          128
        Mode:               FIFO
        Priority class:     8
        Queue limit:        127
        Service policy:     child2
```

show qos policy statistics

Данная команда выводит статистику по переданным и отброшенным пакетам. Команда актуальна только для Policy-based QoS режима интерфейса.

Синтаксис

```
show qos policy statistics [ <IF> | <TUN> ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30#  sh qos policy statistics
gigabitethernet 1/0/2
   Policy pom-1
   Input policy root
   Input class root
   Shape: bytes 750947679, packets 496667, drops 1002200
       Class clm-1
           Shape: bytes 750946896, packets 496658, drops 1002200
       Class class-default
           Shape: bytes 783, packets 9, drops 0
```

show qos statistics

Данная команда выводит статистику по переданным и отброшенным пакетам. Команда актуальна только для basic QoS режима интерфейса.

Синтаксис

```
show qos statistics [ <IF> | <TUN> ]
```

Параметры

<IF> – интерфейс или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos statistics vti 2
vti 2
Queue   Bytes                   Packets                 Drops
-----   --------------------    --------------------    --------------------
1       0                       0                       0
2       0                       0                       0
3       0                       0                       0
4       0                       0                       0
5       0                       0                       0
6       964073836       1413598          0
7       121389180       177990            1235497
8       0                       0                       0
```

show qos tunnel shapers

Данная команда показывает параметры QoS-туннелей.

Синтаксис

```
show qos tunnel shapers <TUN>
```

Параметры

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show qos tunnel shapers vti 2
vti 2
qid   Target        Target
      Committed     Committed
      Rate [Kbps]   Burst [KBytes]
---   -----------   --------------
1     10000         128
2     6000          128
```

traffic-shape

Данная команда устанавливает ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом. Команда актуальна только для Basic QoS режима интерфейса.

Использование отрицательной формы команды (no) снимает ограничение.

Синтаксис

```
traffic-shape { <BANDWIDTH> [BURST] | queue <QUEUE> <BANDWIDTH> [BURST] }
no traffic-shape [ queue <QUEUE> ]
```

Параметры

<QUEUE> – идентификатор очереди, принимает значение [1..8];

<BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значения:

- для интерфейсов gigabitethernet, loopback, e1: [1..10000000];
- для интерфейсов tengigabitethernet: [3000..100000000];
- для интерфейсов fortyengigabitethernet: [3000..40000000];
- для интерфейсов loopback:
    - <BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. Возможно указывать значение только кратное 4.

Значения по умолчанию:

<BANDWIDTH> – отсутствует

<BURST> – 128

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-BRIDGE

CONFIG-LOOPBACK

CONFIG-E1

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-VTI

CONFIG-L2TPV3

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

CONFIG-OPENVPN

Пример

```
wlc-30(config-if-gi)# traffic-shape queue 3 100000 2000
```

29 Мониторинг и управление

- Управление Netflow
- Управление sFlow
- Управление SNMP
- Управление SYSLOG
- Настройка доступа SSH, Telnet
- Настройка протокола LLDP
- Настройка зеркалирования
- Настройка zabbix-agent и zabbix-proxy

Управление Netflow

- ip netflow export
- netflow active-timeout
- netflow collector
- netflow domain-id
- netflow enable
- netflow export-events web-proxy
- netflow export-options
- netflow inactive-timeout
- netflow max-flows
- netflow refresh-rate
- netflow version
- port
- show netflow configuration
- show netflow statistics
- show netflow statistics cpu
- source-address

ip netflow export

Данная команда используется для включения экспорта статистики Netflow на сетевом интерфейсе.

Использование отрицательной формы команды (no) отключает экспорт статистики Netflow на сетевом интерфейсе.

Синтаксис

```
ip netflow export [ <DIRECTION> ]
no ip netflow export
```

Параметры

<DIRECTION> – направление трафика, по которому собирается статистика, принимает значения:

- ingress – статистика собирается только для входящего трафика;
- egress – статистика собирается только для исходящего трафика;
- both – статистика собирается для входящего и исходящего трафика.

Значение по умолчанию

both

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-E1

CONFIG-MULTILINK

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-BRIDGE

CONFIG-LT

CONFIG-PPPOE

Пример

```
wlc-30(config-if-gi)# ip netflow export
```

netflow active-timeout

Данной командой задаётся интервал, по истечении которого информация об активных сессиях экспортируются на коллектор.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow active-timeout <TIMEOUT>
no netflow active-timeout
```

Параметры

<TIMEOUT> – задержка перед отправкой информации об активных сессиях, задается в секундах, принимает значение [5..36000].

Значение по умолчанию

1800 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow active-timeout 30
```

netflow collector

Данная команда используется для создания коллектора Netflow и перехода в командный режим CONFIG-NETFLOW-HOST.

Использование отрицательной формы команды (no) удаляет сконфигурированный коллектор Netflow.

Синтаксис

```
[no] netflow collector <ADDR> [ vrf <VRF> ]
```

Параметры

<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow collector 10.100.100.1
wlc-30(config-netflow-host)#
```

netflow domain-id

Данной командой устанавливается значение Observation Domain ID в пакетах Netflow.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow domain-id <ID>
```

```
no netflow domain-id
```

Параметры

<ID> – значение Observation Domain ID, принимает значение [0.. 4294967295].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow domain-id 35
```

netflow enable

Данной командой активируется Netflow на контроллере.

Использование отрицательной формы команды (no) деактивирует Netflow на контроллере.

Синтаксис

```
[no] netflow enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow enable
```

netflow export-events web-proxy

Данная команда позволяет включить передачу netflow статистики о пакетах, переданных через web-proxy.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] netflow export-events web-proxy
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow export-events web-proxy
```

netflow export-options

Данная команда позволяет включить дополнительные поля в экспортируемую на коллектор информацию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] netflow export-options { http-host | http-url }
```

Параметры

http-host – для HTTP/HTTPS-сессий будет добавляться информация о домене хоста, на который был отправлен HTTP-запрос. Поле в Netflow-пакете имеет идентификатор 24884, размерность 128 байт;

http-url – для HTTP-сессий будет добавляться информация о URL, на который был отправлен HTTP-запрос. Поле в Netflow-пакете имеет идентификатор 24887, размерность 384 байта.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow export-options http-host
```

netflow inactive-timeout

Данной командой задаётся интервал, по истечении которого информация об устаревших сессиях экспортируется на коллектор.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow inactive-timeout <TIMEOUT>
no netflow inactive-timeout
```

Параметры

<TIMEOUT> – задержка перед отправкой информации об устаревших сессиях, задается в секундах, принимает значение [0..240].

Значение по умолчанию

15

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow inactive-timeout 30
```

netflow max-flows

Данной командой задаётся максимальное количество наблюдаемых сессий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow max-flows <COUNT>
no netflow max-flows
```

Параметры

<COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000].

Значение по умолчанию

512000

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow max-flows 300000
```

netflow refresh-rate

Данной командой задаётся частота отправки шаблонов на Netflow-коллектор.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow refresh-rate <RATE>
no netflow refresh-rate
```

Параметры

<RATE> – частота отправки статистики, задается в пакетах на поток, принимает значение [1..10000].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow refresh-rate 100
```

netflow version

Данной командой задаётся версия Netflow-протокола.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
netflow version <VERSION>
no netflow version
```

Параметры

<VERSION> – версия Netflow-протокола: 5, 9 и 10.

Значение по умолчанию

9

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# netflow version 10
```

port

Данной командой определяется порт Netflow-сервиса на сервере сбора статистики.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер UDP-порта, указывается в диапазоне [1..65535].

Значение по умолчанию

2055

Необходимый уровень привилегий

15

Командный режим

CONFIG-NETFLOW-HOST

Пример

```
wlc-30(config-netflow-host)# port 5555
```

show netflow configuration

Командой выполняется просмотр параметров конфигурации Netflow-агента.

Синтаксис

`show netflow configuration`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show netflow configuration
Netflow configuration:
Global state:      Enabled
Version:           9
Maxflows:          10001
Refresh rate:      10
Inactive timeout:  15
Host: 115.0.0.10  Port: 2055
```

show netflow statistics

Команда для просмотра текущей информации о работе Netflow.

Синтаксис

```
show netflow statistics
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show netflow statistics
Flows: active 9 (peak 34 reached 1d4h20m ago), mem 3841K
Hash: size 491496 (mem 3839K). InHash: 760 pkt, 339 K, InPDU 4, 160.
Processed rate   Bits/s           Packets/s
--------------   --------------   ---------------
Current                    5142                2
1 Min Avg                  4921                0
5 Min Avg                  4874                0
Export: Rate 0 bytes/s; Total 3952 pkts, 3 MB, 28818 flows; Errors 2 pkts; Traffic lost 0 pkts,
0 Kbytes, 0 flows.
```

show netflow statistics cpu

Команда для просмотра статистики по распределению информации о нагрузке Netflow на ЦПУ.

Синтаксис

```
show netflow statistics
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show netflow statistics cpu
                Traffic,      Traffic,  Drop,         Drop,
cpu    PPS      Packets       MBytes    Packets       KBytes
-----  -------  ------------  --------  ------------  --------
Total        1        215224        61             0         0
cpu0         0             0         0             0         0
cpu1         0         10485         0             0         0
cpu2         0          2676         0             0         0
cpu3         0         12893         0             0         0
cpu4         0             0         0             0         0
cpu5         1        106264        53             0         0
cpu6         0          2684         0             0         0
cpu7         0         10213         0             0         0
cpu8         0          6770         0             0         0
cpu9         0          5424         0             0         0
cpu10        0          2505         0             0         0
cpu11        0         10919         1             0         0
cpu12        0         13395         0             0         0
cpu13        0          2769         0             0         0
cpu14        0         14050         0             0         0
cpu15        0         14177         1             0         0
```

source-address

Данной командой определяется IP-адрес контроллера, который будет использоваться в качестве IP-адреса источника в отправляемых Netflow-пакетах.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

`source-address <ADDR>`

`no source-address`

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-NETFLOW-HOST

Пример

```
wlc-30(config-netflow-host)# source-address 10.100.100.2
```

Управление sFlow

- ip sflow export
- port
- sflow collector
- sflow enable
- sflow poll-interval
- sflow sampling-rate
- show sflow configuration

ip sflow export

Данная команда используется для включения экспорта статистики sFlow на сетевом интерфейсе. Функция sFlow на сетевом интерфейсе может быть включена, если на интерфейсе выключена функция Firewall (раздел ip firewall disable), в ином случае экспорт статистики sFlow настраивается в правиле Firewall (раздел action).

Использование отрицательной формы команды (no) отключает экспорт статистики sFlow на сетевом интерфейсе.

Синтаксис

```
[no] ip sflow export
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-CELLULAR-MODEM

CONFIG-E1

CONFIG-MULTILINK

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-BRIDGE

CONFIG-LT

CONFIG-PPPOE

Пример

```
wlc-30(config-if-gi)# ip sflow export
```

port

Данной командой определяется порт sFlow-сервиса на сервере сбора статистики.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`port <PORT>`

`no port`

Параметры

<PORT> – номер UDP-порта, указывается в диапазоне [1..65535].

Значение по умолчанию

6343

Необходимый уровень привилегий

15

Командный режим

CONFIG-SFLOW-HOST

Пример

```
wlc-30(config-sflow-host)# port 5556
```

sflow collector

Данная команда используется для создания коллектора sFlow и перехода в командный режим CONFIG-SFLOW-HOST.

Использование отрицательной формы команды (no) удаляет сконфигурированный коллектор sFlow.

Синтаксис

`[no] sflow collector <ADDR>`

Параметры

<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# sflow collector 10.100.100.1
wlc-30(config-sflow-host)#
```

sflow enable

Данной командой активируется sFlow на контроллере.

Использование отрицательной формы команды (no) деактивирует sFlow на контроллере.

Синтаксис

```
[no] sflow enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# sflow enable
```

sflow poll-interval

Данной командой задаётся интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
sflow poll-interval <TIMEOUT>
no sflow poll-interval
```

Параметры

<TIMEOUT> – интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса, принимает значение [1..300].

Значение по умолчанию

10 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# sflow poll-interval 30
```

sflow sampling-rate

Данной командой задаётся частота отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
sflow sampling-rate <RATE>
no sflow sampling-rate
```

Параметры

<RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..65535]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти.

Значение по умолчанию

1000

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# sflow sampling-rate 100
```

show sflow configuration

Командой выполняется просмотр параметров конфигурации sFlow-агента.

Синтаксис

```
show sflow configuration
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show sflow configuration
sFlow configuration:
Global state:   Enabled
Sample rate:    1000
Poll interval:  10
Host: 115.0.0.10  Port: 6800
Host: 115.0.0.20  Port: 6343
Host: 115.0.0.30  Port: 6343
```

Управление SNMP

- access
- authentication access
- authentication algorithm
- authentication key
- client-list
- community
- ip address
- ipv6 address
- enable
- oid-tree
- port
- privacy algorithm
- privacy key
- rmon collection statistics
- snmp-server
- snmp-server community
- snmp-server contact
- snmp-server dscp
- snmp-server enable traps
- snmp-server enable traps config
- snmp-server enable traps entity
- snmp-server enable traps entity-sensor
- snmp-server enable traps environment
- snmp-server enable traps envmon
- snmp-server enable traps files-operations
- snmp-server enable traps flash
- snmp-server enable traps interfaces
- snmp-server enable traps ports
- snmp-server enable traps screens
- snmp-server enable traps snmp
- snmp-server enable traps syslog
- snmp-server enable traps wifi
- snmp-server host
- snmp-server location
- snmp-server system-shutdown
- snmp-server trap link
- snmp-server user
- snmp-server view
- source-address
- source-interface
- view

access

Данной командой определяется уровень доступа по протоколу SNMPv3.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
access <TYPE>
no access
```

Параметры

<TYPE> – уровень доступа:

- ro – доступ только для чтения;
- rw – доступ для чтения и записи.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# access rw
```

authentication access

Данной командой определяется режим безопасности.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
authentication access <TYPE>
no authentication access
```

Параметры

<TYPE> – режим безопасности:

- auth – используется только аутентификация;
- priv – используется аутентификация и шифрование данных.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# authentication algorithm auth
```

authentication algorithm

Данная команда определяет алгоритм аутентификации SNMPv3-запросов.

Использование отрицательной формы команды (no) отключает аутентификацию.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм шифрования:

- md5 – пароль шифруется по алгоритму md5;
- sha1 – пароль шифруется по алгоритму sha1.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# authentication algorithm md5
```

authentication key

Данная команда устанавливает пароль для аутентификации SNMPv3-запросов.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 32 символов;

encrypted – при указании команды задается зашифрованный пароль:

- <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 32 байт (от 16 до 64 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# authentication key ascii-text 123456789
wlc-30(config-snmp-user)# authentication key ascii-text encrypted CDE65039E5591FA3F1
```

client-list

Данной командой активируется фильтрация и устанавливается профиль IP-адресов, с которых могут приниматься SNMPv3 пакеты с данным именем SNMPv3 пользователя.

Использование отрицательной формы команды (no) деактивирует фильтрацию принимаемых SNMPv3-пакетов.

Синтаксис

`[no] client-list <NAME>`

Параметры

<NAME> – имя ранее сознанной object-group, задается строкой до 31 символа.

Значение по умолчанию

Ограничения отключены.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# client-list OBG005
```

community

Данной командой определяется SNMP-community для отправки уведомлений на удаленный сервер.

Использование отрицательной формы команды (no) удаляет значение community.

Синтаксис

`community <COMMUNITY>`

`no community`

Параметры

<COMMUNITY> – сообщество для доступа по протоколу SNMP, задается строкой длинной [1..128] символа.

Значение по умолчанию

community – не задано.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-HOST

Пример

```
wlc-30(config-snmp-host)# community privatekey
```

ip address

Данной командой активируется фильтрация и устанавливается IP-адрес, которому предоставлен доступ к контроллеру под данным SNMPv3-пользователем.

Использование отрицательной формы команды (no) деактивирует фильтрацию принимаемых SNMPv3–пакетов.

Синтаксис

```
[no] ip address <ADDR>
```

Параметры

<ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Ограничения отключены.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# ip address 192.168.85.33
```

ipv6 address

Данной командой активируется фильтрация и устанавливается IPv6-адрес, которому предоставлен доступ к контроллеру под данным SNMPv3-пользователем.

Использование отрицательной формы команды (no) деактивирует фильтрацию принимаемых SNMPv3–пакетов.

Синтаксис

```
[no] ipv6 address <IPV6-ADDR>
```

Параметры

<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# ipv6 address AC:05:12:44::24
```

enable

Данной командой активируется SNMPv3-пользователь.

Использование отрицательной формы команды (no) деактивирует SNMPv3-пользователя.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# enable
```

oid-tree

Данной командой устанавливается OID и действие применяемое к нему (разрешить/запретить). Более длинные OID имеют преимущество.

OID указывается в цифровой нотации.

Использование отрицательной формы команды (no) удаляет запись oid-tree.

Синтаксис

```
oid-tree <OID> <ACTION>
no oid-tree <OID>
```

Параметры

<OID> – OID, задаётся строкой до 255 символов;

<ACTION> – действие, применяемое к OID:

- excluded – запретить использование OID;
- included – разрешить использование OID.

Значение по умолчанию

Разрешено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-VIEW

Пример

```
wlc-30(config-snmp-view)# oid-tree 1.3.6.1.2.1.2.2 excluded
```

port

Данной командой определяется порт коллектора SNMP уведомлений на удаленном сервере.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер UDP-порта, указывается в диапазоне [1..65535].

Значение по умолчанию

162

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-HOST

Пример

```
wlc-30(config-snmp-host)# port 5555
```

privacy algorithm

Данная команда определяет алгоритм шифрования передаваемых данных.

Использование отрицательной формы команды (no) отключает шифрование.

Синтаксис

```
privacy algorithm <ALGORITHM>
no privacy algorithm
```

Параметры

<ALGORITHM> – алгоритм шифрования:

- aes128 – использовать алгоритм шифрования AES-128;
- des – использовать алгоритм шифрования DES.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# privacy algorithm des
```

privacy key

Данная команда устанавливает пароль для шифрования передаваемых данных.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
privacy key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no privacy key
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 32 символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 32 байт (от 16 до 64 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# privacy key ascii-text 123456789
wlc-30(config-snmp-user)# privacy key ascii-text encrypted CDE65039E5591FA3F1
```

rmon collection statistics

Данная команда включается сохранение RMON-статистики для физического интерфейса.

Использование отрицательной формы команды (no) отключается сохранение RMON-статистики для физического интерфейса.

Синтаксис

```
rmon collection statistics <INDEX> owner <OWNER>
no rmon collection statistics
```

Параметры

<INDEX> – RMON-индекс данного интерфейса;

<OWNER> – текстовое поле длинной [1..127] символов описывающее владельца создавшего данный процесс.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример

```
wlc-30(config-if-gi)# rmon collection statistics 17 owner admin
```

snmp-server

Данной командой включается SNMP-сервер как в глобальной таблице маршрутизации так и во всех созданных VRF.

Использование отрицательной формы команды (no) выключает SNMP-сервер.

Синтаксис

```
[no] snmp-server
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server
```

snmp-server community

Данной командой определяется сообщество для доступа по протоколу SNMP.

Использование отрицательной формы команды (no) удаляет настройки сообщества.

Синтаксис

```
[no] snmp-server community <COMMUNITY> [ <TYPE> ] [ { <ADDR> | <IPV6-ADDR> } ] [client-
list <OBJ-GROUP-NETWORK-NAME> ] [ <VERSION> ] [ view <VIEW-NAME> ] [ vrf <VRF> ]
```

Параметры

<COMMUNITY> – сообщество для доступа по протоколу SNMP, задается строкой длинной [1..128] символа;

<TYPE> – уровень доступа:

- ro – доступ только для чтения;
- rw – доступ для чтения и записи.

<ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задаётся строкой до 31 символа;

<VERSION> – версия snmp, поддерживаемая данным community, принимает значения v1 или v2c;

<VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID;

<VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server community public rw
```

snmp-server contact

Данной командой устанавливается значение переменной SNMP, содержащей контактную информацию (по умолчанию не определена). Для удобства в параметрах можно указать ответственного за данное оборудование, например, его фамилию.

Использование отрицательной формы команды (no) удаляет значение переменной SNMP, содержащей контактную информацию.

Синтаксис

```
[no] snmp-server contact <CONTACT>
```

Параметры

<CONTACT> – контактная информация, задаётся строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server contact ivanov_ivan
```

snmp-server dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
snmp-server dscp <DSCP>
no snmp-server dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

61

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server dscp 40
```

snmp-server enable traps

Данная команда разрешает отправку всех типов SNMP-уведомлений.

Использование отрицательной формы команды (no) отменяет разрешение отправки всех типов SNMP-уведомлений.

Синтаксис

```
[no] snmp-server enable traps
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps
```

snmp-server enable traps config

Данная команда разрешает отправку SNMP-уведомлений об операциях с конфигурацией.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps config [ <ACT> ]
```

Параметры

<ACT> – трапы фактов изменения конфигурации:

- commit – применение изменения конфигурации;
- confirm – подтверждение изменения конфигурации.

Без указания ключа <ACT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps config commit
```

snmp-server enable traps entity

Данная команда разрешает отправку SNMP-уведомлений об операциях с running-config.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps entity [ <ENT> ]
```

Параметры

<ENT> – типы фильтров параметров окружения:

- config-change – информация о операциях с running-config.

Без указания ключа <ENT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps entity
```

snmp-server enable traps entity-sensor

Данная команда разрешает отправку SNMP-уведомлений об изменении параметров окружения.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps entity-sensor [ <ENT> ]
```

Параметры

<ENT> – типы фильтров параметров окружения:

- threshold – информация о срабатывании пересечения пороговых значений.

Без указания ключа <ENT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps entity-sensor
```

snmp-server enable traps environment

Данная команда разрешает отправку SNMP-уведомлений об изменении параметров окружения.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps environment [ <ENV> ]
```

Параметры

<ENV> – типы фильтров параметров окружения:

- pwrin – отказ БП;
- pwrin-insert – БП установлен;
- fan – отказ вентилятора;
- fan-speed-changed – изменение скорости вентиляторов;
- fan-speed-high – скорость вращения вентиляторов превысила максимальный порог;
- memory-flash-low – свободный объем NAND меньше заданного порога;
- memory-flash-critical-low – свободный объем NAND меньше заданного критического порога;
- memory-ram-low – свободный объем RAM меньше заданного порога;
- memory-ram-critical-low – свободный объем RAM меньше заданного критического порога;
- cpu-load – высокая нагрузка ЦПУ;
- cpu-overheat-temp – температура CPU превысила заданный максимальный порог;
- cpu-critical-temp – температура CPU превысила заданный критический порог;
- cpu-supercooling-temp – температура CPU упала ниже заданного минимального порога;
- switch-overheat-temp – температура коммутатора превысила заданный максимальный порог;
- switch-supercooling-temp – температура коммутатора упала ниже заданного минимального порога;
- board-overheat-temp – перегрев платы;
- board-supercooling-temp – переохлаждение платы;
- sfp-overheat-temp – перегрев sfp-модуля;
- sfp-supercooling-temp – переохлаждение sfp-модуля.

Без указания ключа <ENV> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps enviroment pwrin
```

snmp-server enable traps envmon

Данная команда разрешает отправку SNMP-уведомлений об изменении параметров окружения.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps envmon [ <ENV> ]
```

Параметры

<ENV> – типы фильтров параметров окружения:

- fan – информация о работе блоков вентиляторов;
- shutdown – информация о отключении контроллера;
- supply – информация о работе блоков питания;
- temperature информация о работе температурных датчиков.

Без указания ключа <ENV> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps envmon fun
```

snmp-server enable traps files-operations

Данная команда разрешает отправку SNMP-уведомлений об операциях с файлами.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps files-operations [ <ACT> ]
```

Параметры

<ACT> – типы фильтров параметров операций с файлами:

- successful – успешно;
- failed – неудачно;

- canceled – отменено.

canceled – отменено.

Без указания ключа <ACT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps files-operations canceled
```

snmp-server enable traps flash

Данная команда разрешает отправку SNMP-уведомлений об операциях с внешними flash-накопителями.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps flash [ <ACT> ]
```

Параметры

<ACT> – типы фильтров параметров операций с файлами:

- insertion – подключение flash-накопителя;
- removal – удаление flash-накопителя.

Без указания ключа <ACT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps flash removal
```

snmp-server enable traps interfaces

Данная команда разрешает отправку SNMP-уведомлений о изменении состояния интерфейсов.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps interfaces [ <ACT> ]
```

Параметры

<ACT> – типы фильтров параметров окружения:

- rx-utilization-high – поток входящих данных превышает порог;
- tx-utilization-high – поток исходящих данный превышает порог;
- number-high – превышение количества IP-интерфейсов.

Без указания ключа <ACT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps interfaces rx-utilization-high
```

snmp-server enable traps ports

Данная команда разрешает отправку SNMP-уведомлений о появлении ошибок на интерфейсах чипа коммутации.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps ports [ <TYPE> ]
```

Параметры

<TYPE> – типы фильтров состояние порта:

- port-counters-errors – ошибки на интерфейсах чипа коммутации.

Без указания ключа <TYPE> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps ports
```

snmp-server enable traps screens

Данная команда разрешает отправку SNMP-уведомлений о срабатывании защиты от определенного вида DoS-атак.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps screens [ <SCREEN> ]
```

Параметры

<SCREEN> – типы фильтров защиты от DoS-атак:

- dest-limit – ограничение количества одновременных сессий на основании адреса назначения;
- source-limit – ограничение количества одновременных сессий на основании адреса источника;
- icmp-threshold – защита от ICMP flood атак;
- udp-threshold – защита от UDP flood атак;
- syn-flood – защита от SYN flood атак;
- land – защита от land атак;
- winnuke – защита от winnuke атак;
- icmp-frag – блокировка фрагментированных ICMP-пакетов;
- syn-flag – блокировка фрагментированных TCP-пакетов, с флагом SYN;
- unknown-proto – блокировка пакетов, с ID протокола в заголовке IP равном 137 и более;
- ip-frag – блокировка фрагментированных пакетов;
- port-scan – защита от port scan атак;
- ip-sweep – защиту от IP-sweep атак;
- syn-fin – блокировка TCP-пакетов, с установленными флагами SYN и FIN;
- fin-no-ack – блокировка TCP-пакетов с установленным флагом FIN и не установленным флагом ACK;
- no-flag – блокировка TCP-пакетов, с нулевым полем flags;
- spoofing – защита от IP spoofing атак;
- reserved – блокировка всех ICMP-пакетов 2 и 7 типов (reserved);
- quench – блокировка всех ICMP-пакетов 4 типа (source quench);
- echo-request – блокировка всех ICMP пакетов 8 типа (echo-request);
- time-exceeded – блокировка всех ICMP-пакетов 11 типа (time exceeded);
- unreachable – блокировка всех ICMP-пакетов 3 типа (destination-unreachable);
- icmp-large – блокировка ICMP-пакетов большого объема;
- tcp-all-flags – блокировка tcp-пакетов с флагами;
- udp-frag – блокировка udp-пакетов с флагами.

Без указания ключа <LINK> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps screens reserved
```

snmp-server enable traps snmp

Данная команда разрешает отправку SNMP-уведомлений об изменении параметров окружения.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps snmp [ <ACT> ]
```

Параметры

<ACT> – типы фильтров параметров окружения:

- authentication – уведомления о snmp-запросах на контроллер с неверными community или snmpv3-паролем;
- coldstart – уведомления о перезапуске snmp-сервера на контроллере;
- linkdown – информация о изменении состояния link в down;
- linkup – информация о изменении состояния link в up.

Без указания ключа <ACT> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps snmp linkup
```

snmp-server enable traps syslog

Данная команда разрешает отправку SNMP-уведомлений с syslog-сообщениями.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps syslog
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps syslog
```

snmp-server enable traps wifi

Данная команда разрешает отправку SNMP-уведомлений с сообщениями о работе wifi-контроллера.

Использование отрицательной формы команды (no) отменяет разрешение отправки указанных типов уведомлений.

Синтаксис

```
[no] snmp-server enable traps wifi [ <NAME> ]
```

Параметры

<NAME> – типы трапа о туннелях softgre:

- wifi-tunnels-number-in-bridge-high – включение трапов о превышении количества sub-gre-тунелей включенных в bridge;
- wifi-tunnels-operation – включение трапов о результате snmp операций с туннелями softgre.

Без указания ключа <NAME> – активируется отправка всех трапов данной группы.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server enable traps syslog
```

snmp-server host

Данной командой включается передача SNMP-уведомлений на указанный IP-адрес и осуществляется переход в режим настройки SNMP-уведомлений.

Использование отрицательной формы команды (no) отключает передачу уведомлений на указанный коллектор SNMP-уведомлений.

Синтаксис

```
[no] snmp-server host { <ADDR> | <IPV6-ADDR> } [vrf <VRF>]
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<VRF> – имя экземпляра VRF, в котором находится коллектор SNMP-уведомлений, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp host 192.168.2.2
```

snmp-server location

Данной командой устанавливается значение переменной SNMP, содержащей информацию о расположении оборудования (по умолчанию не определено). Для удобства в параметрах можно указать город, улицу, район, номер комнаты и т.п.

Использование отрицательной формы команды (no) удаляет значение переменной, содержащей информацию о расположении оборудования.

Синтаксис

```
[no] snmp-server location <LOCATION>
```

Параметры

<LOCATION> – информацию о расположении оборудования, задаётся строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server location duglasa_adamsa_42
```

snmp-server system-shutdown

Данной командой разрешается перезагрузка контроллера при помощи snmp-сообщений.

Использование отрицательной формы команды (no) запрещает перезагрузку контроллера при помощи SNMP-сообщений.

Синтаксис

```
[no] snmp-server system-shutdown
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server system-shutdown
```

snmp-server trap link

Данной командой устанавливается режим отправки SNMP-trap.

Использование отрицательной формы команды (no) устанавливает режим по умолчанию.

Синтаксис

```
snmp-server trap link <MODE>
no snmp-server host
```

Параметры

<MODE> – режим отправки SNMP-trap. Принимает значения:

- ietf;
- cisco.

Значение по умолчанию

ietf

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server trap link cisco
```

snmp-server user

Данной командой создается SNMPv3-пользователь.

Использование отрицательной формы команды (no) удаляет SNMPv3-пользователя.

Синтаксис

```
[no] snmp-server user <NAME>
```

Параметры

<NAME> – имя пользователя, задаётся строкой от 1 до 128 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server user admin
wlc-30(config-snmp-user)#
```

snmp-server view

Данной командой создается профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3).

Использование отрицательной формы команды (no) удаляет профиль snmp view.

Синтаксис

```
[no] snmp-server view <VIEW-NAME>
```

Параметры

<VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# snmp-server view user_access
wlc-30(config-snmp-view)#
```

source-address

Данной командой определяется IP-адрес для отправки уведомлений на удаленный сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
source-address { <ADDR> | <IPV6-ADDR> }
no source-address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Значение по умолчанию

IPv4/IPv6 – адрес интерфейса ближайшего к удаленному SNMP-серверу.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-HOST

Пример

```
wlc-30(config-snmp-host)# source-address 192.168.22.17
```

source-interface

Данной командой определяется интерфейс или туннель контроллера, IPv4/IPv6-адрес которого будет использоваться для отправки уведомлений на удаленный сервер.

Использование отрицательной формы команды (no) удаляет указанный интерфейс или туннель.

Синтаксис

```
source-interface { <IF> | <TUN> }
no source-interface
```

Параметры

<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-HOST

Пример

```
wlc-30(config-snmp-host)# source-interface gigabitethernet 1/0/1
```

view

Данной командой устанавливается профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для SNMPv3 user.

Использование отрицательной формы команды (no) удаляет профиль snmp view.

Синтаксис

```
[no] view <VIEW-NAME>
```

Параметры

<VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SNMP-USER

Пример

```
wlc-30(config-snmp-user)# view user_view
```

Управление SYSLOG

- logging aaa configuration
- logging acl configuration
- logging firewall configuration
- logging login on-failure
- logging nat
- logging service start-stop
- logging syslog configuration
- logging userinfo
- match process-name
- ntp logging
- port
- remote-address
- severity
- source-address
- show syslog
- show syslog configuration
- syslog cli-commands
- syslog console
- syslog file
- syslog file-size
- syslog host
- syslog max-files
- syslog monitor
- syslog reload debugging
- syslog sequence-numbers
- syslog snmp
- syslog sip-level
- transport
- vrf

logging aaa configuration

Данной командой включается запись в локальный syslog-сервер сообщений о изменении конфигурации разделов aaa.

Использование отрицательной формы команды (no) выключает логирование сообщений о изменении конфигурации разделов aaa.

Синтаксис

```
[no] logging aaa configuration
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging aaa configuration
```

logging acl configuration

Данной командой включается запись в локальный syslog-сервер сообщений о изменении конфигурации ACL.

Использование отрицательной формы команды (no) выключает логирование сообщений о изменении конфигурации ACL.

Синтаксис

```
[no] logging acl configuration
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging acl configuration
```

logging firewall configuration

Данной командой включается запись в локальный syslog-сервер сообщений о изменении конфигурации межсетевого экрана.

Использование отрицательной формы команды (no) выключает логирование сообщений о изменении конфигурации межсетевого экрана.

Синтаксис

```
[no] logging firewall configuration
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging firewall configuration
```

logging login on-failure

Данной командой включается запись в локальный syslog-сервер сообщений о неуспешных попытках подключения к CLI.

Использование отрицательной формы команды (no) выключает логирование неудачных подключений.

Синтаксис

```
[no] logging login on-failure
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging login on-failure
```

logging nat

Данной командой включается запись в локальный syslog-сервер сообщений о работе сервиса NAT.

Использование отрицательной формы команды (no) выключает логирование сервиса NAT.

Синтаксис

```
[no] logging nat [<NAT-TYPE>]
```

Параметры

<NAT-TYPE> – тип сервиса NAT подлежащий логированию:

- destination;
- proxy;
- source;

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging nat source
```

logging service start-stop

Данной командой включается запись в локальный syslog-сервер сообщений о запуске и остановке используемых сервисов.

Использование отрицательной формы команды (no) выключает логирование запуска и остановки используемых сервисов.

Синтаксис

```
[no] logging service start-stop
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging service start-stop
```

logging syslog configuration

Данной командой включается запись в локальный syslog-сервер сообщений о изменении конфигурации syslog-сервера.

Использование отрицательной формы команды (no) выключает логирование сообщений о изменении конфигурации syslog-сервера.

Синтаксис

```
[no] logging syslog configuration
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging syslog configuration
```

logging userinfo

Данной командой включается запись в локальный syslog-сервер сообщений о изменении user-profile.

Использование отрицательной формы команды (no) выключает логирование сообщений об изменении user-profile.

Синтаксис

```
[no] logging userinfo
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# logging userinfo
```

match process-name

Данной командой активируется или деактивируется сохранение в локальный syslog-файл или отправка на удаленный syslog-сервер событий работы отдельных процессов контроллера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
match [not] process-name <PROCESS-NAME>
no match process-name { <PROCESS-NAME> | all }
```

Параметры

<PROCESS-NAME> – имя процесса события, которое необходимо или не нужно сохранять в локальный syslog-файл или отправлять на удаленный syslog-сервер. Принимает значения:

- aaa-mgr
- alarm-mgr
- avahi
- cfgsync-mgr
- cli
- cp-mgr
- device-mgr
- dhcp-client
- dhcp-proxy
- dhcp-server
- dns
- e1d
- env-mgr
- wlc-30fs

- file-mgr
- firewall-failover
- firewalld
- haveged
- if-mgr
- if-mgr-ng
- ipc-hub
- ipc-mgr
- ips
- ips-storage-mgr
- ipsec
- key-safed
- l2tpclient
- lb
- lic-mgr
- lldpd
- modem-cfgmgr
- modem-mgr
- multiwan
- nhrp
- ntp
- oi-mgr
- openvpn
- pppoe
- pptp
- prober
- rexd
- routing
- service-mgr
- session-mgr
- sflowd
- sla-mgr
- snmp-server
- ssh-server
- switch
- syslog-mgr
- systemdb
- telnet-server
- vrrp
- zabbix-agent
- zabbix-proxy
- others

all – ключ для удаление всех ранее сконфигурированных процессов.

Значение по умолчанию

Сохраняются/отправляются события всех процессов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SYSLOG-FILE

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-file)# match not process-name dhcp-client
```

ntp logging

Данной командой включается запись в локальный syslog-сервер сообщений о работе с NTP-пирами.

Использование отрицательной формы команды (no) выключает логирование сообщений о работе с NTP-пирами.

Синтаксис

```
[no] ntp logging
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ntp logging
```

port

Данной командой указывается номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port <PORT>
no port
```

Параметры

<PORT> – номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями.

Значение по умолчанию

514

Необходимый уровень привилегий

10

Командный режим

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-host)# port 5014
```

remote-address

Данной командой указывается IPv4/IPv6-адрес удаленного syslog-сервера.

Использование отрицательной формы команды (no) удаляет IPv4/IPv6-адрес удаленного syslog-сервера.

Синтаксис

```
remote-address { <ADDR> | <IPV6-ADDR> }
no remote-address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-host)# remote-address 192.168.0.100
```

severity

Данной командой указывается уровень важности сообщений, которые будут сохраняться в локальный syslog-файл или отправляться на удаленный syslog-сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
severity <SEVERITY>
no severity
```

Параметры

<SEVERITY> – уровень важности сообщения, возможные значения приведены в разделе syslog console.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SYSLOG-FILE

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-file)# severity info
```

source-address

Данной командой указывается IPv4/IPv6-адрес контроллера, от которого будут отправляться пакеты на удаленный syslog-сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
source-address { <ADDR> | <IPV6-ADDR> }
no source-address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Значение по умолчанию

IPv4/IPv6-адрес интерфейса, с которого отправляется пакеты на удаленный syslog-сервер.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-host)# source-address 192.168.54.157
```

show syslog

Команда для просмотра текущей информации о конфигурации syslog-журнала, списка созданных log-файлов, а также для просмотра log-файлов с возможностью фильтрации с помощью регулярных выражений.

Синтаксис

```
show syslog <FILE> [ from-date <YEAR> <MONTH> <DAY> ] [ from-time <TIME> ] [ to-date
<YEAR> <MONTH> <DAY> ]
[ to-time <TIME> ] [ from-end ]
```

Параметры

<FILE> – имя файла, задаётся строкой до 31 символа;

from-date – для вывода информации начиная с указываемой даты;

from-time – для вывода информации начиная с указываемого времени;

to-date – для вывода информации до указываемой даты;

to-time – для вывода информации до указываемого времени;

<YEAR> – год, принимает значения [2001..2037];

<MONTH> – месяц, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December];

<DAY> – день месяца, принимает значения [1..31];

<TIME> – устанавливаемое системное время, задаётся в виде HH MM SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0 .. 59];
- SS – секунды, принимает значение [0 .. 59].

from-end – просмотр содержимого файла с конца, так как последние записи помещаются в конец файла.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# show syslog
   Log files
   ~~~~~~~~~
##     Name                    Size in bytes      Date of last modification
----   --------------------    ----------------   -------------------------
1      debug                   371681             Thu Jan  1 16:17:04 1970
2      debug.1                 524222             Thu Jan  1 01:48:13 1970
3      wlc-30                     97259              Thu Jan  1 16:17:01 1970
----   --------------------    ----------------   -------------------------
Total files: 4
wlc-30# show syslog configuration
SYSLOG
File size: 512 (kiB)
Number of logs: 3
Console: info
   Files:
   ~~~~~~
ID   Name                                Severity
--   ---------------------------------   ----------
0    wlc-30                                 info
```

show syslog configuration

Команда для просмотра текущей информации о конфигурации syslog-журнала.

Синтаксис

`show syslog configuration`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# show syslog configuration

SYSLOG

File size: 500 (kiB)
Number of logs: 1
Console: info
Monitor: info
```

syslog cli-commands

Данной командой включается процесс логирования введённых команд пользователя на локальный syslog-сервер.

Использование отрицательной формы команды (no) выключает логирование команд.

Синтаксис

```
[no] syslog cli-commands
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog cli-commands
```

syslog console

Данной командой устанавливаются уровни syslog-сообщений, которые будут отображаться в консоли. Отображаются сообщения, имеющие уровень важности, заданный в команде или более высокий.

Использование отрицательной формы команды (no) устанавливает уровень отображаемых сообщений по умолчанию.

Синтаксис

```
syslog console <SEVERITY>
```

```
no syslog console
```

Параметры

<SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности):

- emerg – в системе произошла критическая ошибка, система неработоспособна;
- alert – сигналы тревоги, необходимо немедленное вмешательство персонала;
- crit – критическое состояние системы, сообщение о событии;
- error – сообщения об ошибках;
- warning – предупреждения, неаварийные сообщения;
- notice – сообщения о важных системных событиях;
- info – информационные сообщения системы;
- debug – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы;
- none – отключает вывод syslog-сообщений в консоль.

Значение по умолчанию

info

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog console info
```

syslog file

Данной командой включается сохранение сообщений syslog в указанный файл и происходит переход в режим конфигурирования параметров данного syslog-файла.

Использование отрицательной формы команды (no) отключает сохранение сообщений syslog в указанный файл.

Синтаксис

```
syslog file { flash:syslog/<NAME> | tmpsys:syslog/<NAME> }
```

```
no syslog file { flash:syslog/<NAME> | tmpsys:syslog/<NAME> | all}
```

Параметры

flash – файл располагается в энергонезависимой памяти устройства;

tmpsys – файл располагается в энергозависимой памяти устройства;

<NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут отключено сохранение во все сконфигурированные syslog-файлы.

Размер файловой системы tmpsys составляет 100 МБ.
Настраивая число файлов в ротации и размер файла, необходимо следить за тем, чтобы суммарный размер файлов не превышал эти ограничения.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog file wlc-30 info
```

syslog file-size

Командой устанавливается максимальный размер файла журнала. По превышении указанного размера будет автоматически производиться ротация файлов.

Использование отрицательной формы команды (no) устанавливает значение размера файла журнала в значение по умолчанию.

Синтаксис

```
syslog file-size <SIZE>
no syslog file-size
```

Параметры

<SIZE> – размер файла, принимает значение [10..10000000] Кбайт.

Значение по умолчанию

500 Кбайт

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog file-size 10000
```

syslog host

Данной командой включается передача сообщений syslog на удаленный syslog-сервер и происходит переход в режим конфигурирования параметров данного syslog-сервера.

Использование отрицательной формы команды (no) отключает передачу сообщений syslog на удаленный syslog-сервер.

Синтаксис

```
syslog host <HOSTNAME>
no syslog host { <HOSTNAME> | all }
```

Параметры

<HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде **no syslog host all** для удаления всех syslog-серверов;

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog host eltex 192.168.2.2
```

syslog max-files

Данная команда устанавливает максимальное количество файлов, сохраняемых при ротации.

Использование отрицательной формы команды (no) устанавливает количество хранимых файлов журнала в значение по умолчанию.

Синтаксис

```
syslog max-files <NUM>
no syslog max-files
```

Параметры

<NUM> – максимальное количество файлов, принимает значения [1 .. 1000].

Значение по умолчанию

15

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog max-files 100
```

syslog monitor

Данной командой устанавливается уровень syslog-сообщений, которые будут отображаться при удаленных подключениях (Telnet, SSH). Отображаются сообщения, имеющие уровень важности, заданный в команде или более высокий.

Использование отрицательной формы команды (no) устанавливает уровень отображаемых сообщений по умолчанию.

Синтаксис

```
syslog monitor <SEVERITY>
no syslog monitor
```

Параметры

<SEVERITY> – уровень важности сообщения, возможные значения приведены в разделе syslog console.

Значение по умолчанию

info

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog monitor info
```

syslog reload debugging

Данной командой включается режим debugging в процессе перезагрузки для локального syslog-сервера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] syslog reload debugging
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog reload debugging
```

syslog sequence-numbers

Данной командой включается добавление порядкового номера к записям в локальный syslog-сервер. Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] syslog sequence-numbers
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog sequence-numbers
```

syslog snmp

Данной командой устанавливается уровень syslog-сообщений, которые будут отправляться на snmp-сервер в виде snmp-trap. Отправляются сообщения, имеющие уровень важности, заданный в команде или более высокий.

Использование отрицательной формы команды (no) устанавливает уровень отображаемых сообщений по умолчанию.

Синтаксис

```
syslog snmp <SEVERITY>
```

```
no syslog snmp
```

Параметры

<SEVERITY> – уровень важности сообщения, возможные значения приведены в разделе syslog console.

Значение по умолчанию

info

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog snmp info
```

syslog sip-level

Данной командой устанавливается уровень логирования sip-событий.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] syslog sip-level <LEVEL>
```

Параметры

<LEVEL> – уровень sip-сообщений, который будут попадать в syslog. Принимает значение в диапазоне [0..9].

Значение по умолчанию

0

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# syslog sip-level 8
```

transport

Данной командой указывается транспортный протокол для передачи пакетов на удаленный syslog-сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
transport { tcp | udp }
no transport
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

udp

Необходимый уровень привилегий

10

Командный режим

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-host)# transport tcp
```

vrf

Данной командой указывается имя экземпляра VRF, в рамках которого будут отправляться пакеты на удаленный syslog-сервер.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
vrf <VRF>
no vrf
```

Параметры

<VRF> – имя экземпляра VRF, в котором доступен удаленный syslog-сервер, задается строкой до 31 символа.

Значение по умолчанию:

Отсутствует (глобальная таблица маршрутизации).

Необходимый уровень привилегий

10

Командный режим

CONFIG-SYSLOG-HOST

Пример

```
wlc-30(config-syslog-host)# vrf MGMT
```

Настройка доступа SSH, Telnet

- ip ftp client password
- ip ftp client username
- ip sftp client password
- ip sftp client username
- ip ssh authentication algorithm disable
- ip ssh authentication retries
- ip ssh authentication timeout
- ip ssh client password
- ip ssh client source-ip
- ip ssh client username
- ip ssh dscp
- ip ssh encryption algorithm disable
- ip ssh key-exchange algorithm disable
- ip ssh key-exchange time
- ip ssh key-exchange volume
- ip ssh port
- ip ssh server
- ip telnet dscp
- ip telnet port
- ip telnet server
- show crypto key mypubkey
- update ssh-host-key

ip ftp client password

Данной командой определяется пароль по умолчанию для операций копирования по протоколу FTP.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
ip ftp client password { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
[no] ftp client password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [1 .. 16] символов, принимает значения [0-9a-fA-F];

<ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [2..32] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ftp client password test
```

ip ftp client username

Данной командой определяется имя пользователя по умолчанию для операций копирования по протоколу FTP.

Использование отрицательной формы команды (no) удаляет имя пользователя.

Синтаксис

```
ip ftp client username <NAME>
no ftp client username
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ftp client username test
```

ip sftp client password

Данная команда задает значения пароля пользователя для клиента протокола SFTP.

Использование отрицательной формы команды (no) удаляет значения пароля пользователя для клиента протокола SFTP.

Синтаксис

```
ip sftp client password { <TEXT> | encrypted < ENCRYPTED-TEXT > }
no ip sftp client password
```

Параметры

<TEXT> – строка [1..16] ASCII-символов;

<ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32].

Значение по умолчанию

Имя пользователя не задано.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sftp client password 123456789
```

ip sftp client username

Данная команда задает значения имени пользователя для клиента протокола SFTP.

Использование отрицательной формы команды (no) удаляет значения имени пользователя для клиента протокола SFTP.

Синтаксис

```
ip sftp client username <USERNAME>
no ip sftp client username
```

Параметры

<USERNAME> – имя пользователя, задаётся строкой до 31 символа.

Значение по умолчанию

Имя пользователя не задано.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sftp client username wlc-30user
```

ip ssh authentication algorithm disable

Данная команда запрещает использование определенного алгоритма аутентификации для SSH-сервера.

Использование отрицательной формы команды (no) разрешает использование определенного алгоритма аутентификации для SSH-сервера.

Синтаксис

```
[no] ip ssh authentication algorithm <ALGORITHM> disable
```

Параметры

<ALGORITHM> – алгоритм хеширования, принимает значения [md5, md5-96, sha1, sha1-96, sha2-256, sha2-512, ripemd160].

Необходимый уровень привилегий

15

Значение по умолчанию

Разрешены все алгоритмы аутентификации.

Командный режим

CONFIG

Пример

```
wlc-30(config)# no ip ssh authentication algorithm md5 disable
```

ip ssh authentication retries

Данная команда устанавливает количество попыток аутентификации для SSH-сервера.

Использование отрицательной формы команды (no) устанавливает количество попыток аутентификации для SSH-сервера по умолчанию.

Синтаксис

```
ip ssh authentication retries <NUM>
no ip ssh authentication retries
```

Параметры

<NUM> – количество попыток аутентификации для SSH-сервера [1..10].

Необходимый уровень привилегий

10

Значение по умолчанию

6

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh authentication retries 5
```

ip ssh authentication timeout

Данная команда устанавливает период времени ожидания аутентификации для SSH-сервера.

Использование отрицательной формы команды (no) устанавливает период времени ожидания аутентификации для SSH-сервера по умолчанию.

Синтаксис

```
ip ssh authentication timeout <SEC>
no ip ssh authentication timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [30..360].

Необходимый уровень привилегий

10

Значение по умолчанию

120

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh authentication timeout 60
```

ip ssh client password

Данной командой определяется пароль по умолчанию для операций копирования по протоколу SCP.

Использование отрицательной формы команды (no) удаляет пароль.

Синтаксис

```
ip ssh client password { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no ssh client password
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой [1 .. 16] символов, принимает значения [0-9a-fA-F];

<ENCRYPTED-TEXT > – зашифрованный пароль, задаётся строкой [2..32] символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh client password test132
```

ip ssh client source-ip

Данной командой определяется IP-адрес контроллера, от которого будут устанавливаться SSH-сессии на другие устройства.

Использование отрицательной формы команды (no) удаляет имя пользователя.

Синтаксис

```
ip ssh client source-ip <ADDR>
no ssh client source-ip
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Указываемый IP-адрес должен быть назначен на каком-либо интерфейсе/туннеле контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh client source-ipt 192.168.22.78
```

ip ssh client username

Данной командой определяется имя пользователя по умолчанию для операций копирования по протоколу SCP.

Использование отрицательной формы команды (no) удаляет имя пользователя.

Синтаксис

```
ip ssh client username <NAME>
no ssh client username
```

Параметры

<NAME> – имя пользователя, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh client username tester
```

ip ssh dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов SSH-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ip ssh dscp <DSCP>
no ip ssh dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

32

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh dscp 40
```

ip ssh encryption algorithm disable

Данная команда запрещает использование определенного алгоритма шифрования для SSH-сервера.

Использование отрицательной формы команды (no) разрешает использование определенного алгоритма шифрования для SSH-сервера.

Синтаксис

```
[no] ip ssh encryption algorithm <ALGORITHM> disable
```

Параметры

<ALGORITHM> – идентификатор алгоритма шифрования, принимает значения [aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, arcfour, arcfour128, arcfour256, blowfish, cast128, 3des].

Необходимый уровень привилегий

15

Значение по умолчанию

Все алгоритмы разрешены.

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh encryption algorithm aes128 disable
```

ip ssh key-exchange algorithm disable

Данная команда запрещает использование определенного алгоритма обмена ключами для SSH-сервера.

Использование отрицательной формы команды (no) разрешает использование определенного алгоритма обмена ключами для SSH-сервера.

Синтаксис

```
[no] ip ssh key-exchange algorithm <ALGORITHM> disable
```

Параметры

<ALGORITHM> – идентификатор протокола обмена ключами, принимает значения [dh-group1-sha1, dh-group14-sha1, dh-group-exchange-sha1, dh-group-exchange-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521].

Необходимый уровень привилегий

15

Значение по умолчанию

Все алгоритмы разрешены.

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
```

ip ssh key-exchange time

Данная команда устанавливает период времени смены ключей аутентификации для SSH-сервера.

Использование отрицательной формы команды (no) устанавливает период времени смены ключей аутентификации для SSH-сервера по умолчанию.

Синтаксис

```
ip ssh key-exchange time <SEC>
no ip ssh key-exchange time
```

Параметры

<SEC> – период времени в часах, принимает значения [1..72].

Необходимый уровень привилегий

15

Значение по умолчанию

1

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh key-exchange time 24
```

ip ssh key-exchange volume

Данная команда устанавливает объем данных, после прохождения которого произойдет обновление ключей аутентификации для SSH-сервера.

Использование отрицательной формы команды (no) устанавливает объем данных, после прохождения которого произойдет обновление ключей аутентификации для SSH-сервера по умолчанию.

Синтаксис

```
ip ssh key-exchange volume <DATA>
no ip ssh key-exchange volume
```

Параметры

<DATA> – объем данных в мегабайтах, принимает значения [1..4096].

Необходимый уровень привилегий

15

Значение по умолчанию

1000

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh key-exchange volume 512
```

ip ssh port

Данной командой определяется порт SSH-сервера на контроллере.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip ssh port <PORT>`

`no ip ssh port`

Параметры

<PORT> – номер порта, указывается в диапазоне [1..65535].

Значение по умолчанию

22

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip ssh port 3001
```

ip ssh server

Данной командой включается SSH-сервер на контроллере.

Использование отрицательной формы команды (no) отключает SSH-сервер.

Синтаксис

```
[no] ip ssh server [ vrf <VRF>]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать SSH-сервер.

Значение по умолчанию

SSH-сервер выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# no ip ssh server
```

ip telnet dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов Telnet-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ip telnet dscp <DSCP>
no ip telnet dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

32

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip telnet dscp 40
```

ip telnet port

Данной командой определяется порт Telnet-сервера на контроллере.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip telnet port <PORT>`

`no ip telnet port`

Параметры

<PORT> – номер порта, принимает значения [1..65535].

Значение по умолчанию

23

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip telnet port 2001
```

ip telnet server

Данной командой включается Telnet-сервер на контроллере.

Использование отрицательной формы команды (no) отключает Telnet-сервер.

Синтаксис

`[no] ip telnet server [vrf <VRF>]`

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать Telnet-сервер.

Значение по умолчанию

Telnet-сервер выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# no ip telnet server
```

show crypto key mypubkey

Команда используется для просмотра открытых ключей устройства, используемых при установлении соединения по протоколу SSH.

Синтаксис

```
show crypto key mypubkey <OPTIONS>
```

Параметры

<OPTIONS> – алгоритм генерации нового криптографического ключа:

- dsa – алгоритм DSA;
- ecdsa – алгоритм ECDSA;
- ed25519 – алгоритм ED25519;
- rsa – алгоритм RSA;
- rsa1 – алгоритм RSA1.

Необходимый уровень привилегий

15

Командный режим

ROOT

Пример

```
wlc-30# show crypto key mypubkey rsa
Key data
-----------------------------------------------------------
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDz750sWCQrnNufg1yhuksTFYCYdEfg
JZ9tWUvcssAZhCJWMewprXBuZMABzFmfBg157pgapxn2qJXJ8ESMV7X7gPfy
xQQah6l376z3SFcpKvwudNgwHiS5HCYPRQWx2Xdaz/nJtYr5NpYgLPba68NC
iXcqEp7EPR5GojDVxpuDuk0hPFcihzmt5Yx8ZptJRzRtsuDQYlowv0Qa24kd
OlQ90/1qKfbAhB6XI60l+dK5VEj7giBESarcRn69/e/YVbdGBdTE93QWFPKI
bm63imfbxRwWtcwsFdIHi8Blv9ZqDqqF/IO3TkIKa31hV9GnsawlAXi/IdyY
bYPboHRdcTlH/ root@wlc-30-1000
```

update ssh-host-key

Данной командой генерируется пара новых криптографических ключей для установления соединения по протоколу SSH.

Синтаксис

```
update ssh-host-key { dsa | escda <ESCDA> | ed25519 <ED25519> | rsa <RSA> }
```

Параметры

dsa – алгоритм DSA;

ecdsa – алгоритм ECDSA:

- <ECDSA> – размер ключа, принимает значение 256, 384 или 521;
- Без указания, используется размер ключа 521.

ed25519 – алгоритм ED25519:

- <ED25519> – размер ключа, принимает значение [256..2048];
- Без указания, используется размер ключа 2048.

rsa – алгоритм RSA с указанием длины ключа:

- <RSA> – размер ключа, принимает значение [1024..2048];
- Без указания, используется размер ключа 2048.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# update ssh-host-key ecdsa
```

Настройка протокола LLDP

- lldp enable
- lldp hold-multiplier
- lldp management-address
- lldp med fast-start enable
- lldp med fast-start tx-interval
- lldp receive
- lldp system-description
- lldp system-name
- lldp timer
- lldp transmit
- show lldp neighbors
- show lldp statistics

lldp enable

Данной командой на контроллере включается поддержка протокола LLDP.

Использование отрицательной формы команды (no) отключает поддержку протокола LLDP.

Синтаксис

```
[no] lldp enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp enable
```

lldp hold-multiplier

Данной командой устанавливается количество периодов lldp-timer, в течении которых контроллер хранит информацию, полученную по протоколу LLDP.

Использование отрицательной формы команды (no) устанавливает соответствующий параметр в значение по умолчанию.

Синтаксис

```
lldp hold-multiplier <SEC>
no lldp hold-multiplier
```

Параметры

<SEC> – период времени в секундах, принимает значение [1..10].

Значение по умолчанию

4

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp hold-multiplier 5
```

lldp management-address

Данной командой устанавливается IP-адрес, который будет передаваться в LLDP TLV в качестве management-address.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию для поля LLDP TLV management-address.

Синтаксис

```
lldp management-address <ADDR>
no lldp management-address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Указываемый IP-адрес должен быть назначен на каком-либо интерфейсе/туннеле контроллера.

Значение по умолчанию

Один из существующих.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp management-address 192.168.54.42
```

lldp med fast-start enable

Данной командой включается рассылка LLDP-MED сообщений на интерфейсах с настроенной сетевой политикой (см. раздел lldp network-policy).

Использование отрицательной формы команды (no) выключает рассылку LLDP-MED сообщений на интерфейсах с настроенной сетевой политикой.

Синтаксис

```
[no] lldp med fast-start enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Рассылка LLDP-MED сообщений отключена.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp med fast-start enable
```

lldp med fast-start tx-interval

Данной командой настраивается период рассылки LLDP-MED сообщений на интерфейсах с настроенной сетевой политикой (см. раздел lldp network-policy).

Использование отрицательной формы команды (no) устанавливается значение по умолчанию периода рассылки LLDP-MED сообщений на интерфейсах с настроенной сетевой политикой.

Синтаксис

```
lldp med fast-start tx-interval <SEC>
[no] lldp med fast-start tx-interval
```

Параметры

<SEC> – период времени, принимает значения [1.. 32768] секунд.

Значение по умолчанию

1 секунда

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp med fast-start tx-interval 20
```

lldp receive

Данной командой включается обработка LLDPDU на физическом интерфейсе.

Использование отрицательной формы команды (no) отключает обработку LLDPDU на физическом интерфейсе.

Синтаксис

```
[no] lldp receive
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Прием LLDP-пакетов выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример

```
wlc-30(config-if-gi)# lldp receive
```

lldp system-description

Данной командой устанавливается поле, который будет передаваться в LLDP TLV в качестве system-description.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию для поля LLDP TLV system-description.

Синтаксис

```
lldp system-description <DESCRIPTION>
no lldp system-description
```

Параметры

<DESCRIPTION> – идентификатор описания системы, задаётся строкой до 255 символа.

Значение по умолчанию

Содержит информацию о модели и версии ПО контроллера.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp system-description wlc-30-1000-1.3.0
```

lldp system-name

Данной командой устанавливается поле, который будет передаваться в LLDP TLV в качестве system-name.

Использование отрицательной формы команды (no).

Синтаксис

```
lldp system-name <NAME>
no lldp system-name
```

Параметры

<NAME> – идентификатор имени системы, задаётся строкой до 255 символа.

Значение по умолчанию

Совпадает с заданным hostname.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp system-name wlc-30-100-branch-12
```

lldp timer

Данной командой устанавливается период отправки LLDPDU.

Использование отрицательной формы команды (no) устанавливает период отправки LLDPDU по умолчанию.

Синтаксис

`lldp timer <SEC>`

`no lldp timer`

Параметры

<SEC> – период времени в секундах, принимает значение [1..32768].

Значение по умолчанию

30

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# lldp timer 3
```

lldp transmit

Данной командой включается отправка LLDPDU на физическом интерфейсе.

Использование отрицательной формы команды (no), отправка LLDPDU на физическом интерфейсе отключается.

Синтаксис

```
[no] lldp transmit
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отправка LLDP-пакетов выключен.

Необходимый уровень привилегий

15

Командный режим

CONFI-IF-GI

CONFI-IF-TE

Пример

```
wlc-30(config-if-gi)# lldp transmit
```

show lldp neighbors

Данной командой выводится информация о подключенных устройствах, от которых получена информация по протоколу LLDP.

Синтаксис

```
show lldp neighbors <IF>
```

Параметры

<IF> – наименование физического интерфейса или группы физических интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.
Допустимо использовать только физические интерфейсы (gigabitethernet или tengigabitethernet). Без указания интерфейса выводится информация о всех обнаруженных по LLDP устройствах.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# show lldp neighbors
LLDP Neighbor Information:

Local Information:
    Index:              0
    Local Interface:    gi1/0/4

Neighbour Information:
    Chassis type:       mac
    Chassis ID:         a8:f9:4b:aa:8c:90
    Management ip:      192.168.1.5
    Management ip:      fe80::2052:e5ff:fe36:226f
    Port type:          local
    Port ID:            gi1/0/8
    Port description:   wlc-30200-lldp-test
    Time to live:       120
    System name:        wlc-30-200-test
    System Description: Eltex Router wlc-30-200 1.3.0 build 79 (date 14/08/2017 time 10:19:13)

System capabilities:
    Bridge:             false
    Router:             true
    Station:            true
    Wlan:               false
```

show lldp statistics

Данной командой выводится статистика работы протокола LLDP на интерфейсах, на которых включен протокол LLDP.

Синтаксис

```
show lldp statistics <IF>
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера. Допустимо использовать только физические интерфейсы (gigabitethernet или tengigabitethernet). Без указания интерфейса выводится информация о всех обнаруженных по LLDP устройствах.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show lldp statistics
Interface  Transmitted  Received  Discarded  Unrecognized  Ageout  Inserted   Deleted
---------  -----------  --------  ---------  ------------   ------  --------   -------
 gi1/0/1         1           0          0            0           0        0         0
```

Настройка зеркалирования

- port monitor
- port monitor interface
- port monitor mode
- show interfaces switch-port monitor

port monitor

Данной командой включается режим зеркалирования трафика.

Использование отрицательной формы команды (no) отключается режим зеркалирования трафика.

Синтаксис

```
[no] port monitor
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример

```
wlc-30(config-if-gi)# port monitor interface gigabitethernet 1/0/5
```

port monitor interface

Данной командой определяются контролируемые порты.

Использование отрицательной формы команды (no) удаляет контролируемый порт.

Синтаксис

```
port monitor interface <IF> <DIRECTION>
no port monitor
```

Параметры

<IF> – физический интерфейс или группа физических интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<DIRECTION> – направление трафика:

- tx – зеркалирование только исходящего трафика;
- rx – зеркалирование только входящего трафика.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

Пример

```
wlc-30(config-if-gi)# port monitor interface gigabitethernet 1/0/5
```

port monitor mode

Данной командой определяется режим порта, передающего отзеркалированный трафик.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
port monitor mode <MODE>
no port monitor mode
```

Параметры

<MODE> – режим:

- network – совмещенный режим передачи данных и зеркалирование;
- monitor-only – только зеркалирование.

Значение по умолчанию

network

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# port monitor mode monitor-only
```

show interfaces switch-port monitor

Команда используется для просмотра настроек зеркалирования.

Синтаксис

```
show interfaces switch-port monitor
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces switch-port monitor
Port monitor mode:         network
RSPAN configuration RX:    VLAN 222
RSPAN configuration TX:    VLAN 222
Source Port    Destination Port   Type     RSPAN
------------   ----------------   ------   --------
gi1/0/7        gi1/0/6            RX,TX    Enabled
```

Настройка zabbix-agent и zabbix-proxy

- active-server
- config-retrieve
- database
- enable
- hostname
- port
- remote-commands
- server
- server
- show zabbix-agent configuration
- show zabbix-proxy configuration
- source-address
- timeout
- zabbix-agent
- zabbix-proxy

active-server

Данной командой задается адрес и порт Zabbix-сервера для активных проверок.

Использование отрицательной формы команды (no) удаляет сервер для активных проверок.

Синтаксис

```
active-server <ADDR> [ port <PORT> ]
no active-server
```

Параметры

<ADDR> – IP-адрес сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – номер порта, указывается в диапазоне [1..65535].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

Пример

```
wlc-30(config-zabbix-agent)# active-server 192.168.16.54
```

config-retrieve

Данной командой задаётся интервал обновления данных конфигурации от сервера.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию.

Синтаксис

```
config-retrieve <SEC>
no config-retrieve
```

Параметры

<SEC> – период времени в секундах, принимает значения [1..604800].

Значение по умолчанию

3600

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-proxy)# config-retrieve 200
```

database

Данной командой устанавливается место хранения базы данных zabbix-proxy.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
database <PATH>
no database
```

Параметры

<PATH> – место хранения базы данных zabbix-proxy.

Значение по умолчанию

По умолчанию база данных zabbix хранится в энергозависимой памяти контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-proxy)# database flash:data/zabbix.dat
```

enable

Данной командой активируется функционал Zabbix-агента.

Использование отрицательной формы команды (no) отключает функционал Zabbix-агента.

Синтаксис

```
[no] enable
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# enable
```

hostname

Данной командой задается имя агента. Hostname должен совпадать с именем хоста в панели управления Zabbix.

Использование отрицательной формы команды (no) устанавливает имя агента по умолчанию.

Синтаксис

```
hostname <NAME>
no hostname
```

Параметры

<NAME> – идентификатор имени системы, задаётся строкой до 63 символов.

Значение по умолчанию

Совпадает с настроенным hostname контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# hostname branch_12
```

port

Данной командой задается TCP-порт, который будет использоваться для обращений Zabbix-сервера к агенту.

Использование отрицательной формы команды (no) удаляет значение TCP-порта.

Синтаксис

```
port <PORT>
[no] port
```

Параметры

<PORT> – номер порта, указывается в диапазоне [1024..32767].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# port 20050
```

remote-commands

Данной командой активируем возможность выполнение команд на контроллере с Zabbix-сервера.

Использование отрицательной формы команды (no) отключает возможность выполнение команд на контроллере с Zabbix-сервера.

Синтаксис

```
[no] remote-commands
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# remote-commands
```

server

Данной командой задается IP-адрес Zabbix-сервера для zabbix-agent, с которого разрешено принимать входящие соединения.

Использование отрицательной формы команды (no) удаляет IP-адрес Zabbix-сервера.

Синтаксис

```
server <ADDR>
no server
```

Параметры

<ADDR> – IP-адрес сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

Пример

```
wlc-30(config-zabbix-agent)# server 192.168.18.54
```

server

Данной командой задается IP-адрес и порт Zabbix-сервера для zabbix-proxy, с которого разрешено принимать входящие соединения.

Использование отрицательной формы команды (no) удаляет конфигурацию Zabbix-сервера для zabbix-proxy.

Синтаксис

`server <ADDR> [port <PORT>]`

`no server`

Параметры

<ADDR> – IP-адрес сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<PORT> – номер UDP-порта, указывается в диапазоне [1024..32767].

Значение по умолчанию

<ADDR> – отсутствует;

<PORT> – 10051.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-proxy)# server 192.168.18.54 port 1285
```

show zabbix-agent configuration

Данной командой осуществляется вывод конфигурации Zabbix-агента.

Синтаксис

```
show zabbix-agent configuration
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show zabbix-agent configuration
VRF:                          --
State:                        Enabled
Active server:                --
Active server port:           --
Hostname:                     wlc-30
Port:                         --
Remote commands:              Disabled
Server:                       192.168.18.54
Source address:               --
Timeout:                      3
```

show zabbix-proxy configuration

Данной командой осуществляется вывод конфигурации Zabbix-proxy.

Синтаксис

show zabbix-proxy configuration

Параметры

Отсутствуют.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show zabbix-proxy configuration
VRF:                          --
State:                        Enabled
Hostname:                     wlc-30-10SLA
Port:                         --
Remote commands:              Enabled
Server:                       192.168.32.228
Server port:                  --
Source address:               --
Timeout:                      3
Configuration retrieve:       30
```

source-address

Данной командой указывается адрес с которого будет устанавливаться соединение с Zabbix-сервером.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`source-address <ADDR>`

`no source-address`

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

IP-адрес интерфейса, с которого отправляются пакеты на Zabbix-сервер.

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# source-address 192.168.1.57
```

timeout

Данной командой задается максимальное время на обработку запроса Zabbix-сервера.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
timeout
no timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [1..30].

Значение по умолчанию

3

Необходимый уровень привилегий

10

Командный режим

CONFIG-ZABBIX-AGENT

CONFIG-ZABBIX-PROXY

Пример

```
wlc-30(config-zabbix-agent)# timeout 20
```

zabbix-agent

Данной командой осуществляется переход в режим конфигурирования Zabbix-агента в глобальном режиме или VRF.

Использование отрицательной формы команды (no) удаляет настройки Zabbix-агента в глобальном режиме или VRF.

Синтаксис

```
[no] zabbix-agent [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.

Значение по умолчанию

Отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# zabbix-agent
```

zabbix-proxy

Данной командой осуществляется переход в режим конфигурирования Zabbix-proxy в глобальном режиме или VRF.

Использование отрицательной формы команды (no) удаляет настройки Zabbix-proxy в глобальном режиме или VRF.

Синтаксис

```
[no] zabbix-proxy [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа;

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# zabbix-proxy
```

30 Настройка DHCP

- Управление DHCP-клиентом
  - ip address dhcp
  - ip dhcp client ignore
  - ip dhcp client lease-time
  - ip dhcp client reboot
  - ip dhcp client retry
  - ip dhcp client select-timeout
  - ip dhcp client timeout
  - ip dhcp client vendor-class-id
  - ip dhcp server address
  - renew dhcp
- Управление IPv6 DHCP-клиентом
  - ipv6 address dhcp
  - ipv6 dhcp client ignore
  - ipv6 dhcp client lease-time
  - ipv6 dhcp client reboot
  - ipv6 dhcp client retry
  - ipv6 dhcp client select-timeout
  - ipv6 dhcp client timeout
  - ipv6 dhcp client vendor-class-id
  - ipv6 dhcp server address
  - renew ipv6 dhcp
- Управление DHCP Relay агентом
  - ip dhcp information option
  - ip dhcp information option action
  - ip dhcp information option format-type access-node-id
  - ip dhcp information option format-type circuit-id
  - ip dhcp information option format-type option
  - ip dhcp information option format-type remote-id
  - ip dhcp information option suboption-type
  - ip dhcp-relay
  - ip helper-address
  - ip helper-address vrrp-group
- Управление IPv6 DHCP Relay агентом
  - ipv6 dhcp-relay
  - ipv6 dhcp-relay interface
- Настройка и мониторинг DHCP-сервера
  - clear ip dhcp binding
  - address
  - address-range
  - default-lease-time
  - default-router
  - dns-server
  - domain-name
  - excluded-address-range
  - ip dhcp-server
  - ip dhcp-server dscp
  - ip dhcp-server pool
  - ip dhcp-server vendor-class-id
  - max-lease-time
  - netbios-name-server
  - network
  - option
  - show ip dhcp binding

    - show ip dhcp server dscp
    - show ip dhcp server pool
    - show ip dhcp server vendor-specific
    - suboption
    - tftp-server
    - vendor-specific
    - vendor-specific-options
- Настройка и мониторинг IPv6 DHCP-сервера
    - address
    - address-range
    - default-lease-time
    - dns-server
    - domain-name
    - excluded-address-range
    - ipv6 dhcp-server
    - ipv6 dhcp-server pool
    - ipv6 dhcp-server vendor-class-id
    - max-lease-time
    - network
    - option
    - show ipv6 dhcp binding
    - show ipv6 dhcp server pool
    - show ipv6 dhcp server vendor-specific

Управление DHCP-клиентом

ip address dhcp

Данной командой включается получение динамического IP-адреса конфигурируемого интерфейса по протоколу DHCP.

Использование отрицательной формы команды (no) выключает получение динамического IP-адреса по протоколу DHCP.

Синтаксис

```
[no] ip address dhcp
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip address dhcp
```

ip dhcp client ignore

Данной командой указываются DHCP-опции, которые будут игнорироваться клиентом.

Синтаксис

```
[no] ip dhcp client ignore <OPTION>
```

Параметры

<OPTION> – принимает следующие значения:

- dns-nameserver – DHCP-опция 23, список DNS-серверов;
- domain-name – DHCP-опция 24, имя домена;
- netbios-nameserver – DHCP-опция 44, список NetBios-серверов;
- router – DHCP-опция 3, список шлюзов по умолчанию;
- classless-static-route – DHCP-опция 121, список бесклассовых статических маршрутов;
- classful-static-route – DHCP-опция 33, список классовых статических маршрутов;
- tftp-server-address – DHCP-опция 66, имя TFTP-сервера (не применима для Bridge-интерфейсов);
- vendor-specific – DHCP-опция 17, информация определенная производителем.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client ignore router
```

ip dhcp client lease-time

Данной командой устанавливается запрашиваемое время аренды сетевого адреса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip dhcp client lease-time <TIME>
no ip dhcp client lease-time
```

Параметры

<TIME> – запрашиваемое время аренды, задаётся в виде DD:HH:MM, где:

- DD – дни, принимает значение [0..364];
- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0..59].

Значение по умолчанию

1 день

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client lease-time 00:12:00
```

ip dhcp client reboot

Данной командой задаётся время, в течение которого DHCP-клиент будет пытаться получить старый IP-адрес, перед тем как начать получать новый.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip dhcp client reboot <SEC>
no ip dhcp client reboot
```

Параметры

<SEC> – период времени в секундах, принимает значение [1..600].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client reboot 60
```

ip dhcp client retry

Данной командой задаётся интервал, через который DHCP-клиент возобновит попытки получить IP-адрес, если было установлено, что DHCP-сервер не отвечает.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip dhcp client retry <SEC>
no ip dhcp client retry
```

Параметры

<SEC> – период времени в секундах, принимает значение [1..600].

Значение по умолчанию

300

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client retry 180
```

ip dhcp client select-timeout

Данной командой задаётся период времени, в течение которого DHCP-клиент будет выбирать среди предложений по аренде от серверов, если такие существуют. Это используется в сетях с несколькими DHCP-серверами. Клиенту в ответ на запрос IP-адреса может быть отправлено несколько предложений. Возможно, что одно из этих предложений предпочтительнее другого (например, одно предложение может иметь адрес, который клиент использовал ранее).

Клиент ждет указанный период времени с момента отправки запроса на получение IP-адреса, на случай, если он получит несколько предложений от различных DHCP-серверов. По истечении указанного времени клиент принимает одно из предложений.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip dhcp client select-timeout <SEC>`

`no ip dhcp client select-timeout`

Параметры

<SEC> – период времени в секундах, принимает значение [0..600].

Значение по умолчанию

0 секунд – клиент примет первое полученное предложение.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client select-timeout 30
```

ip dhcp client timeout

Данной командой задаётся интервал, по истечении которого клиент считает, что DHCP-сервер недоступен. Если в базе данных IP-адресов клиента есть какие-либо арендованные адреса, срок аренды которых еще не истек, то клиент будет проверять последовательно каждый из них и, если найдет корректную, то IP-адрес из неё будет присвоен интерфейсу. Если нет действующих аренд в базе данных, то клиент будет повторно запрашивать IP-адрес по истечении интервала повтора (dhcp retry). Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ip dhcp client timeout <SEC>`

`no ip dhcp client timeout`

Параметры

<SEC> – период времени в секундах, принимает значения [1 .. 600].

Значение по умолчанию

60 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client timeout 300
```

ip dhcp client vendor-class-id

Данной командой устанавливается значение DHCP Опции 60 для получения дополнительных настроек по DHCP Опции 43.

Использование отрицательной формы команды (no) отключает запрос данной опции.

Синтаксис

```
ip dhcp client vendor-class-id <NAME>
no ip dhcp client vendor-class-id
```

Параметры

<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF
CONFIG-QINQ-IF
CONFIG-PORT-CHANNEL
CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp client vendor-class-id ELTEX
```

ip dhcp server address

Данной командой устанавливается IP-адрес DHCP-сервера, у которого будет запрашиваться IP-адрес.
Использование отрицательной формы команды (no) удаляет установленный IP-адрес DHCP-сервера.

Синтаксис

```
ip dhcp server address <ADDR>
no ip dhcp server address
```

Параметры

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI
CONFIG-IF-TE
CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp server address 10.10.10.1
```

renew dhcp

Данной командой отправляется запрос на обновление IP-адреса на по протоколу DHCP.

Синтаксис

```
renew dhcp <IF>
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# renew dhcp gigabitethernet 1/0/1
```

Управление IPv6 DHCP-клиентом

ipv6 address dhcp

Данной командой включается получение динамического IPv6-адреса конфигурируемого интерфейса по протоколу IPv6 DHCP.

Использование отрицательной формы команды (no) выключает получение динамического IPv6-адреса по протоколу IPv6 DHCP.

Синтаксис

```
[no] ipv6 address dhcp
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 address dhcp
```

ipv6 dhcp client ignore

Данной командой указываются DHCP-опции, которые будут игнорироваться клиентом.

Синтаксис

```
ipv6 dhcp client ignore <OPTION>
no ipv6 dhcp client ignore
```

Параметры

<OPTION> – принимает следующие значения:

- dns-nameserver – DHCP-опция 23, Список DNS-серверов;
- domain-name – DHCP-опция 24, Имя домена;
- vendor-specific – DHCP-опция 17, Информация, определенная производителем.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client ignore dns-nameserver
```

ipv6 dhcp client lease-time

Данной командой устанавливается запрашиваемое время аренды сетевого адреса.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 dhcp client lease-time <TIME>
no ipv6 dhcp client lease-time
```

Параметры

<TIME> – запрашиваемое время аренды, задаётся в виде DD:HH:MM, где:

- DD – дни, принимает значение [0..364];
- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0..59].

Значение по умолчанию

1 день

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client lease-time 00:12:00
```

ipv6 dhcp client reboot

Данной командой задаётся время, в течение которого IPv6 DHCP-клиент будет пытаться получить старый IPv6-адрес перед тем, как начать получать новый.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 dhcp client reboot <SEC>
no ipv6 dhcp client reboot
```

Параметры

<SEC> – период времени в секундах, принимает значение [1..600].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client reboot 60
```

ipv6 dhcp client retry

Данной командой задаётся интервал, через который IPv6 DHCP-клиент возобновит попытки получить IPv6-адрес, если было установлено, что IPv6 DHCP-сервер не отвечает.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ipv6 dhcp client retry <SEC>
no ipv6 dhcp client retry
```

Параметры

<SEC> – период времени в секундах, принимает значение [1..600].

Значение по умолчанию

300

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client retry 180
```

ipv6 dhcp client select-timeout

Данной командой задаётся период времени, в течение которого IPv6 DHCP-клиент будет выбирать среди предложений по аренде от серверов, если такие существуют. Это используется в сетях с несколькими IPv6 DHCP-серверами – в этом случае клиенту в ответ на запрос IPv6-адреса может быть отправлено несколько предложений. Возможно, что одно из этих предложений предпочтительнее другого (например, одно предложение может иметь адрес, который клиент использовал ранее).

Клиент ждет указанный период времени с момента отправки запроса на получение IP-адреса, на случай, если он получит несколько предложений от различных DHCPv6-серверов. По истечении указанного времени клиент принимает одно из предложений.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ipv6 dhcp client select-timeout <SEC>`

`no ipv6 dhcp client select-timeout`

Параметры

<SEC> – период времени в секундах, принимает значение [0..600].

Значение по умолчанию

0 – клиент примет первое предложенное предложение.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client select-timeout 30
```

ipv6 dhcp client timeout

Данной командой задаётся интервал, по истечении которого клиент считает, что IPv6 DHCP-сервер недоступен. Если в базе данных IPv6-адресов клиента есть какие-либо арендованные адреса, срок аренды которых ещё не истек, то клиент будет проверять последовательно каждый из них, и если найдет корректную, то IPv6-адрес из неё будет присвоен интерфейсу. Если нет действующих аренд в базе данных, то клиент будет повторно запрашивать IPv6-адрес по истечении интервала повтора (dhcp retry).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

`ipv6 dhcp client timeout <SEC>`

`no ipv6 dhcp client timeout`

Параметры

<SEC> – период времени в секундах, принимает значения [1..600].

Значение по умолчанию

60 секунд

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client timeout 300
```

ipv6 dhcp client vendor-class-id

Данной командой устанавливается значение DHCP Опции 60 для получения дополнительных настроек по DHCP Опции 43.

Использование отрицательной формы команды (no) отключает запрос данной опции.

Синтаксис

```
ipv6 dhcp client vendor-class-id <NAME>
no ipv6 dhcp client vendor-class-id
```

Параметры

<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp client vendor-class-id ELTEX
```

ipv6 dhcp server address

Данной командой устанавливается IPv6-адрес DHCP-сервера, у которого будет запрашиваться IPv6-адрес.

Использование отрицательной формы команды (no) удаляет установленный IPv6-адрес DHCP-сервера.

Синтаксис

```
ipv6 dhcp server address <IPV6-ADDR>
no ipv6 dhcp server address
```

Параметры

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp server address fc00::1
```

renew ipv6 dhcp

Данной командой отправляется запрос на обновление IPv6-адреса на по протоколу DHCP.

Синтаксис

```
renew ipv6 dhcp <IF>
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# renew ipv6 dhcp gigabitethernet 1/0/1
```

Управление DHCP Relay агентом

ip dhcp information option

Данной командой включается обработка опции 82 DHCP Relay агентом.

Использование отрицательной формы команды (no) отключает обработку опции 82 DHCP Relay агентом.

Синтаксис

```
[no] ip dhcp information option
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp information option
```

ip dhcp information option action

Данная команда позволяет изменить решение, которое будет принято контроллером при получении пакета с установленной опцией 82.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip dhcp information option action { replace | keep | drop }
no ip dhcp information option action
```

Параметры

- replace – заменить установленную опцию 82 новой;

- keep – оставить установленную опцию 82 без изменений;
- drop – удалить пакет, если в нем обнаружена установленная опция 82.

Значение по умолчанию

keep

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp information option action drop
```

ip dhcp information option format-type access-node-id

Данная команда позволяет задать Access-node-ID в поле Circuit ID опции 82 при использовании формата tr101.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ip dhcp information option format-type access-node-id <NODE-ID>
```

Параметры

<NODE-ID> – значение Access-node-ID, задаётся строкой до 31 символа.

Значение по умолчанию

Hostname устройства.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp information option format-type access-node-id R1
```

ip dhcp information option format-type circuit-id

Данная команда позволяет задать значение поля Circuit ID опции 82 при использовании любого формата.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ip dhcp information option format-type circuit-id <CIRCUIT-ID>
```

Параметры

<CIRCUIT-ID> – значение Circuit ID, задаётся строкой до 63 символов.

Значение по умолчанию

Определяется используемым форматом.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp information option format-type circuit-id gi1_0_1
```

ip dhcp information option format-type option

Данная команда позволяет задать формат идентификатора порта в поле Circuit ID опции 82 при использовании формата tr101.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ip dhcp information option format-type option <FORMAT> [ delimeter <DELIMITER> ]
```

Параметры

<FORMAT> – формат идентификатора порта, принимает одно из следующих значений:

- sp – строка содержащая номер слота и порта;
- sv – строка содержащая номер слота и VLAN;
- pv – строка содержащая номер порта и VLAN;
- spv – строка содержащая номер слота, порта и VLAN;
- bin – бинарный формат: VLAN(4 байта), слот(1 байт), порт(4 байта).

<DELIMITER> – разделитель между параметрами в строке, может принимать одно из следующих значений [. , ; # / space].

Значение по умолчанию

Формат – spv

Разделитель «:» для форматов: sp, sv, pv

Разделитель «/» и «:» для формата spv

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp information option format-type option spv delimeter #
```

ip dhcp information option format-type remote-id

Данная команда позволяет задать значение поля Remote ID опции 82 при использовании любого формата.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] ip dhcp information option format-type remote-id <REMOTE-ID>
```

Параметры

<REMOTE-ID> – значение Remote ID, задаётся строкой до 63 символов.

Значение по умолчанию

Определяется используемым форматом.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip dhcp information option format-type remote-id R1
```

ip dhcp information option suboption-type

Данной командой выбирается формат опции 82.

Использование отрицательной формы команды (no) устанавливает формат по умолчанию.

Синтаксис

```
[no] ip dhcp information option suboption-type { tr101 | custom }
```

Параметры

tr101 – формат рекомендованный TR-101 опции 82 согласно синтаксису, принятому в рекомендациях TR-101 (см. таблицу 10);

custom – формат опции 82 в соответствии с форматом, приведенном в таблице 11.

Таблица 10 – Формат полей опции 82 согласно рекомендациям TR-101

Поле	Передаваемая информация
Circuit ID	Access-Node-Id, по умолчанию hostname устройства (формат можно изменить командой «ip dhcp information option format-type access-node-id», описанной в разделе ip dhcp information option format-type access-node-id) Строка вида eth <stacked/slotid/interfaceid>:<vlan> (формат можно изменить командой «ip dhcp information option format-type option», описанной в разделе ip dhcp information option format-type option) Последний байт – номер порта, к которому подключено устройство, отправляющее dhcp-запрос.
Remote agent ID	Enterprise number – 0089c1 MAC-адрес устройства

Таблица 11 – Формат полей опции 82 режима custom

Поле	Передаваемая информация
Circuit ID	Длина (1 байт) Тип Circuit ID Длина (1 байт) VLAN (2 байта) Номер модуля (1 байт) Номер порта (4 байта)
Remote agent ID	Длина (1 байт) Тип Remote ID (1 байт) Длина (1 байт) MAC-адрес коммутатора

Значение по умолчанию

tr101

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp information option suboption-type custom
```

ip dhcp-relay

Данная команда включает агент DHCP-relay.

Использование отрицательной формы команды (no) отключает агент DHCP-relay.

Синтаксис

```
[no] ip dhcp-relay
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-relay
```

ip helper-address

Данной командой указывается IP-адрес DHCP-сервера, которому будут отправляться DHCP Discover пакеты, перехваченные DHCP Relay-агентом.

Использование отрицательной формы команды (no) удаляет IP-адрес из списка DHCP-серверов для DHCP Relay-агента.

Синтаксис

```
[no] ip helper-address <IP>
```

Параметры

<IP> – IP-адрес DHCP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 4 IP-адресов, список задаётся через запятую.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip helper-address 10.10.10.1
```

ip helper-address vrrp-group

Данной командой запрещается отправка DHCP Discover пакетов, перехваченные DHCP Relay-агентом, если VRRP-группа находится в состоянии DOWN.

Использование отрицательной формы команды (no) разрешает отправку DHCP Discover пакетов, перехваченные DHCP Relay-агентом, если VRRP-группа находится в состоянии DOWN.

Синтаксис

```
ip helper-address vrrp-group <GRID>
no ip helper-address vrrp-group
```

Параметры

<GRID> – идентификатор группы VRRP-контроллера, принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ip helper-address vrrp-group 7
```

Управление IPv6 DHCP Relay агентом

ipv6 dhcp-relay

Данная команда включает IPv6 DHCP-агент.

Использование отрицательной формы команды (no) выключает IPv6 DHCP-агент.

Синтаксис

```
[no] ipv6 dhcp-relay
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 dhcp-relay
```

ipv6 dhcp-relay interface

Данной командой указывается исходящий интерфейс и IPv6-адрес DHCP-сервера, которому будут отправляться DHCP Solicit-пакеты, перехваченные IPv6 DHCP Relay-агентом.

Использование отрицательной формы команды (no) удаляет исходящий интерфейс из списка интерфейсов для IPv6 DHCP Relay-агента.

Синтаксис

```
ipv6 dhcp-relay interface <IF> [ <IPV6-ADDR> ]
no ipv6 dhcp-relay interface <IF>
```

Параметры

<IF> – наименование интерфейса или группы интерфейсов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера.

<IPV6-ADDR> – IPv6-адрес DHCP-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Если адрес не задан, то пакеты отправляются на ff02::1:2. Все IPv6 DHCP-сервера и агенты в локальном сетевом сегменте.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

Пример

```
wlc-30(config-if-gi)# ipv6 dhcp-relay interface gigabitethernet 1/0/2 fc00::1
```

Настройка и мониторинг DHCP-сервера

clear ip dhcp binding

Данная команда позволяет очистить таблицу выданные DHCP-сервером IP-адресов.

Синтаксис

```
clear ip dhcp binding [ <ADDR> ] [vrf <VRF>]
```

Параметры

<ADDR> – IP-адрес, опциональный параметр, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если в команде задан параметр <ADDR>, то будет отображена информация связанная только с указанным адресом.

<VRF> – имя экземпляра VRF, по которому будет выводиться информация. Задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear ip dhcp binding
```

address

Данная команда позволяет добавить IP-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес.

Синтаксис

```
address <ADDR> { mac-address <MAC> | client-identifier <CLIENT-ID> }
no address <ADDR>
```

Параметры

<ADDR> – IP-адрес клиента, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если использовать команду для удаления, то при указании значения «all» будут удалены все IP-адреса;

<MAC> – MAC-адрес клиента, которому будет выдан IP-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];

<CLIENT-ID> – идентификатор клиента согласно DHCP option 61.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# address 192.168.3.21 mac-address A8:F9:4B:AA:00:40
```

address-range

Данная команда позволяет добавить диапазон IP-адресов к пулу адресов, конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный диапазон IP-адресов.

Синтаксис

```
address-range <FROM-ADDR>-<TO-ADDR>
no address-range { <FROM-ADDR>-<TO-ADDR> | all }
```

Параметры

<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую.

all – удалить все сконфигурированные диапазоны IP-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# address-range 192.168.3.1-192.168.3.20,192.168.3.24
```

default-lease-time

Данная команда позволяет задать время аренды, на которое клиенту будет выдан IP-адрес, если клиент не запрашивал определенное время аренды. Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
default-lease-time <TIME>
no default-lease-time
```

Параметры

<TIME> – время аренды IP-адреса, в формате DD:HH:MM, где:

- DD – количество дней, принимает значения [0..364];
- HH – количество часов, принимает значения [0..23];
- MM – количество минут, принимает значения [0..59].

Значение по умолчанию

12 часов

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# default-lease-time 00:04:00
```

default-router

Данная команда позволяет задать список IP-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP опцию 3.

Использование отрицательной формы команды (no) удаляет указанные адреса из списка шлюзов.

Синтаксис

```
default-router <ADDR>
no default-router { <ADDR> | all }
```

Параметры

<ADDR> – IP-адрес шлюза по умолчанию, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. Если использовать команду для удаления, то при указании значения «all» будут удалены все шлюзы по умолчанию.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# default-router 192.168.3.1,192.168.3.2
```

dns-server

Данная команда позволяет задать список IP-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опций.

Использование отрицательной формы команды удаляет указанный DNS-сервер из списка.

Синтаксис

```
dns-server <ADDR>
no dns-server { <ADDR> | all }
```

Параметры

<ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. Если использовать команду для удаления, то при указании значения «all» будут удалены все DNS-серверы.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# dns-server 8.8.8.8,8.8.4.4
```

domain-name

Данная команда позволяет задать DNS-имя сетевого домена. Имя домена передается клиентам в составе DHCP-опций 15.

Использование отрицательной формы команды (no) удаляет установленное имя домена.

Синтаксис

```
domain-name <NAME>
no domain-name
```

Параметры

<NAME> – DNS-имя домена клиента, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# domain-name eltex.loc
```

excluded-address-range

Данная команда позволяет исключить диапазон IP-адресов из пула адресов, конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный диапазон IP-адресов.

Синтаксис

```
[no] excluded-address-range <FROM-ADDR>-<TO-ADDR>
```

Параметры

<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# excluded-address-range 192.168.3.1-192.168.3.20,192.168.3.24
```

ip dhcp-server

Данная команда включает DHCP-сервер.

Использование отрицательной формы команды (no) выключает DHCP-сервер.

Синтаксис

```
[no] ip dhcp-server [vrf <VRF>]
```

Параметры

<VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задается строкой до 31 символа.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-server
```

ip dhcp-server dscp

Команда задаёт значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера.

Использование отрицательной формы команды (no) устанавливает значение DSCP по умолчанию.

Синтаксис

```
ip dhcp-server dscp <DSCP>
no ip dhcp-server dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Значение по умолчанию

61

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-server dscp 40
```

ip dhcp-server pool

Команда используется для создания пула IP-адресов DHCP-сервера и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный пул IP-адресов.

Синтаксис

```
ip dhcp-server pool <NAME> [vrf <VRF>]
no ip dhcp-server pool { <NAME> | all }
```

Параметры

<NAME> – имя пула IP-адресов DHCP-сервера, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все пулы IP-адресов. Если использовать команду для удаления, то при указании значения «all» будут удалены все IP-адреса;

<VRF> – имя экземпляра VRF, в рамках которого будет работать данный пул IP-адресов DHCP-сервера. Задается строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-server pool lan
```

ip dhcp-server vendor-class-id

Данная команда необходима для создания идентификатора класса поставщика (DHCP Опция 60) и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный идентификатор класса поставщика.

Синтаксис

```
[no] ip dhcp-server vendor-class-id <NAME>
```

Параметры

<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все идентификаторы класса поставщика.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip dhcp-server vendor-class-id ELTEX
```

max-lease-time

Данная команда позволяет задать максимальное время аренды IP-адресов. Если DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой. Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
max-lease-time <TIME>
no max-lease-time
```

Параметры

<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где:

- DD – количество дней, принимает значения [0..364];
- HH – количество часов, принимает значения [0..23];
- MM – количество минут, принимает значения [0..59].

Значение по умолчанию

1 день

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# max-lease-time 00:16:00
```

netbios-name-server

Данная команда позволяет сконфигурировать 44 опцию DHCP (задает IP-адрес NetBIOS-сервера).

Использование отрицательной формы команды (no) выключает передачу IP-адреса NetBIOS-сервера (44 опцию).

Синтаксис

```
[no] netbios-name-server <ADDR>
```

Параметры

<ADDR> – IP-адрес NetBIOS-сервера задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно задать до 4 IP-адресов. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все IP-адреса.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# netbios-name-server 192.168.45.15
```

network

Данная команда задает IP-адрес и маску для подсети, из которой будет выделен пул IP-адресов.

Использование отрицательной формы команды (no) удаляет настройки подсети в пуле.

Синтаксис

```
network <ADDR/LEN>
no network
```

Параметры

<ADDR/LEN> – IP-подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# network 192.168.3.0/24
```

option

Данная команда позволяет задать опции DHCP.

Использование отрицательной формы удаляет заданную опцию.

Синтаксис

```
option <CODE> { ip-address <ADDR> | ascii-text <STRING> | hex-bytes <HEX> }
no option { <CODE> | all }
```

Параметры

<CODE> – код опции DHCP, задается в форме числа [0..255];

<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 255 байт;

<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 15 IP-адресов, список задаётся через запятую;

<STRING> – текст, задаётся строкой от 1 до 255 символов;

all – удаляет все опции.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# option 43 ip-address 10.10.1.1
```

show ip dhcp binding

Данная команда позволяет посмотреть выданные DHCP-сервером IP-адреса.

Синтаксис

```
show ip dhcp binding [ <ADDR> ] [vrf <VRF>]
```

Параметры

<ADDR> – IP-адрес, опциональный параметр, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если в команде задан параметр <ADDR>, то будет отображена информация связанная только с указанным адресом;

<VRF> – имя экземпляра VRF, по которому будет выводиться информация. Задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip dhcp binding
Allocated          MAC address          Binding    Lease expires at
address                                 type
----------------   ------------------   --------   ----------------------------
192.168.1.3        50:46:5d:a5:3f:91    dynamic    Thursday 2014/01/01 12:42:12
```

show ip dhcp server dscp

Данная команда позволяет посмотреть значение DSCP для сообщений DHCP-сервера.

Синтаксис

```
show ip dhcp server dscp
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30 # show ip dhcp server dscp
DSCP:    32
```

show ip dhcp server pool

Данная команда позволяет посмотреть настроенные пулы IP-адресов. При указании имени выводится информация только для заданного пула.

Синтаксис

`show ip dhcp server pool [ <POOL_NAME> ]`

Параметры

<POOL_NAME> – имя пула, опциональный параметр.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip dhcp server pool lan-pool
name:               lan-pool
network:            192.168.1.0/24
address-ranges:     192.168.1.2-192.168.1.254
default-router:     192.168.1.1
max lease time:     1:0:0 (day:hour:min)
default lease time: 0:12:0 (day:hour:min)
```

show ip dhcp server vendor-specific

Данная команда позволяет посмотреть настроенные DHCP-опции 43 и 60.

Синтаксис

`show ip dhcp server vendor-specific`

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip dhcp server vendor-specific
Vendor ID          Vendor options
----------------   --------------------------------
 ELTEX             0x0b0931302e312e39302e32
```

suboption

Данная команда позволяет задать подопцию опции 43.

Использование отрицательной формы команды (no) удаляет заданную подопцию.

Синтаксис

```
suboption <CODE> {ascii-text <TEXT> | hex-bytes <HEX>}
no suboption <CODE> | all
```

Параметры

<CODE> – код подопции, задается в форме числа [0..255];

<STRING> – текст, задаётся строкой от 1 до 255 символов;

<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 255 байт;

all – удаляет все опции.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER-VENDOR-SPECIFIC

Пример

```
wlc-30(config-dhcp-server-vendor-specific)# suboption 15 ascii-text "http://192.168.1.1:8042"
```

tftp-server

Данная команда позволяет задать IP-адрес TFTP-сервера. Адрес передаётся клиентам в составе DHCP-опции 150.

Использование отрицательной формы команды (no) удаляет установленный IP-адрес TFTP-сервера.

Синтаксис

```
tftp-server <ADDR>
no tftp-server
```

Параметры

<ADDR> – IP-адрес TFTP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# tftp-server 192.168.0.1
```

vendor-specific

Данная команда позволяет задать специфическую информацию поставщика (DHCP Опция 43).

Использование отрицательной формы команды (no) удаляет специфическую информацию поставщика.

Синтаксис

```
vendor-specific
no vendor-specific
```

Параметры

Отсутствуют.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-SERVER

Пример

```
wlc-30(config-dhcp-server)# vendor-specific
wlc-30(config-dhcp-server-vendor-specific)#
```

vendor-specific-options

Данная команда позволяет задать специфическую информацию поставщика (DHCP Опция 43).

Использование отрицательной формы команды (no) удаляет специфическую информацию поставщика.

Синтаксис

```
vendor-specific-options <HEX>
no vendor-specific-options
```

Параметры

<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-DHCP-VENDOR-ID

Пример

```
wlc-30(config-dhcp-vendor-id)# vendor-specific-options 0b0931302e312e39302e320
```

Настройка и мониторинг IPv6 DHCP-сервера

address

Данная команда позволяет добавить IPv6-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный IPv6-адрес.

Синтаксис

```
address <IPV6-ADDR> mac-address <MAC>
no address <IPV6-ADDR>
```

Параметры

<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Если использовать команду для удаления, то при указании значения «all» будут удалены все IPv6-адреса;

<MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# address fc00::2 mac-address A8:F9:4B:AA:00:40
```

address-range

Данная команда позволяет добавить диапазон IPv6-адресов к пулу адресов конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный диапазон IPv6-адресов.

Синтаксис

```
[no] address-range <FROM-ADDR>-<TO-ADDR>
no address-range all
```

Параметры

<FROM-ADDR> – начальный IPv6-адрес диапазона, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Можно указать до 32 диапазонов IPv6-адресов, список задаётся через запятую.

all – удалить все сконфигурированные диапазоны IPv6-адресов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# address-range fc00::1-fc00:12,fc00::15-fc00::25
```

default-lease-time

Данная команда позволяет задать время аренды, на которое клиенту будет выдан IPv6-адрес, если клиент не запрашивал определенное время аренды.

Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
default-lease-time <TIME>
no default-lease-time
```

Параметры

<TIME> – время аренды IP-адреса, в формате DD:HH:MM, где:

- DD – количество дней, принимает значения [0..364];
- HH – количество часов, принимает значения [0..23];
- MM – количество минут, принимает значения [0..59].

Значение по умолчанию

12 часов

Необходимый уровень привилегий

1

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# default-lease-time 00:04:00
```

dns-server

Данная команда позволяет задать список IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опций.

Использование отрицательной формы команды удаляет указанный DNS-сервер из списка.

Синтаксис

```
dns-server <IPV6-ADDR>
no dns-server { <IPV6-ADDR> | all }
```

Параметры

<IPV6-ADDR> – IPv6-адрес DNS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов, список задаётся через запятую. Если использовать команду для удаления, то при указании значения «all» будут удалены все DNS-серверы.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# dns-server 8.8.8.8,8.8.4.4
```

domain-name

Данная команда позволяет задать имя сетевого домена. Имя домена передаётся клиентам в составе DHCP-опций.

Использование отрицательной формы команды (no) удаляет установленное имя домена.

Синтаксис

```
domain-name <NAME>
no domain-name
```

Параметры

<NAME> – имя домена клиента, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# domain-name eltex.loc
```

excluded-address-range

Данная команда позволяет исключить диапазон IPv6-адресов из пула адресов, конфигурируемого DHCP-сервера.

Использование отрицательной формы команды (no) удаляет указанный диапазон IPv6-адресов.

Синтаксис

```
[no] excluded-address-range <FROM-ADDR>-<TO-ADDR>
```

Параметры

<FROM-ADDR> – начальный IPv6-адрес диапазона, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];

<TO-ADDR> – конечный IPv6-адрес диапазона, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Можно указать до 32 диапазонов IPv6-адресов, список задаётся через запятую.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# excluded-address-range 10::1-10::9
```

ipv6 dhcp-server

Данная команда включает IPv6 DHCP-сервер.

Использование отрицательной формы команды (no) выключает IPv6 DHCP-сервер.

Синтаксис

```
[no] ipv6 dhcp-server [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать DHCP-сервер.

Значение по умолчанию

Выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 dhcp-server
```

ipv6 dhcp-server pool

Команда используется для создания пула IPv6-адресов DHCP-сервера и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный пул IPv6-адресов.

Синтаксис

```
[no] ipv6 dhcp-server pool <NAME> [vrf <VRF>]
```

Параметры

<NAME> – имя пула IPv6-адресов DHCP-сервера, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все пулы IPv6-адресов;

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать данный пул IP-адресов DHCP-сервера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 dhcp-server pool lan
```

ipv6 dhcp-server vendor-class-id

Данная команда необходима для создания идентификатора класса поставщика (DHCP Опция 60) и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный идентификатор класса поставщика.

Синтаксис

```
[no] ipv6 dhcp-server vendor-class-id <NAME>
```

Параметры

<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа. При выполнении отрицательной формы команды со значением параметра «all» будут удалены все идентификаторы класса поставщика.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ipv6 dhcp-server vendor-class-id ELTEX
```

max-lease-time

Данная команда позволяет задать максимальное время аренды IPv6-адресов. Если IPv6 DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой. Использование отрицательной формы команды устанавливает значение по умолчанию.

Синтаксис

```
max-lease-time <TIME>
no max-lease-time
```

Параметры

<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где:

- DD – количество дней, принимает значения [0..364];
- HH – количество часов, принимает значения [0..23];
- MM – количество минут, принимает значения [0..59].

Значение по умолчанию

1 день

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# max-lease-time 00:16:00
```

network

Данная команда задает IPv6-адрес и маску для подсети, из которой будет выделен пул IP-адресов.

Использование отрицательной формы команды (no) удаляет настройки подсети в пуле.

Синтаксис

```
network <IPV6-ADDR/LEN>
no network
```

Параметры

<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# network fc00::/110
```

option

Данная команда позволяет задать опции DHCP.

Использование отрицательной формы удаляет данную опцию.

Синтаксис

```
option <CODE> { ip-address <IPV6-ADDR> | ascii-text <STRING> | hex-bytes <HEX> }
no option { <CODE> | all }
```

Параметры

<CODE> – код опции DHCP, задается в форме числа [1..255];

<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 255 символов;

<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IP-адресов, список задаётся через запятую;

<STRING> – текст, задаётся строкой от 1 до 255 символов;

all – удаляет все опции.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IPV6-DHCP-SERVER

Пример

```
wlc-30(config-ipv6-dhcp-server)# option 43 ip-address fc00::/110
```

show ipv6 dhcp binding

Данная команда позволяет посмотреть выданные DHCP-сервером IPv6-адреса.

Синтаксис

```
show ipv6 dhcp binding [ <IPV6-ADDR> ]
```

Параметры

<IPV6-ADDR> – IPv6-адрес, опциональный параметр, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Если в команде задан параметр <IPV6-ADDR>, то будет отображена информация, связанная только с указанным адресом.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 dhcp binding
IPv6 address                                          Lease expires at
----------------------------------------------------  --------------------------
2001:db8:0:1::18                                      Tuesday 2015/06/09 23:39:45
```

show ipv6 dhcp server pool

Данная команда позволяет посмотреть настроенные пулы IPv6-адресов. При указании имени выводится информация только для заданного пула.

Синтаксис

```
show ipv6 dhcp server pool [ <POOL_NAME> ]
```

Параметры

<POOL_NAME> – имя пула, опциональный параметр, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 dhcp server pool lan-pool-ipv6
name:               lan-pool-ipv6
network:            fc00::/110
domain name:        example.com
address-ranges:     fc00::1-fc00::2
                           fc00::3
addresses:          --
dns-server:         fc00:2::3
max lease time:     001:00:00 (day:hour:min)
default lease time: 000:12:00 (day:hour:min)
```

show ipv6 dhcp server vendor-specific

Данная команда позволяет посмотреть настроенные DHCP-опции 43 и 60.

Синтаксис

```
show ipv6 dhcp server vendor-specific
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ipv6 dhcp server vendor-specific
Vendor ID          Vendor options
----------------   ---------------------------------
 ELTEX             0x0b0931302e312e39302e32
```

31 Настройка SLA

- Общие команды настройки SLA
  - enable
  - frequency
  - ip sla
  - ip sla logging
  - ip sla logging level
  - ip sla mode
  - ip sla responder cisco
  - ip sla responder cisco port
  - ip sla test
  - ip sla schedule
  - packet-size
  - show ip sla configuration
  - show ip sla test configuration
  - show ip sla test statistics
  - thresholds delay
  - thresholds jitter
  - thresholds losses
- Настройка Eltex-SLA
  - authentication algorithm
  - authentication key-chain
  - authentication key-string
  - control-phase authentication algorithm
  - control-phase authentication key-id
  - control-phase authentication key-string
  - control-phase destination-port
  - control-phase retry
  - control-phase source-port
  - control-phase timeout
  - dscp
  - history
  - icmp-echo
  - ip sla key-chain
  - ip sla responder
  - ip sla responder eltex
  - ip sla responder eltex port
  - timeout
  - timeout
  - ttl
  - udp-jitter
  - vrf
- Настройка SLA Weelink (система мониторинга качества услуг)
  - ip sla hostname
  - ip sla portal
  - ip sla responder udp ports
  - ip sla responder udp ports
  - udp-jitter

Общие команды настройки SLA

enable

Данной командой активируется SLA-тест.

Использование отрицательной формы команды (no) деактивирует SLA-тест.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Выключен

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# enable
```

frequency

Данной командой устанавливается время между запусками SLA-сессии.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
frequency <TIME>
no frequency
```

Параметры

<TIME> – время, определяется в секундах [1..604800].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# frequency 3600
```

ip sla

Данной командой включает функционал IP-SLA (SLA-agent).

Использование отрицательной формы команды (no) отключает функционал IP-SLA.

Синтаксис

```
[no] ip sla
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla
```

ip sla logging

Данной командой включается логирование событий SLA.

Использование отрицательной формы команды (no) отключает логирование SLA.

Синтаксис

```
[no] ip sla logging
```

Параметры

Команда не содержит параметров

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla logging
```

ip sla logging level

Данной командой устанавливается уровень важности сообщения для логирования событий IP-SLA.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`ip sla logging level <SEVERITY>`

`no ip sla logging level`

Параметры

<SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности):

- error – сообщения об ошибках;
- warning – предупреждения, неаварийные сообщения;
- notice – сообщения о важных системных событиях;
- information – информационные сообщения системы;
- debug – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы;
- trace – полная информация о всех событиях.

Значение по умолчанию

info

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla logging level warning
```

ip sla mode

Данной командой устанавливается режим работы SLA-agent.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ip sla mode <MODE>
no ip sla mode
```

Параметры

<MODE> – режим работы SLA-agent. Принимает значения:

- eltex – работа SLA-agent в режиме разработанном компанией ELTEX;
- wisla-local – работа SLA-agent в режиме разработанном компанией Wellink;
- wisla-remote – работа SLA-client в режиме разработанном компанией Wellink.

Значение по умолчанию

eltex

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla mode wisla
```

ip sla responder cisco

Данной командой на интерфейсе активируется функционал SLA-responder для Cisco-SLA-agent.

Использование отрицательной формы команды (no) на интерфейсе деактивируется функционал SLA-responder для Cisco-SLA-agent.

Синтаксис

```
[no] ip sla responder cisco
```

Параметры

Отсутствуют

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP

CONFIG-L2TP

CONFIG-PPTP

CONFIG-VTI

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ip sla responder cisco
```

ip sla responder cisco port

Данной командой устанавливается UDP-порт, на котором будет идти прослушивание запросов от Cisco-SLA-agent.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ip sla responder cisco port <PORT>
no ip sla responder cisco port
```

Параметры

<PORT> – номер UDP-порта, задается в диапазоне [1..65535].

Значение по умолчанию

Не ограничено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP

CONFIG-L2TP

CONFIG-PPTP

CONFIG-VTI

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ip sla responder cisco port 7777
```

ip sla test

Данная команда используется для создания SLA-теста (SLA-agent) и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный SLA-тест.

Синтаксис

```
[no] ip sla test <NUM>
```

Параметры

<NUM> – номер SLA-теста, задается в диапазоне [1..10000].

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla test 10
```

ip sla schedule

Данной командой устанавливается расписание работы SLA-тестов. Если SLA-тест создан и активирован, для него необходимо создать данное расписание.

Использование отрицательной формы команды (no) удаляет расписание работы SLA-тестов.

Синтаксис

```
ip sla schedule <TEST-NUMBER> [ life { <LIFE-TIME> | forever } ] [ start-time { <MONTH> <DAY> <TIME> | now } ]
```

```
[no] ip sla schedule <TEST-NUMBER>
```

Параметры

<TEST-NUMBER> – номер SLA-теста, принимает значения в диапазоне [1..10000];

<LIFE-TIME> – время жизни теста, принимает значения в диапазоне [1..2147483647] секунд;

forever – время жизни теста не ограничено;

<TIME> – время начала теста, задаётся в виде HH:MM:SS, где:

- HH – часы, принимает значение [0..23];
- MM – минуты, принимает значение [0..59];
- SS – секунды, принимает значение [0..59].

<MONTH> – месяц начала теста, принимает значения [January / February / March / April / May / June / July / August / September / October / November / December];

<DAY> – день месяца начала теста, принимает значения [1..31];

now – начать тест немедленно.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla schedule 1 forever now
```

packet-size

Данной командой задается размер исходящих на SLA-responder пакетов.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
packet-size <SIZE>
```

```
no packet-size
```

Параметры

<SIZE> – размер тестовых пакетов SLA-теста, принимает значения в диапазоне [70..10000] байта.

Значение по умолчанию

74

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# packet-size 256
```

show ip sla configuration

Данной командой выводится информация о текущих настройках SLA-agent.

Синтаксис

```
show ip sla configuration
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show ip sla configuration
Mode:                          Eltex
State:                         Enabled
Logging:                       information
```

show ip sla test configuration

Данной командой выводится информация о сконфигурированных SLA-тестах.

Синтаксис

```
show ip sla test configuration [ <NUM> ] [ vrf <VRF> ]
```

Параметры

<NUM> – номер SLA-теста, задается в диапазоне [1..10000];

<VRF> – имя VRF, задается строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh ip sla test configuration 1
Test number:                 1
State:                       Enabled
Control phase:               Disabled
Authentication:              Disabled
Destination address:         1.1.1.1
Destination port:            1000
Frequency:                   10
Interval:                    20
Number of packets:           100
Packet size:                 74
Source address:              192.168.1.100
Source interface:            --
Source port:                 --
DSCP:                        0
COS:                         0
Timeout:                     3000
Number of history records:   10
wlc-30#
```

show ip sla test statistics

Данной командой выводится информация об актуальных результатах работы SLA-тестов.

Синтаксис

```
show ip sla test statistics [ <NUM> ] [ vrf <VRF> ] [ microseconds ]
```

Параметры

<NUM> – номер SLA-теста, задается в диапазоне [1..10000];

<VRF> – имя VRF, задается строкой до 31 символа;

microseconds – ключ для отображения статистики в микросекундах.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# sh ip sla test statistics 1
Test number:                                1
Transmitted packets:                        100
Lost packets:                               0 (0%)
Lost packets in forward direction:          0 (0%)
Lost packets in reverse direction:          0 (0%)
One-way delay forward min/avg/max:          0/0/12 milliseconds
One-way delay reverse min/avg/max:          0/0/12 milliseconds
One-way jitter forward min/avg/max:         1/1/1 milliseconds
One-way jitter reverse min/avg/max:         1/1/1 milliseconds
Two-way delay min/avg/max:                  0/0/25 milliseconds
Duplicate packets:                          0
Out of sequence packets in forward direction: 0
Out of sequence packets in reverse direction: 0
```

thresholds delay

Данной командой устанавливаются пороги срабатывания оповещений о превышении (high) или нормализации (low) значений задержки.

Использование отрицательной формы команды (no) удаляет пороги и отключает отслеживание параметров задержки.

Синтаксис

`thresholds delay { high <DELAY> | low <DELAY> | forward { high <DELAY> | low <DELAY> } | reverse {high <DELAY> | low <DELAY> } }`

`no thresholds delay { high | low | forward { high | low } | reverse { high | low } }`

Параметры

high – порог срабатывания оповещения о превышении значения параметра теста;

low – порог срабатывания оповещения о нормализации значения параметра теста;

forward – значения задержки в направлении от SLA-agent до SLA-responder;

reverse – значения задержки в направлении от SLA- responder до SLA-agent;

Без указания forward/reverse – задаются суммарные параметры задержки.

<DELAY> – значение задержки, принимает значения в диапазоне [1..60000] миллисекунд.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# thresholds delay low 2000
```

thresholds jitter

Данной командой устанавливаются пороги срабатывания оповещений о превышении (high) или нормализации (low) значений джиттера.

Использование отрицательной формы команды (no) удаляет пороги и отключает отслеживание параметров джиттера.

Синтаксис

```
thresholds jitter { high <JITTER> | low <JITTER> | forward { high <JITTER> | low <JITTER> } | reverse { high <JITTER> | low <JITTER> } }
```

```
no thresholds jitter { high | low | forward { high | low } | reverse { high | low } }
```

Параметры

high – порог срабатывания оповещения о превышении значения параметра теста;

low – порог срабатывания оповещения о нормализации значения параметра теста;

forward – значения джиттера в направлении от SLA-agent до SLA-responder;

reverse – значения джиттера в направлении от SLA- responder до SLA-agent;

Без указания forward/reverse – задаются суммарные параметры джиттера.

<JITTER> – значение джиттера, принимает значения в диапазоне [1..60000] миллисекунд.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# thresholds jitter 50000
```

thresholds losses

Данной командой устанавливаются пороги срабатывания оповещений о превышении (high) или нормализации (low) значений потерь пакетов.

Использование отрицательной формы команды (no) удаляет пороги и отключает отслеживание параметров потерь пакетов.

Синтаксис

```
thresholds losses { high <NUM-PACKETS> | low <NUM-PACKETS> | forward { high <NUM-PACKETS>
| low <NUM-PACKETS> }
| reverse { high <NUM-PACKETS> | low <NUM-PACKETS> } }

no thresholds losses { high | low | forward | low } | reverse { high | low } }
```

Параметры

high – порог срабатывания оповещения о превышении значения параметра теста;

low – порог срабатывания оповещения о нормализации значения параметра теста;

forward – значения количества потерянных пакетов в направлении от SLA-agent до SLA-responder;

reverse – значения количества потерянных пакетов в направлении от SLA- responder до SLA-agent;

Без указания forward/reverse – задаются суммарные количества потерянных пакетов.

<NUM-PACKETS> – количество пакетов, принимает значения в диапазоне [1..60000] миллисекунд.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# thresholds losses
```

Настройка Eltex-SLA

authentication algorithm

Данной командой указывается алгоритм для аутентификации приходящих запросов от SLA-agent.

Использование отрицательной формы команды (no) удаляет алгоритм для аутентификации приходящих запросов от SLA-agent.

Синтаксис

```
authentication algorithm <ALGORITHM>
no authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм аутентификации: sha-256, hmac-sha-256.

Значение по умолчанию

Не задан

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-RESPONDER

Пример

```
wlc-30(config-sla-responder)# authentication algorithm sha-256
```

authentication key-chain

Данной командой указывается набор ключей для аутентификации приходящих запросов от SLA-agent.

Использование отрицательной формы команды (no) удаляет набор ключей для аутентификации приходящих запросов от SLA-agent.

Синтаксис

```
authentication key-chain <KEYCHAIN>
no authentication key-chain
```

Параметры

<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Значение по умолчанию

Не задан

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-RESPONDER

Пример

```
wlc-30(config-sla-responder)# authentication key-chain sla-chain
```

authentication key-string

Данной командой указывается пароль для аутентификации приходящих запросов от SLA-agent.

Использование отрицательной формы команды (no) удаляет пароль для аутентификации приходящих запросов от SLA-agent.

Синтаксис

```
authentication key-string ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }
no authentication key-string
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;
<ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Значение по умолчанию

Отсутствует

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-RESPONDER

Пример

```
wlc-30(config-sla-responder)# authentication key-string ascii-text aukey
```

control-phase authentication algorithm

Данной командой задается алгоритм аутентификации для SLA-теста.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
control-phase authentication algorithm <ALGORITHM>
no control-phase authentication algorithm
```

Параметры

<ALGORITHM> – алгоритм хеширования, принимает значения [sha-256, hmac-sha-256].

Значение по умолчанию

Без шифрования

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase authentication algorithm hmac-sha-256
```

control-phase authentication key-id

Данной командой выбирается номер ключа в key-chain, сконфигурированном командой ip sla key-chain (см. раздел authentication key-chain), который будет отправляться для аутентификации на SLA-responder.

Использование отрицательной формы команды (no) удаляет номер ключа.

Синтаксис

```
control-phase authentication key-id <ID>
no control-phase authentication key-id
```

Параметры

<ID> – идентификатор ключа, задается в диапазоне [1..255].

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase authentication key-id 2
```

control-phase authentication key-string

Данной командой задается ключ аутентификации, который будет отправляться для аутентификации на SLA-responder.

Использование отрицательной формы команды (no) удаляет ключ аутентификации, который будет отправляться для аутентификации на SLA-responder.

Синтаксис

```
control-phase authentication key-string ascii-text { <CLEAR-TEXT> |encrypted <ENCRYPTED-TEXT>}

no control-phase authentication key-string
```

Параметры

<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;

<ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase authentication key-string ascii-text conphkey
```

control-phase destination-port

Данной командой устанавливается UDP-порт, на который будут отправляться запросы на Eltex-SLA-responder.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
control-phase destination-port <PORT>

no control-phase destination-port
```

Параметры

<PORT> – номер UDP-порта, задается в диапазоне [1..65535].

Значение по умолчанию

1800

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase destination-port 9999
```

control-phase retry

Данной командой устанавливается периодичность попыток установления контрольной фазы SLA-теста.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
control-phase retry <TIME>
no control-phase retry
```

Параметры

<TIME> – время ожидания перед повторной попыткой установления контрольной фазы SLA-теста, определяется в секундах [1..86400].

Значение по умолчанию

1

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase retry 300
```

control-phase source-port

Данной командой устанавливается UDP-порт, с которого будут отправляться запросы на Eltex-SLA-responder.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
control-phase source-port <PORT>
no control-phase source-port
```

Параметры

<PORT> – номер UDP-порта, задается в диапазоне [1..65535].

Значение по умолчанию

Отсутствует

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase source-port 3333
```

control-phase timeout

Данной командой устанавливается время ожидания ответа от SLA-responder, по истечении которого контрольная фаза SLA-теста будет считаться неудачной.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
control-phase timeout <TIME>
no control-phase timeout
```

Параметры

<TIME> – время отведенное на прохождение контрольной фазы SLA-теста, определяется в миллисекундах [1..4294967295].

Значение по умолчанию

3000

Необходимый уровень привилегий

15

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# control-phase timeout 5000
```

dscp

Данной командой задается значение DSCP для исходящих на SLA-responder пакетов.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
dscp <DSCP>
no dscp
```

Параметры

<DSCP> – значение кода DSCP, принимает значения [0..63].

Значение по умолчанию

0

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# dscp 58
```

history

Данной командой задается количество сохраняемых результатов SLA-тестов.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
history <SIZE>
no history
```

Параметры

<SIZE> – число сохраняемых результатов, принимает значения [1..10000].

Значение по умолчанию

10

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# history 100
```

icmp-echo

Данной командой задаётся icmp-режим тестирования канала связи и параметры тестирования.

Использование отрицательной формы команды (no) удаляет конфигурацию режима и параметров тестирования.

Синтаксис

```
icmp-echo <DST-ADDRESS> { source-ip <SRC-ADDRESS> | source-interface { <IF> | <TUN> } }
[ interval <INTERVAL> ]
[ num-packets <NUM-PACKETS> ]
```

```
no icmp-echo
```

Параметры

<DST-ADDRESS> – IPv4-адрес SLA-responder. IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-ADDRESS> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IF> – тип и идентификатор интерфейса/туннеля, IP-адрес которого будет использоваться в качестве адреса источника пакетов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<INTERVAL> – интервал отправки тестовых пакетов, принимает значение [1..6000] миллисекунд;

<NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках теста, принимает значение [1..100000].

Значение по умолчанию

<INTERVAL> – 20

<NUM-PACKETS> – 100

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# icmp-echo 10.10.1.1 source-ip 192.168.54.22 num-packets 50 interval 15
```

ip sla key-chain

Данная команда определяет набор паролей для аутентификации через алгоритм хеширования md5 с SLA-responder/agent.

Использование отрицательной формы команды (no) удаляет привязку к набору паролей.

Синтаксис

```
ip sla key-chain <NAME>
no ip sla key-chain
```

Параметры

<NAME> – имя, задаётся строкой от 1 до 16 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla key-chain KEY10
```

ip sla responder

Данной командой выполняется переход в режим конфигурирования параметров SLA-responder.

Использование отрицательной формы команды (no) удаляет примененные ранее параметры SLA-responder.

Синтаксис

```
[no] ip sla responder [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра SLA-responder включается в указанном VRF.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla responder
```

ip sla responder eltex

Данной командой на интерфейсе активируется функционал SLA-responder для Eltex-SLA-agent.

Использование отрицательной формы команды (no) на интерфейсе деактивируется функционал SLA-responder для Eltex-SLA-agent.

Синтаксис

```
[no] ip sla responder eltex
```

Параметры

Отсутствуют.

Значение по умолчанию

Отключено

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP

CONFIG-L2TP

CONFIG-PPTP

CONFIG-VTI

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ip sla responder eltex
```

ip sla responder eltex port

Данной командой устанавливается UDP-порт, на котором будет идти прослушивание запросов от Eltex-SLA-agent.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`ip sla responder eltex port <PORT>`

`no ip sla responder eltex port`

Параметры

<PORT> – номер UDP-порта, задается в диапазоне [1..65535].

Значение по умолчанию

1800

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-GRE

CONFIG-IP4IP

CONFIG-L2TP

CONFIG-PPTP

CONFIG-VTI

CONFIG-E1

CONFIG-MULTILINK

CONFIG-LOOPBACK

Пример

```
wlc-30(config-if-gi)# ip sla responder eltex port 5555
```

timeout

Данной командой устанавливается время ожидания очередного пакета от SLA-responder, по истечении которого SLA-agent закроет SLA-сессию.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
timeout <TIME>
no timeout
```

Параметры

<TIME> – время ожидания, определяется в миллисекундах [1..4294967295].

Значение по умолчанию

3000

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# timeout 1000
```

timeout

Данной командой устанавливается время ожидания очередного пакета от SLA-agent, по истечении которого SLA-responder закроет SLA-сессию.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
timeout <TIME>
no timeout
```

Параметры

<TIME> – время отведенное на прохождение SLA-теста, определяется в миллисекундах [1..4294967295].

Значение по умолчанию

3000

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-RESPONDER

Пример

```
wlc-30(config-sla-responder)# timeout
```

ttl

Данной командой задается значение TTL для исходящих на SLA-responder пакетов.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

`ttl <TTL>`

`no ttl`

Параметры

<TTL> – значение TTL, принимает значения в диапазоне [1..255].

Значение по умолчанию

64

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# ttl
```

udp-jitter

Данной командой задаётся UDP-режим тестирования канала связи и параметры тестирования.

Использование отрицательной формы команды (no) удаляет.

Синтаксис

```
udp-jitter <DST-ADDRESS> <DST-PORT> { source-ip <SRC-ADDRESS> | source-interface { <IF> |
<TUN> } } [ source-port <SRC-PORT> ]
[ interval <INTERVAL> ] [ num-packets <NUM-PACKETS> ]

no udp-jitter
```

Параметры

<DST-ADDRESS> – IPv4-адрес SLA-responder. IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<DST-PORT> – номер UDP-порта назначения тестовых пакетов, принимает значения [1..65535];

<SRC-ADDRESS> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<IF> – тип и идентификатор интерфейса/туннеля, IP-адрес которого будет использоваться в качестве адреса источника пакетов, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов контроллера;

<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей контроллера;

<SRC-PORT> – номер UDP-порта источника тестовых пакетов, принимает значения [1..65535];

<INTERVAL> – интервал отправки тестовых пакетов, принимает значение [1..255] миллисекунд;

<NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках теста, принимает значение [1..6000];

<SRC-ADDRESS> – source адрес тестовых пакетов SLA-теста, задается IPv4-адресом. Может принимать значение IPv4-адреса.

Значение по умолчанию

control enable

<INTERVAL> – 20

<NUM-PACKETS> – 100

<SRC-PORT> – любой свободный

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# udp-jitter 10.10.1.1 50000 source-ip 192.168.54.22 num-packets 50
interval 15
```

vrf

Данной командой задается экземпляр VRF, в адресном пространстве которого должен работать SLA-тест.

Использование отрицательной формы команды (no) возвращает SLA-тест в адресное пространство глобального контроллера.

Синтаксис

```
vrf <VRF>
no vrf
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# vrf subrouter
```

Настройка SLA Weelink (система мониторинга качества услуг)

⚠ Данный функционал активируется только при наличии лицензии.

ip sla hostname

Данной командой задается имя контроллера для его идентификации в системе wiSLA.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip sla hostname <NAME>
no ip sla hostname
```

Параметры

<NAME> – сетевое имя контроллера, задаётся строкой до 31 символов.

Значение по умолчанию

Совпадает с hostname контроллера.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla hostname wlc-302517
```

ip sla portal

Данной командой задается имя контроллера для его идентификации в системе wiSLA.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip sla portal <URL>
no ip sla portal
```

Параметры

<URL> – адрес ссылки, задаётся строкой от 8 до 255 символов.

Значение по умолчанию

Не задан.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla portal wislaurl.loc
```

ip sla responder udp ports

Данной командой включается SLA responder и указываются используемые им TCP/UDP-порты.

Использование отрицательной формы команды (no) отключает SLA responder.

Синтаксис

```
[no] ip sla responder udp ports <PORT-SET-NAME>
```

Параметры

<PORT-SET-NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.

Значение по умолчанию

Выключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla responder udp ports SLA_PORTS
```

ip sla responder udp ports

Данной командой ограничивается список UDP-портов на которые можно принимать тестовые IP SLA-пакеты.

Использование отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
ip sla responder udp ports <OBJECT-GROUP-SERVICE>

no ip sla responder udp ports
```

Параметры

<OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.

Значение по умолчанию

Ограничений нет.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# ip sla responder udp ports OGS_SLA
```

udp-jitter

Данной командой настраивается udp jitter тест.

Использование отрицательной формы команды (no) удаляет udp jitter тест.

Синтаксис

```
[no] udp-jitter <DST-ADDRESS> <DST-PORT> [ control { enable | disable } ] [ interval
<INTERVAL> ] [ num-packets <NUM-PACKETS> ]
[ source-ip <SRC-ADDRESS> ] [ source-port <SRC-PORT> ]
```

Параметры

<DST-ADDRESS> – адрес responder SLA-теста, задается IPv4-адресом. Может принимать значение ipv4-адреса;

IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

<DST-PORT> – номер UDP-порта назначения тестовых пакетов, принимает значения [1..65535];

enable – включить контрольную фазу;

disable – выключить контрольную фазу;

<INTERVAL> – интервал отправки тестовых пакетов, принимает значение [1..6000] миллисекунд;

<NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках теста, принимает значение [1..100000];

<SRC-ADDRESS> – source адрес тестовых пакетов SLA-теста, задается IPv4-адресом. Может принимать значение IPv4-адреса.

IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

<SRC-PORT> – номер UDP-порта источника тестовых пакетов, принимает значения [1..65535].

Значение по умолчанию

control enable

<INTERVAL> – 20

<NUM-PACKETS> – 100

<SRC-ADDRESS> – IP-адрес интерфейса, через который доступен SLA responder

<SRC-PORT> – любой свободный

Необходимый уровень привилегий

10

Командный режим

CONFIG-SLA-TEST

Пример

```
wlc-30(config-sla-test)# udp-jitter 10.10.1.1 50000 control enable num-packets 50 interval 15
```

32 Настройка контроля абонентов (BRAS)

⚠ Данный функционал поддерживается при наличии лицензии.

- aaa das-profile
- aaa services-radius-profile
- aaa sessions-radius-profile
- backup traffic-processing transparent
- bypass-traffic-acl
- class-map
- clear subscriber-control sessions
- default-action
- default-service
- description
- dhcp-option-82-include accept-time
- dhcp-option-82-include enable
- dhcp-option-82-include lease-time
- dhcp-option-82-include size
- enable
- filter-action
- filter-name
- ip proxy http listen-ports
- ip proxy https listen-ports
- ip proxy source-address
- location
- nas-interface
- nas-ip-address
- quota-expired-reauth
- service-subscriber-control
- session accounting
- session ip-authentication
- session l2-roaming disable
- session l2-roaming realtime-accounting
- session mac-authentication
- session unknown-mac-address
- session-timeout
- show subscriber-control configuration
- show subscriber-control radius-servers
- show subscriber-control services count
- show subscriber-control services counters
- show subscriber-control services status
- show subscriber-control sessions count
- show subscriber-control sessions counters
- show subscriber-control sessions status
- subscriber-control
- subscriber-control application-filter
- subscriber-control apps-server-url
- subscriber-control filters-server-url
- subscriber-control peer-address
- subscriber-control thresholds sessions-number
- subscriber-control unused-filters-remove-delay
- thresholds sessions-number
- vrrp-group

aaa das-profile

Данная команда используется для выбора профиля серверов динамической авторизации (DAS), на которые будут приходить CoA запросы от WLC об изменении политики обслуживания, а также запросы оперативной информации от CaptivePortal.

Использование отрицательной формы команды (no) удаляет заданный профиль серверов динамической авторизации (DAS).

Синтаксис

```
[no] aaa das-profile <NAME>
```

Параметры

<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# aaa das-profile profile1
```

aaa services-radius-profile

Данная команда используется для выбора профиля RADIUS-серверов, на которые будут отправляться запросы для получения параметров сервиса пользователя. Если профиль не задан, то будет использоваться профиль «aaa sessions-radius-profile».

Использование отрицательной формы команды (no) удаляет заданный профиль RADIUS-серверов.

Синтаксис

```
[no] aaa services-radius-profile <NAME>
```

Параметры

<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# aaa services-radius-profile profile1
```

aaa sessions-radius-profile

Данная команда используется для выбора профиля RADIUS-серверов, на которые будут отправляться запросы для получения параметров сессии пользователя.

Использование отрицательной формы команды (no) удаляет заданный профиль RADIUS-серверов.

Синтаксис

```
[no] aaa sessions-radius-profile <NAME>
```

Параметры

<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# aaa sessions-radius-profile profile1
```

backup traffic-processing transparent

Данная команда используется для включения прозрачного пропускания трафика в состоянии backup для BRAS.

Использование отрицательной формы команды (no) отключает прозрачное пропускание трафика в состоянии backup для BRAS.

Синтаксис

```
[no] backup traffic-processing transparent
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# backup traffic-processing transparent
```

bypass-traffic-acl

Данная команда используется для организации прозрачного пропускания служебного трафика (DHCP, DNS и т.д.) на основе фильтров.

Использование отрицательной формы команды (no) отключает прозрачное пропускание трафика.

Синтаксис

```
bypass-traffic-acl <NAME>
no bypass-traffic-acl
```

Параметры

<NAME> – имя привязываемого ACL, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# bypass-traffic-acl LANs
```

class-map

Данная команда используется для привязки указанного QoS-класса к сервису по умолчанию. Прохождение трафика не входящего в QoS-класс запрещено.

Использование отрицательной формы команды (no) удаляет привязку класса к сервису по умолчанию.

Синтаксис

```
[no] class-map <NAME>
```

Параметры

<NAME> – имя привязываемого класса, задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-DEFAULT-SERVICE

Пример

```
wlc-30(config-subscriber-default-service)# class-map LAN
```

clear subscriber-control sessions

Данной командой осуществляется удаление активных сессий контроля пользователей.

Синтаксис

```
clear subscriber-control sessions [ vrf <VRF> ] [ username <USER-NAME> ] [ session-id
<SESSION-ID> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут удалены активные сессии в указанном VRF;

<USER-NAME> – имя пользователя, задаётся строкой до 230 символов;

<SESSION-ID> – идентификатор сессии, принимает значения [1..18446744073709551615].

Необходимый уровень привилегий

10

Командный режим

ROOT

Пример

```
wlc-30# clear subscriber-control sessions
```

default-action

Данная команда используется для указания действия, которое должно быть применено для HTTP/HTTPS пакетов, URL (HTTP Host для HTTPS пакетов), в которых не входит в список URL назначенный командой «filter-name» (см. раздел filter-name).

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
default-action <ACT>
no default-action
```

Параметры

<ACT> – назначаемое действие:

- permit – прохождение трафика разрешается;
- deny – прохождение трафика запрещается;
- redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-DEFAULT-SERVICE

Пример

```
wlc-30(config-subscriber-default-service)# default-action redirect http://192.162.1.2/cp
```

default-service

Переход в режим конфигурирования сервиса по умолчанию. Сервис по умолчанию применяется для всех новых пользовательских сессий. После прохождения аутентификации пользователю назначаются персональные сервисы.

Синтаксис

```
default-service
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# default-service
```

description

Данной командой определяется описание профиля контроля пользователей.

Использование отрицательной формы команды (no) удаляет описание.

Синтаксис

```
description <DESCRIPTION>
no description
```

Параметры

<DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов.

Необходимый уровень привилегий

10

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# description "Wi-Fi BRAS"
```

dhcp-option-82-include accept-time

Данная команда устанавливает время, через которое неподтвержденная опция будет удалена.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] dhcp-option-82-include accept-time <SEC>
```

Параметры

<SEC> – период времени в секундах, принимает значения [10..3600].

Значение по умолчанию

10 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# dhcp-option-82-include accept-time 30
```

dhcp-option-82-include enable

Данная команда актирует поиск option 82 в пакетах DHCP.

Использование отрицательной формы (no) деактивирует поиск optin 82 в пакетах DHCP.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# enable
```

dhcp-option-82-include lease-time

Данная команда устанавливает время, через которое запись об подтвержденной опции 82 будет считаться устаревшей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] dhcp-option-82-include lease-time <SEC>
```

Параметры

<SEC> – период времени в секундах, принимает значения [60..86400].

Значение по умолчанию

3600 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# dhcp-option-82-include lease-time 7200
```

dhcp-option-82-include size

Данная команда устанавливает максимальный размер таблицы для хранения option 82.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] dhcp-option-82-include size <SIZE>
```

Параметры

<SIZE> – размер таблицы option 82 [100..2000].

Значение по умолчанию

1000

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# dhcp-option-82-include size 25000
```

enable

Данной командой активируется профиль контроля пользователей.

Использование отрицательной формы команды (no) деактивирует профиль контроля пользователей.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс выключен.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# enable
```

filter-action

Данная команда используется для указания действия, которое должно быть применено для HTTP/HTTPS пакетов, URL (HTTP Host для HTTPS пакетов), в которых входит в список URL назначенный командой «filter-name» (см. раздел filter-name).

Использование отрицательной формы команды (no) удаляет назначенное действие.

Синтаксис

```
filter-action <ACT>
no filter-action
```

Параметры

<ACT> – назначаемое действие:

- permit – прохождение трафика разрешается;
- deny – прохождение трафика запрещается;
- redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-DEFAULT-SERVICE

Пример

```
wlc-30(config-subscriber-default-service)# filter-action redirect http://192.162.1.2/forbidden
```

filter-name

Данная команда используется для указания имени списка URL, который будет использоваться для фильтрации HTTP/HTTPS-трафика не аутентифицированных пользователей. Список может быть настроен локально с помощью профиля URL, либо получен с удаленного сервера (см. раздел subscriber-control application-filter).

Использование отрицательной формы команды (no) удаляет имя списка.

Синтаксис

```
filter-name { local <LOCAL-NAME> | remote <REMOTE-NAME> }
no filter-name
```

Параметры

<LOCAL-NAME> – имя профиля URL, задаётся строкой до 31 символа;

<REMOTE-NAME> – имя списка URL на удаленном сервере, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-DEFAULT-SERVICE

Пример

```
wlc-30(config-subscriber-default-service)# filter-name local BLACK_LIST
```

ip proxy http listen-ports

Данной командой определяется с каких TCP-портов назначения трафик будет перенаправлен на HTTP Proxy-сервер маршрутизатора.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip proxy http listen-ports <NAME>
no ip proxy http listen-ports
```

Параметры

<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# ip proxy http listen-ports HTTP_PORTS
```

ip proxy https listen-ports

Данной командой определяется с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер маршрутизатора.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
ip proxy https listen-ports <NAME>
no ip proxy https listen-ports
```

Параметры

<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# ip proxy https listen-ports HTTPS_PORTS
```

ip proxy source-address

Данной командой определяется IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых Proxy-сервером HTTP/HTTPS пакетах.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

```
ip proxy source-address <ADDR>
no ip proxy source-address
```

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

По умолчанию используется IP-адрес интерфейса, с которого будет отправляться пакет.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# ip proxy source-address 10.100.100.2
```

location

Данная команда используется для изменения идентификатора сетевого интерфейса. Данный идентификатор используется при HTTP-редиректах на CaptivePortal, а также передается в учетной информации RADIUS и при экспорте информации через Netflow протокол.

Использование отрицательной формы команды (no) удаляет идентификатор.

Синтаксис

```
location <ID>
no location
```

Параметры

<ID> – идентификатор сетевого интерфейса, задаётся строкой до 220 символов.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

10

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-L2TPV3

Пример

```
wlc-30(config-if-gi)# location “Guest SSID”
```

nas-interface

Данной командой определяется интерфейс маршрутизатора, IP-адрес которого будет использоваться в качестве IP-адреса источника в отправляемых RADIUS пакетах.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

```
nas-interface {<IF> | <TUN>}
no nas-interface
```

Параметры

<IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.

Значение по умолчанию

Не задано.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# nas-interface gi 1/0/1
```

nas-ip-address

Данной командой определяется IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS пакетах.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

```
nas-ip-address <ADDR>
no nas-ip-address
```

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# nas-ip-address 10.100.100.2
```

quota-expired-reauth

Данной командой можно включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени. В ином случае, после истечения квоты сервис будет деактивирован, и пользователю будет назначен сервис по умолчанию.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] quota-expired-reauth
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

При истечении квоты пользователю будет назначен сервис по умолчанию.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# quota-expired-reauth
```

service-subscriber-control

Данная команда используется для включения контроля пользователей на интерфейсе. При выполнении со значением параметра «any» контроль пользователей будет работать для пакетов из любой подсети, в ином случае только для пакетов из подсетей указанных в профиле IP-адресов.

Использование отрицательной формы команды (no) выключает контроль пользователей на интерфейсе.

Синтаксис

```
service-subscriber-control { any | object-group <NAME> }
no service-subscriber-control
```

Параметры

<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-IP4IP4

CONFIG-GRE

Пример

```
wlc-30(config-if-gi)# service-subscriber-control object-group LAN
```

session accounting

Данной командой устанавливается режим отправки сообщений RADIUS-accounting.

При использовании отрицательной формы команды (no) устанавливается значение по умолчанию.

Синтаксис

```
session accounting { all | auth-only }
```

Параметры

all – отправка для всех сессий;

auth-only – отправка для авторизированных сессий.

Значение по умолчанию

all

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session accounting all
```

session ip-authentication

Данной командой можно включить аутентификацию сессий по IP-адресу.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] session IP-authentication
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session ip-authentication
```

session l2-roaming disable

Данной командой можно выключить режим прозрачного роуминга абонентов между L2-интерфейсами BRAS. В случае изменения L2-интерфейса абоненту необходимо будет заново пройти аутентификацию.

Использование отрицательной формы команды (no) включает режим прозрачного роуминга абонентов между L2-интерфейсами BRAS.

Синтаксис

```
[no] session l2-roaming disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Включен режим прозрачного роуминга абонентов между L2 интерфейсами BRAS.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session l2-roaming disable
```

session l2-roaming realtime-accounting

Данной командой можно включить режим отправки RADIUS-аккаунтинга в реальном времени при изменении L2-интерфейса BRAS, по которому приходит работа с абонентом.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] session l2-roaming realtime-accounting
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

RADIUS-аккаунтинг с измененным L2-интерфейсом отправляется по истечению Interim-Update.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session l2-roaming realtime-accounting
```

session mac-authentication

Данной командой можно включить аутентификацию сессий по MAC-адресу.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] session mac-authentication
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Отключено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session mac-authentication
```

session unknown-mac-address

Данной командой можно запретить прохождение трафика в аутентифицированной сессии для пакетов, у которых изменился MAC-адрес источника с момента аутентификации пользователя. Также при получении пакета с отличающимся MAC-адресом источника будет выведено сообщение в SYSLOG.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] session unknown-mac-address filtering
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Прохождение трафика с отличающимся MAC-адресом источника разрешено.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# session unknown-mac-address
```

session-timeout

Данной командой задаётся интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
session-timeout <SEC>
no session-timeout
```

Параметры

<SEC> – период времени в секундах, принимает значения [120..3600].

Значение по умолчанию

120 секунд

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-DEFAULT-SERVICE

Пример

```
wlc-30(config-subscriber-default-service)# session-timeout 155
```

show subscriber-control configuration

Командой выполняется просмотр параметров конфигурации контроля пользователей.

Синтаксис

```
show subscriber-control configuration [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control configuration
State:                Enabled
Description:          --
NAS IP address:       192.168.107.201
Sessions radius profile:       RADIUS
Services radius profile:       --
DAS profile:          bras2
Quota expired reauth: Disabled
Default service:
 Class map:            list1
 Filter name:          defaultserv
 Filter type:          local
 Filter action:        permit
 Default action:       redirect
 Default redirect URL: http://192.168.107.213:8080/eltex_portal/
```

show subscriber-control radius-servers

Данная команда используется для просмотра информации об используемых RADIUS-серверах.

Синтаксис

```
show subscriber-control radius-servers [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены используемые RADIUS-сервера в указанном VRF.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control radius-servers
IP address         Port     VRF             Usage           Connections count   Dead interval
Dead time
----------------   ------   -------------   -------------   -----------------   -------------
---------
172.16.0.134       31813    --              services acct   0                   10
--
172.16.0.134       31812    --              services auth   0                   10
--
172.16.0.135       31813    --              sessions acct   0                   10
--
172.16.0.135       31812    --              sessions auth   0                   10
--
```

show subscriber-control services count

Данные команды используются для просмотра информации и статистики по сервисам сессий контроля пользователей.

Синтаксис

```
show subscriber-control services count [ { vrf <VRF> | service <SERVICE-NAME> } ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сервисы в указанном VRF.

<SERVICE-NAME> – имя сервиса, задаётся строкой до 220 символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control services count
Service           Active        Not active
---------------   -----------   -----------
INTERNET          17            0
WELCOME           0             2
```

show subscriber-control services counters

Данные команды используются для просмотра счетчиков по сервисам сессий контроля пользователей.

Синтаксис

```
show subscriber-control services counters session-id <SESSION-ID> [ vrf <VRF> ]
[ service-id <SERVICE-ID> ] [ service <SERVICE-NAME> ]
```

Параметры

counters – просмотр статистики по сервису пользователя;

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сервисы в указанном VRF.

<SESSION-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615].

<SERVICE-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615].

<SERVICE-NAME> – имя сервиса, задаётся строкой до 220 символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control services status counters session-id 5116089176692896081
Service id             Service name      Recv packets     Recv bytes       Send packets
Send bytes
--------------------   ---------------   --------------   --------------   --------------
--------------
5152117973711859021    A INTERNET        2018             1615309          1761
281017
```

show subscriber-control services status

Данные команды используются для просмотра оперативной информации по сервисам сессий контроля пользователей.

Синтаксис

```
show subscriber-control services status [ session-id <SESSION-ID> ] [ { service-id
<SERVICE-ID> | service <SERVICE-NAME> ] [ vrf <VRF> ]
```

Параметры

status – просмотр оперативной информации по сервису пользователя;

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сервисы в указанном VRF;

<SESSION-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615];

<SERVICE-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615];

<SERVICE-NAME> – имя сервиса, задаётся строкой до 220 символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control services status
Service id    Session id    Service name    User name    Quota volume    Quota time
                                                         (Bytes)         (Seconds)
------------  ------------  --------------  -----------  --------------  --------------
2522015791    2161727821    INTERNET5       79001110011  --              --
```

show subscriber-control sessions count

Данные команды используются для просмотра информации и статистики по сессиям контроля пользователей.

Синтаксис

```
show subscriber-control sessions count [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сессии в указанном VRF;

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control sessions count
All:               18
Authenticated:     17
Not authenticated: 1
```

show subscriber-control sessions counters

Данные команды используются для просмотра счетчиков по сессии пользователей.

Синтаксис

```
show subscriber-control sessions counters { session-id <SESSION-ID> | username <SERVICE-NAME> } [ vrf <VRF> ]
```

Параметры

status – просмотр оперативной информации по сессии пользователя;

counters – просмотр статистики по сессии пользователя;

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сессии в указанном VRF;

<SESSION-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615];

<USER-NAME> – имя пользователя, задаётся строкой до 230 символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control sessions counters session-id 5116089176692896081
User name         Recv packets     Recv bytes       Send packets     Send bytes
---------------   --------------   --------------   --------------   --------------
79231552525       2198             1697762          1984             313452
```

show subscriber-control sessions status

Данные команды используются для просмотра оперативной информации по сессии пользователей.

Синтаксис

```
show subscriber-control sessions status [ { session-id <SESSION-ID> | username <SERVICE-NAME> } ] [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа. При указании данного параметра будут отображены активные сессии в указанном VRF;

<SESSION-ID> – идентификатор сессии, принимает значения [1.. 18446744073709551615];

<USER-NAME> – имя пользователя, задаётся строкой до 230 символов.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show subscriber-control sessions status
Session id    User name    IP address       MAC address         Interface   Domain
------------  -----------  ------------     -----------------   ---------   ---------
2161727821    79001110011  192.168.244.12   c4:12:f5:d4:af:70   bridge 13   root
wlc-30# show subscriber-control sessions counters session-id 2161727821
User name         Recv packets     Recv bytes       Send packets     Send bytes
---------------   --------------   --------------   --------------   --------------
79001110011       243              87056            294              35961
```

subscriber-control

Команда используется для создания профиля контроля пользователей и перехода в режим его конфигурирования.

Использование отрицательной формы команды (no) удаляет указанный профиль контроля пользователей.

Синтаксис

```
[no] subscriber-control [ vrf <VRF> ]
```

Параметры

<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control
```

subscriber-control application-filter

Данная команда используется для включения контроля приложений на интерфейсе.

Использование отрицательной формы команды (no) выключает контроль приложений на интерфейсе.

Синтаксис

```
subscriber-control application-filter <NAME>
no subscriber-control application-filter
```

Параметры

<NAME> – имя профиля приложений, задаётся строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-IF-GI

CONFIG-IF-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-IP4IP4

CONFIG-GRE

CONFIG-L2TPV3

Пример

```
wlc-30(config-if-gi)# subscriber-control application-filter LIST
```

subscriber-control apps-server-url

Данная команда используется для задания URL-адреса сервера, предоставляющего списки приложений для фильтрации трафика. Списки запрашиваются у сервера в момент аутентификации пользователя.

Использование отрицательной формы команды (no) удаляет заданный URL-сервера.

Синтаксис

```
subscriber-control apps-server-url <URL>
no subscriber-control apps-server-url
```

Параметры

<URL> – адрес ссылки, задаётся строкой от 8 до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control apps-server-url "http://192.168.1.1/files/"
```

subscriber-control filters-server-url

Данная команда используется для задания адреса сервера, предоставляющего списки URL для фильтрации HTTP/HTTPS-трафика. Списки запрашиваются у сервера в момент аутентификации пользователя.

Использование отрицательной формы команды (no) удаляет заданный URL-сервера.

Синтаксис

```
subscriber-control filters-server-url <URL>
no subscriber-control filters-server-url
```

Параметры

<URL> – адрес ссылки, задаётся строкой до 255 символов.

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control filters-server-url "http://192.168.1.1/files/"
```

subscriber-control peer-address

Данной командой определяется IP-адрес соседа, с которым будет осуществляться синхронизация таблицы с option 82.

Использование отрицательной формы команды (no) удаляет IP-адрес соседнего маршрутизатора из конфигурации.

Синтаксис

```
subscriber-control peer-address <ADDR>
no subscriber-control peer-address
```

Параметры

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

Отсутствует.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control peer-address 10.24.80.100
```

subscriber-control thresholds sessions-number

Данная команда используется для задания порога количества сессий BRAS всех профилей контроля пользователей для отправки snmp-trap eltexBrasSessionsNumberHigh и eltexBrasSessionsNumberHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
subscriber-control thresholds sessions-number { high <TH-HIGH> | low <TH-LOW> }
```

```
no subscriber-control thresholds sessions-number { high | low }
```

Параметры

<TH-HIGH> – порог количества сессий BRAS для отправки snmp-trap eltexBrasSessionsNumberHigh, допустимы значения от 0 до 1000;

<TH-LOW> – порог количества сессий BRAS для отправки snmp-trap eltexBrasSessionsNumberHighOk допустимы значения от 0 до 1000.

Значение по умолчанию

<TH-HIGH> - 900,

<TH-LOW> - 850.

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control thresholds sessions-number high 800
```

subscriber-control unused-filters-remove-delay

Данная команда используется для задания интервала, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
subscriber-control unused-filters-remove-delay <DELAY>
no subscriber-control unused-filters-remove-delay
```

Параметры

<DELAY> – временной интервал в секундах, принимает значения [10800..86400].

Значение по умолчанию

10800

Необходимый уровень привилегий

15

Командный режим

CONFIG

Пример

```
wlc-30(config)# subscriber-control unused-filters-remove-delay 40000
```

thresholds sessions-number

Данная команда используется для задания порога количества сессий BRAS для отправки snmp-trapeltexBrasSessionsNumberHighи eltexBrasSessionsNumberHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
thresholds sessions-number { high <TH-HIGH> | low <TH-LOW> }
no thresholds sessions-number { high | low }
```

Параметры

<TH-HIGH> – порог количества сессий BRAS для отправки snmp-trap eltexBrasSessionsNumberHigh, допустимы значения от 0 до 1000;

<TH-LOW> – порог количества сессий BRAS для отправки snmp-trapeltexBrasSessionsNumberHighOk, допустимы значения от 0 до 1000.

Значение по умолчанию

<TH-HIGH> - 0,

<TH-LOW> - 0.

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# thresholds sessions-number high 8000
```

vrrp-group

Данной командой определяется VRRP-группа, на основе которой определяется состояние (основной/резервный) сервиса контроля абонентов. При переключении VRRP в состояние BACKUP происходит сброс всех сессий контроля пользователей.

Использование отрицательной формы команды (no) удаляет идентификатор VRRP.

Синтаксис

```
vrrp-group <GRID>
```

```
no vrrp-group
```

Параметры

<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].

Необходимый уровень привилегий

15

Командный режим

CONFIG-SUBSCRIBER-CONTROL

Пример

```
wlc-30(config-subscriber-control)# vrrp-group 10
```

33 Настройка Wi-Fi контроллера туннелей

- aaa das-profile
- aaa radius-profile
- data-tunnel configuration
- enable
- failure-count
- keepalive mode
- keepalive-disable
- nas-ip-address
- peer-address
- resp-time
- retry-time
- show interfaces bridge switch-communities
- show interfaces bridge switch-communities community
- show interfaces bridge switch-communities community include
- show interfaces bridge switch-communities summary
- thresholds tunnels-number
- thresholds sub-tunnels-number
- vrrp-group
- wireless-controller

aaa das-profile

Данная команда используется для выбора профиля серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF об изменении политики обслуживания.

Использование отрицательной формы команды (no) удаляет заданный профиль серверов динамической авторизации (DAS).

Синтаксис

```
[no] aaa das-profile <NAME>
```

Параметры

<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.

Необходимый уровень привилегий

15

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# aaa das-profile profile1
```

aaa radius-profile

Данная команда используется для выбора профиля RADIUS-серверов, на которые будут отправляться запросы для получения конфигурации SoftGRE DATA туннелей (обслуживаемых SSID и параметров шейпинга).

Использование отрицательной формы команды (no) удаляет заданный профиль RADIUS-серверов.

Синтаксис

```
[no] aaa radius-profile <NAME>
```

Параметры

<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.

Значение по умолчанию

default_radius

Необходимый уровень привилегий

15

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# aaa radius-profile default_radius
```

data-tunnel configuration

Данной командой устанавливается режим конфигурации SoftGRE DATA туннелей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
data-tunnel configuration { local | radius }
no data-tunnel configuration
```

Параметры

local – режим конфигурации, при котором параметры SoftGRE DATA туннелей получаются из локальной конфигурации маршрутизатора.

radius – режим, при котором параметры SoftGRE DATA туннелей запрашиваются у RADIUS-сервера.

Значение по умолчанию

wlc

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# data-tunnel configuration wlc
```

enable

Данной командой активируется контроллер Wi-Fi.

Использование отрицательной формы команды (no) деактивирует контроллер Wi-Fi.

Синтаксис

```
[no] enable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс включен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# enable
```

failure-count

Данной командой определяется количество последовательных неудачных ICMP-запросов после которых, при отсутствии ответа от встречной стороны, туннель считается нерабочим и удаляется из системы.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
[no] failure-count <VALUE>
```

Параметры

<VALUE> – количество неудачных ping запросов, принимает значения [1..100].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# failure-count 8
```

keepalive mode

Данной командой устанавливается режим работы механизма keepalive для SoftGRE туннелей.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

```
keepalive mode { proactive | reactive }
no keepalive mode
```

Параметры

- proactive – режим проверки SoftGRE туннелей через icmp проверку удаленного адреса;
- reactive – режим проверки SoftGRE туннелей через прием icmp пакетов с payload: “ELTEX_GRE IPv4 < туннельный ip address устройства>” от удаленных устройств внутри туннеля.

Значение по умолчанию

proactive

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# keepalive mode reactive
```

keepalive-disable

Данная команда отключает обмен ICMP-сообщениями, которые используются для проверки доступности удаленного шлюза туннелей Wi-Fi контроллера.

Использование отрицательной формы команды (no) включает обмен ICMP-сообщениями.

Синтаксис

```
[no] keepalive-disable
```

Параметры

Команда не содержит параметров.

Значение по умолчанию

Процесс отключен.

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# keepalive-disable
```

nas-ip-address

Данной командой определяется IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS-пакетах.

Использование отрицательной формы команды (no) удаляет указанный IP-адрес источника.

Синтаксис

```
nas-ip-address <ADDR>
no nas-ip-address
```

Параметры

<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Значение по умолчанию

127.0.0.1

Необходимый уровень привилегий

15

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# nas-ip-address 10.100.100.2
```

peer-address

Данной командой определяется IP-адрес соседа, с которым будет осуществляться резервирование туннелей.

Использование отрицательной формы команды (no) удаляет IP-адрес соседнего маршрутизатора из конфигурации.

Синтаксис

```
[no] peer-address <ADDR>
```

Параметры

<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# peer-address 192.168.0.15
```

resp-time

Данной командой определяется время ожидания ответа, после истечении которого ICMP-запрос считается отклоненным.

Использование отрицательной формы устанавливает значение resp-time по умолчанию.

Синтаксис

```
[no] resp-time <TIME >
```

Параметры

<TIME > – количество секунд, принимает значения [1..30].

Значение по умолчанию

5

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# resp-time 30
```

retry-time

Данной командой устанавливается время между ICMP-запросами.

Использование отрицательной формы команды (no) устанавливает значение retry-time по умолчанию.

Синтаксис

```
[no] retry time < TIME >
```

Параметры

< TIME > – количество секунд, принимает значения [60..3600].

Необходимый уровень привилегий

10

Значение по умолчанию

60

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# retry-time 12
```

show interfaces bridge switch-communities

Командой выполняется просмотр списка сформированных switch-community.

Синтаксис

show interfaces bridge switch-communities [<BRIDGE-ID>]

Параметры

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces bridge switch-communities
bridge 10
Location                          Community                                  Interfaces
--------------------------------  -----------------------------------------
-----------------------------------------
data10                            Eltex.Novosibirsk.Novosibirskaya_oblast   softgre 2.10,
softgre 4.10, softgre 6.10,
                                  .MRF_Sibir.Local.AllClients.root          softgre 8.10

data10                            TEST.Novosibirsk.Novosibirskaya_oblast   softgre 2.310,
softgre 4.310, softgre
                                  .MRF_Sibir.Local.AllClients.root          6.310, softgre
8.310


bridge 11
Location                          Community                                  Interfaces
--------------------------------  -----------------------------------------
-----------------------------------------
data11                            Eltex.Novosibirsk.Novosibirskaya_oblast   softgre 2.311,
softgre 4.311, softgre
                                  .MRF_Sibir.Local.AllClients.root          6.311, softgre
8.311
```

show interfaces bridge switch-communities community

Командой выполняется просмотр списка сформированных switch-community, соответствующих определенному названию домена СУ EMS.

Синтаксис

show interfaces bridge switch-communities community <EMS-DOMAIN> [<BRIDGE-ID>]

Параметры

<EMS-DOMAIN> – имя домена СУ EMS, WORD(1-246).

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces bridge switch-communities community
Eltex.Novosibirsk.Novosibirskaya_oblast.MRF_Sibir.Local.AllClients.root
bridge 10
Location                         Community                                  Interfaces
-------------------------------  -----------------------------------------
----------------------------------------
data10                           Eltex.Novosibirsk.Novosibirskaya_oblast    softgre 2.10,
softgre 4.10, softgre 6.10,
                                 .MRF_Sibir.Local.AllClients.root           softgre 8.10


bridge 11
Location                         Community                                  Interfaces
-------------------------------  -----------------------------------------
----------------------------------------
data11                           Eltex.Novosibirsk.Novosibirskaya_oblast    softgre 2.311,
softgre 4.311, softgre
                                 .MRF_Sibir.Local.AllClients.root           6.311, softgre
8.311
```

show interfaces bridge switch-communities community include

Командой выполняется просмотр списка сформированных switch-community, соответствующих определенному шаблону в названии домена СУ EMS.

Синтаксис

show interfaces bridge switch-communities community include <WORD> [<BRIDGE-ID>]

Параметры

<WORD> - шаблон, по которому выполняется поиск в имени домена СУ EMS, WORD(1-246).

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces bridge switch-communities community include eltex
bridge 10
Location                         Community                                  Interfaces
-------------------------------  -----------------------------------------
----------------------------------------
data10                           Eltex.Novosibirsk.Novosibirskaya_oblast    softgre 2.10,
softgre 4.10, softgre 6.10,
                                 .MRF_Sibir.Local.AllClients.root           softgre 8.10


bridge 11
Location                         Community                                  Interfaces
-------------------------------  -----------------------------------------
----------------------------------------
data11                           Eltex.Novosibirsk.Novosibirskaya_oblast    softgre 2.311,
softgre 4.311, softgre
                                 .MRF_Sibir.Local.AllClients.root           6.311, softgre
8.311
```

show interfaces bridge switch-communities summary

Командой выполняется просмотр количества сформированных switch-community.

Синтаксис

show interfaces bridge switch-communities summary [<BRIDGE-ID>]

Параметры

<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.

Необходимый уровень привилегий

1

Командный режим

ROOT

Пример

```
wlc-30# show interfaces bridge switch-communities summary
Bridges      Communities
----------   -----------
bridge 10    2
bridge 11    1
```

thresholds tunnels-number

Данная команда используется для задания порога количества туннелей SoftGRE для отправки snmp - trap eltexInterfacesNumberHigh и eltexInterfacesNumberHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
thresholds tunnels-number { high <TH-HIGH> | low <TH-LOW> }
no thresholds tunnels-number { high | low }
```

Параметры

<TH-HIGH> – порог количества туннелей SoftGRE для отправки snmp-trap eltexInterfacesNumberHigh;

<TH-LOW> – порог количества туннелей SoftGRE для отправки snmp-trap eltexInterfacesNumberHighOk.

Значение по умолчанию

<TH-HIGH> – 400, <TH-LOW> – 350

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# thresholds tunnels-number high 1000
```

thresholds sub-tunnels-number

Данная команда используется для задания порога количества сабтуннелей SoftGRE для отправки snmp – trap eltexInterfacesNumberHigh и eltexInterfacesNumberHighOk.

Использование отрицательной формы команды (no) устанавливает значения по умолчанию.

Синтаксис

```
thresholds sub-tunnels-number { high <TH-HIGH> | low <TH-LOW> }
no thresholds sub-tunnels-number { high | low }
```

Параметры

<TH-HIGH> – порог количества сабтуннелей SoftGRE для отправки snmp-trap eltexInterfacesNumberHigh;

<TH-LOW> – порог количества сабтуннелей SoftGRE для отправки snmp-trap eltexInterfacesNumberHighOk.

Значение по умолчанию

<TH-HIGH> – 1000, <TH-LOW> – 900

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# thresholds sub-tunnels-number high 2000
```

vrrp-group

Данной командой определяется VRRP-группа, на основе которой определяется состояние (основной/резервный) Wi-Fi контроллера.

Использование отрицательной формы команды (no) удаляет идентификатор VRRP.

Синтаксис

```
vrrp-group <GRID>
no vrrp-group
```

Параметры

<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].

Необходимый уровень привилегий

10

Командный режим

CONFIG-WIRELESS

Пример

```
wlc-30(config-wireless)# vrrp-group 10
```

wireless-controller

Переход в режим конфигурирования контроллера Wi-Fi.

Использование отрицательной формы команды (no) очищает конфигурацию и выключает контроллер Wi-Fi туннелей.

Синтаксис

```
[no] wireless-controller
```

Параметры

Команда не содержит параметров.

Необходимый уровень привилегий

10

Командный режим

CONFIG

Пример

```
wlc-30(config)# wireless-controller
```

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex-co.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: https://eltex-co.ru

Технический форум: https://eltex-co.ru/forum

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex-co.ru/support/downloads