Коммутатор Symanitron серии Enterprise

Руководство пользователя по Интерфейсу Командной Строки CLI (ИКС)

(12.2017)

УВЕДОМЛЕНИЕ ОБ АВТОРСКИХ ПРАВАХ

ТОРГОВАЯ МАРКА

SYMANITRON зарегистрированная торговая марка Symanitron LTD.

Все прочие товарные знаки являются собственностью их соответствующих владельцев.

ЗАЯВЛЕНИЕ О СООТВЕТСТВИИ

Продукты, обозначенные в данной публикации, соответствуют всем заявленным характеристикам. Для получения подробной информации обратитесь к данному Руководству.

ГАРАНТИЯ

Symanitron гарантирует, что все продукты не имеют дефектных материалов и дефектов изготовления в течение указанного гарантийного срока (5 лет для большинства продуктов). Symanitron обеспечит ремонт или замену продуктов в течение гарантийного срока,. Данная гарантия не распространяется на модификации продуктов или ремонт, которые были выполнены не уполномоченными компанией лицами, а также данная гарантия не распространяется на продукты, которые были установлены (смонтированы) не в соответствии с данным руководством или имеют механические повреждения.

Пожалуйста, обратитесь к соответствующему разделу в описании продукта для получения информации о фактическом гарантийном сроке.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ

Symanitron не несет ответственности за использование данного руководства третьими лицами в собственных целях. В данной публикации могут содержаться непреднамеренные ошибки. Symanitron оставляет за собой право изменять содержание данной публикации без предварительного уведомления.

КОНТАКТНАЯ ИНФОРМАЦИЯ

Symanitron LTD.
Вебсайт: www.symanitron.ru

Техническая поддержка
E-mail: support@symanitron.ru

Содержание

1. Использование интерфейса командной строки (ИКС)

После успешного подключения к коммутатору в соответствии с документом «Краткое руководство пользователя», коммутатором можно управлять с помощью встроенного в программное обеспечение Интерфейса командной строки (ИКС). Данный интерфейс позволяет вводить команды и соответствующие параметры для настройки всех функций системы. В данном разделе дано общее описание ИКС и рекомендации по его использованию.

Вы также можете использовать telnet и ssh для доступа к командной строке коммутатора.

1.1 Рекомендации по использованию ИКС

В таблице представлены условные обозначения, использующиеся в синтаксисе команд ИКС.

Условные знаки в командах интерфейса командной строки

Условный знак или форматирование	**Описание**
`Courier New`	Полужирным шрифтом Courier New приводятся вводимые команды
`Courier New`	Курсивом и шрифтом Courier New указывается параметр или переменная, вместо которой необходимо задать соответствующее значение
`Courier New`	Шрифтом Courier New указаны примеры введенных команд и результаты их выполнения
[ ]	В квадратных скобках указываются дополнительные необязательные параметры команды
{ }	В фигурных скобках указывается список обязательных параметров, разделенных знаком «|», при этом необходимо выбрать один из вариантов
<Enter>, **<Ctrl+F4>**	Полужирным шрифтом в угловых скобках указана клавиша клавиатуры или сочетание клавиш, наживаемых одновременно
`all`	Когда в команде для определения диапазона портов или параметров требуется задать определенный аргумент, и одним из его значений является all, то оно является значением по умолчанию

1.2 Режимы ИКС

Для удобства настройки оборудования ИКС разделен на несколько командных режимов. Каждый режим имеет собственный характерный набор команд. При вводе знака вопроса “?” в строке консоли отображается полный список команд, доступных в данном отдельном режиме.

Специальная команда, разная для разных режимов, используется для переключения между режимами. Следующий порядок доступа к режимам является стандартным: Пользовательский

режим **User EXEC**, привилегированный режим **Privileged EXEC**, режим общей настройки **Global Configuration** и режимы настройки интерфейсов **Interface Configuration.**

При запуске сессии начальным режимом для непривилегированных пользователей является режим *User EXEC*. В нем доступен только ограниченный набор команд. Такой уровень зарезервирован для задач, в которых конфигурация устройства не изменяется. Привилегированные пользователи могут напрямую зайти в режим *Privileged EXEC*, введя соответствующий пароль. В данном режиме доступны режимы настройки устройства.

Далее описаны указанные режимы.

Пользовательский режим User EXEC

При подключении к устройству пользователь, не являющийся привилегированным, автоматически входит в режим команд *User EXEC*. В целом команды режима *User EXEC* позволяют пользователю выполнить основные тесты и отобразить системные данные.

Привилегированный режим Privileged EXEC

Для предотвращения несанкционированного использования привилегированный режим защищен паролем, т.к. многие из команд данного режима устанавливают системные параметры работы коммутатора. Привилегированные пользователи входят напрямую в режим *Privileged EXEC*. Для возврата в режим *User EXEC* необходимо использовать команду **`disable`**, описание которой дано ниже.

Режим Общей настройки Global Configuration

Команды режима *Global Configuration* применяются для настройки параметров системы в целом, а не только какого-то конкретного интерфейса. Для входа в данный режим необходимо в режиме *Privileged EXEC* ввести команду **`configure terminal`** и нажать клавишу <**Enter**>. Для возврата в режим *Privileged EXEC* необходимо использовать команды **`exit`, `end`** или сочетание клавиш <**Ctrl+z**>.Описание указанных здесь команд дано ниже в соответствующих разделах.

Режимы Настройки интерфейсов Interface Configuration

С помощью команд следующих режимов выполняются действия над конкретными интерфейсами:

- **Настройка соединения** (**Line Configuration**) – состоит из команд для настройки подключения терминала. К ним относятся команды для настройки скорости линии, времени ожидания и т.д. Для входа в режим настройки соединения *Line Configuration* используется команда **`line`** режима *Global Configuration.*
- **Конфигурирование VLAN** (**VLAN DataBASE**) – состоит из команд для создания виртуальных локальных сетей (VLAN) в целом. Для входа в режим настройки интерфейсов виртуальных локальных сетей *VLAN DataBASE Interface Configuration* используется команда **`vlan dataBASE`** режима *Global Configuration.*
- **Списки доступа для управления** (**Management Access List**) – состоит из команд для определения списков доступа к управлению устройством. Для входа в режим настройки и управления списками доступа *Management Access List Configuration* используется команда **`management access-list`** режима *Global Configuration.*
- **Агрегирование каналов** (**Port Channel**) – состоит из команд для настройки агрегированных каналов (port-channels), например, для назначения портов в виртуальной локальной сети (VLAN) или агрегированном канале (port-channel). Для входа в режим настройки интерфейса

агрегирования каналов *Port Channel Interface Configuration* используется команда **`port-channel`** режима *Global Configuration*.

- **Последовательность открытых ключей SSH (SSH Public Key-Chain)** – состоит из команд для установки открытых ключей SSH другого устройства вручную. Для входа в режим настройки последовательности открытых ключей *SSH Public Key-chain Configuration* используется команда **`crypto key pubkey-chain ssh`** режима *Global Configuration*.
- **Интерфейс (Interface)** – состоит из команд для настройки отдельных интерфейсов. Для входа в режим настройки интерфейса *Interface Configuration* используется команда **`interface`** режима *Global Configuration*.

Примечание: В системе также реализован режим отладки *Debug Mode*, который используется для редактирования MIB-файлов и выполнения других специальных функций. Для выполнения необходимых процедур в указанном режиме и получения по нему дополнительной информации обращайтесь к производителю.

1.3 Ввод команд

Команды ИКС представляют собой последовательность ключевых слов и аргументов. Ключевые слова определяют команды, а с помощью аргументов устанавливаются параметры настройки. Например, в команде "`show interfaces status gi1/1/5`" слова `show`, `interfaces` и `status` являются ключевыми, `gi` является аргументом, задающим тип интерфейса, а `1/1/5` является аргументом, задающим конкретный порт. Если параметры команды имеют значения по умолчанию, то они становятся активными при вводе таких команд без указания параметров.

При вводе команд с обязательными параметрами необходимые аргументы задаются после ключевых слов. Например, для того чтобы установить пароль администратора, нужно ввести:

```
console(config)# username admin password Bloomenbergensteinenthal
```

В процессе работы пользователь может получить справочную информацию по необходимым командам и их аргументам:

- Просмотр ключевых слов – вместо команды вводится символ вопроса "?". При этом отображается список всех применимых команд с соответствующими справочными сообщениями.
- Просмотр параметров команды – после ключевых слов вместо параметров команды вводится символ вопроса "?". При этом отображается список всех соответствующих параметров команды.

Далее описаны функции, которые могут быть полезны при использовании ИКС.

1.4 Буфер команд

Каждая команда, введенная в ИКС, записывается в буфер истории команд, имеющий внутреннее управление. Команды в данном буфере хранятся по принципу "Первый зашел – первый вышел" (FIFO). При этом команды могут быть вызваны повторно, отредактированы и выполнены снова. После перезагрузки устройства содержимое буфера не сохраняется. В Таблице 4.2 представлены клавиши, с помощью которых можно получить доступ к командам из буфера.

По умолчанию буфер истории команд включен, но его в любой момент можно отключить. Подробная информация о синтаксисе команд для включения и отключения буфера истории команд приведена в разделе описания команды **history**.

В буфере по умолчанию хранится стандартное число команд, равное 10. Это число может быть увеличено до 256. Установка нулевого значения числа команд равносильна отключению буфера. Подробная информация о синтаксисе команд для настройки буфера истории команд приведена в разделе описания команды **history size**. Для отображения содержимого буфера используется команда **show history**.

Отмена действия команды

Перед многими командами, использующимися при настройке устройства, можно ввести префикс "**no**" для отмены действия команды или для сброса настройки к значению по умолчанию. В данном руководстве описано такое обращение действия всех применимых команд.

Автоматическое заполнение команды

Если команда введена не полностью, не правильно или имеет недостающие или неверные параметры, то на экране появится соответствующее сообщение об ошибке. Для завершения не полностью введенной команды необходимо нажать клавишу <**Tab**>. Если при этом уже введенных символов недостаточно для однозначной идентификации команды, то необходимо ввести знак вопроса "**?**" для отображения всех возможных команд, подходящих под введенные символы.

Неправильные или неполные команды автоматически отображаются перед курсором. Если должен быть добавлен параметр, то его можно записать после автоматически введенной команды. На следующем примере показано, что для команды `interface` требуется задать недостающий параметр:

```
console(config)#interface
% Incomplete command
console(config)#
```

1.5 Горячие клавиши ИКС

ИКС поддерживает ряд "горячих" клавиш, облегчающих ввод команд. Указанные клавиши описаны в таблице.

"Горячие" клавиши ИКС

Клавиша или сочетание клавиш	**Описание**
Клавиша со стрелкой вверх	Повторно вызывает команды из буфера истории, начиная с самой последней выполненной команды. Более ранние команды вызываются повторным нажатием клавиши соответствующее число раз
Клавиша со стрелкой вниз	Возвращает к последним командам из буфера после использования повторного вызова команд клавишей со стрелкой вверх. Более поздние команды вызываются повторным нажатием клавиши соответствующее число раз.

Ctrl+A	Перемещение курсора в начало командной строки
Ctrl+E	Перемещение курсора в конец командной строки
Ctrl+W	Удалить последнюю введенную команду
Ctrl+Z/End	Возврат в режим EXEC из любого другого режима
Клавиша возврата (backspace)	Перемещение курсора на одну позицию назад

В данном руководстве детально описано управление коммутатором с помощью Интерфейса командной строки (ИКС).

2. Команды для выбора режима интерфейса командной строки

Как описано ранее, ИКС содержит несколько командных режимов, каждый из которых имеет собственный характерный набор команд. Для перехода из одного режима в другой используются специальные команды.

В таблице показано состояние строки ввода команд при входе в каждый режим ИКС.

Состояние строки ввода команд в режимах ИКС

Режим ИКС	**Строка ввода команд**
Пользовательский режим (*User EXEC*)	`console>`
Привилегированный режим (*Privileged EXEC*)	`console#`
Режим Общей настройки (*Global Configuration*)	`console(config)#`
Режим Настройки интерфейсов (*Interface Configuration*)	`console(config-if)#`
Режим Настройки соединения (*Line Configuration*)	`console(config-line)#`
Режим конфигурирования VLAN (*VLAN DataBASE*)	`console(config-vlan)#`
Режим Настройки IP-интерфейсов	`console(config-ip)#`
Режим настройки Списков контроля доступа для управления (*Management Access List*)	`console(config-macl)#`
Режим настройки Списков контроля доступа по IP-адресу	`console(config-ip-al)#`
Режим настройки Списков контроля доступа по MAC-адресу	`console(config-mac-al)#`
Режим настройки Последовательности открытых ключей SSH (SSH Public Key-Chain)	`console(config-pubkey-chain)#`

2.1 Базовые команды, доступные во всех режимах ИКС

Далее описаны базовые команды, которые можно использовать во всех режимах ИКС.

do – выполнение команды пользовательского режима *User EXEC* из любого режима конфигурирования.

help – вывод справочной информации по используемым командам.

2.2 Команды для управления Пользовательским режимом User EXEC

После загрузки системы и ввода имени пользователя и пароля по умолчанию доступен Пользовательский режим *User EXEC*. Далее рассмотрены команды, использующиеся для входа в данный режим и выхода из него.

`login` – завершение текущей сессии пользовательского режима и смена пользователя.

`exit` – завершение активной терминальной сессии пользовательского режима.

2.3 Команды для управления Привилегированным режимом Privileged EXEC

Далее рассмотрены команды, использующиеся для входа в Привилегированный режим *Privileged EXEC* и выхода из него.

`enable` [*`privilege-level`*] – вход в Привилегированный режим с уровнем привилегий *`privilege-level`*, который может принимать значения от 1 до 15. Наивысшему уровню привилегий соответствует значение 15, низшему уровню соответствует 1. По умолчанию уровень привилегий равен 15.

`disable` [*`privilege-level`*] – выход из Привилегированного режима с уровнем привилегий *`privilege-level`* в Пользовательский режим. Наивысшему уровню привилегий соответствует значение 15, низшему уровню соответствует 1. По умолчанию уровень привилегий равен 1.

`show privilege` – отображение уровня привилегий текущего пользователя.

`debug-mode` – переход в Режим отладки *Debug Mode.*

2.4 Команды для управления режимом Общей настройки Global Configuration

Далее рассмотрены команды, использующиеся для входа в режим Общей настройки *Global Configuration* и выхода из него.

`configure`[*`terminal`*] – переход в режим конфигурирования терминала *`terminal`*.

`exit` – выход из любого режима конфигурирования на следующий ближайший уровень в иерархии режимов ИКС.

`end` – выход из любого режима конфигурирования в Привилегированный режим *Privileged EXEC.*

3. Создание новых пользователей, настройка подключений к системе

3.1 Создание новых учетных записей пользователей системы

По умолчанию в системе присутствует одна учетная запись привилегированного пользователя *admin* с пустым паролем и максимальным уровнем привилегий - 15. При первом включении коммутатора по умолчанию загружается сессия указанной учетной записи. Далее можно создать других пользователей и задать им уровни привилегий и пароли.

Внимание: после первой загрузки системы рекомендуется установить пароль пользователю *admin* для обеспечения защищенного входа под данной учетной записью в дальнейшем. Сразу после создания первого пользователя учетная запись автоматически *admin* удаляется.

Имя пользователя и пароль вводятся при входе в систему во время сеансов администрирования устройства. Для создания нового пользователя или настройки его параметров (имя пользователя, пароль, уровень привилегий) используется следующая команда привилегированного режима:

username

Синтаксис:
username *name* **password** *password* **privilege** {*privilege level*}

Параметры:

- *name* – имя создаваемого пользователя,
- *password* – пароль,
- *privilege level* – уровень привилегий (1-15).

Примечание: Уровень привилегий 1 является низшим и открывает доступ к коммутатору без права его настройки. Уровень привилегий 15 является наивысшим и дает право настройки всех параметров коммутатора.

Далее приведен пример создания пользователя *user1* с паролем *123* и уровнем привилегий *1*:

```
console# configure
console(config)# username user1 password 123 privilege 1
console (config)# exit
console#
```

3.2 Настройка локального и удаленного подключения к системе

Управление коммутатором можно производить, подключившись к нему локально или удаленно. Для локальной настройки системы предусмотрено подключение как через консольный порт RS-232, так и через *Management Port*, в качестве которого может быть назначен один из нисходящих портов. Назначение одного из портов на роль управляющего (*Management Port*), настройка его параметров и правил доступа к нему производится в режиме локального подключения к консоли коммутатора через интерфейс RS-232.

Для удаленного управления системой предусмотрены следующие виды подключений:

- подключение к удаленной консоли по протоколу *Telnet*,
- подключение к удаленной защищенной консоли по протоколу *SSH*,
- подключение к Графическому интерфейсу по протоколу *HTTP*,
- подключение к Графическому интерфейсу по защищенному протоколу *HTTPS* с использованием протокола *SSL*.

Далее описаны команды, использующиеся для настройки параметров локальной и удаленной консоли.

`line`

Команда используется для выбора терминала для его настройки и входа в режим его конфигурирования.

Синтаксис:
`line` {*`console | telnet | ssh`*}

Параметры:

- *`console`* – локальная консоль,
- *`telnet`* – удаленная консоль (*Telnet*),
- *`ssh`* – защищенная удаленная консоль.

Режим ИКС:
Режим Общей настройки

`speed`

Команда устанавливает скорость доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли). Использование префикса **`no`** сбрасывает скорость до значения по умолчанию.

Синтаксис:
`speed` *`bps`*
`no speed`

Параметры:

- *`bps`* – скорость доступа в битах в секунду (бодах). Возможные значения: 2400, 4800, 9600, 19200, 38400, 57600, 115200 бит/с (бод).

Состояние по умолчанию:
115200 бит/с

Режим ИКС:
Режим Настройки соединения

`autobaud`

Команда включает автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли). Использование префикса **`no`** выключает автоматическое определение скорости доступа по локальной консоли.

Синтаксис:
autobaud
no autobaud

Состояние по умолчанию:
Автоматическое определение скорости доступа по локальной консоли выключено.

Режим ИКС:
Режим Настройки соединения

exec-timeout

Команда задает время, в течение которого система ожидает ввода символов пользователем. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:
exec-timeout *minutes* [*seconds*]
no exec-timeout

Параметры:
- *minutes* – количество минут (диапазон 0-65535),
- *seconds* – количество секунд (диапазон 0-59).

Состояние по умолчанию:
10 минут

Режим ИКС:
Режим Настройки соединения

Пояснения:
Чтобы снять какие-либо ограничения на время ожидания ввода символов, необходимо установить значения параметров *0 0*.

Пример:
В следующем примере показана настройка терминала удаленной консоли с установкой скорости доступа 115200 бод, включением ее автоматического определения и установкой времени ожидания ввода символов 15 минут.

```
console# configure
console(config)# line telnet
console(config-line)# speed 115200
console(config-line)# autobaud
console(config-line)# exec-timeout 15
```

show line

Команда отображает настройки терминала.

Синтаксис:
show line [*console* | *telnet* | *ssh*]

Параметры:

- *console* – локальная консоль,
- *telnet* – удаленная консоль (*Telnet*),
- *ssh* – защищенная удаленная консоль.

Состояние по умолчанию:
Если параметры не заданы, то отображаются настройки всех терминалов.

Режим ИКС:
Пользовательский режим

ip telnet server

Команда включает поддержку сервера Telnet и разрешает удаленное конфигурирование устройства по протоколу Telnet. Использование префикса **no** отключает удаленный доступ к устройству по протоколу Telnet.

Синтаксис:
ip telnet server
no ip telnet server

Состояние по умолчанию:
Удаленный доступ к устройству по протоколу Telnet отключен.

Режим ИКС:
Режим Общей настройки

ip ssh server

Команда включает поддержку сервера SSH и разрешает удаленное конфигурирование устройства по защищенному протоколу SSH. Использование префикса **no** отключает удаленный достауп к устройству по протоколу SSH.

Синтаксис:
ip ssh server
no ip ssh server

Состояние по умолчанию:
Удаленный доступ к устройству по протоколу SSH отключен.

Режим ИКС:
Режим Общей настройки

Пояснения:
Для генерации частного и публичного ключей сервера SSH необходимо использовать команды **crypto key generate dsa** и **crypto key generate rsa**.

ip ssh port

Команда используется для назначения TCP-порта, который используется сервером SSH. Использование префикса **no** возвращает номер порта по умолчанию.

Синтаксис:
ip ssh port *port-number*

no ip ssh port

Параметры:
port-number – номер TCP-порта для SSH-сервера (диапазон 1-65535).

Состояние по умолчанию:
Номер TCP-порта по умолчанию: 22

Режим ИКС:
Режим Общей настройки

show ip ssh

Команда используется для отображения текущей конфигурации SSH-сервера.

Синтаксис:
show ip ssh

Режим ИКС:
Привилегированный режим

3.3 Настройка доступа к графическому пользовательскому интерфейсу

Далее описаны команды для включения и настройки удаленного доступа к управлению коммутатором через русифицированный графический пользовательский интерфейс.

ip http server

Команда включает управление коммутатором и просмотр его состояния через графический пользовательский интерфейс. Использование префикса **no** отключает данную функцию.

Синтаксис:
ip http server
no ip http server

Состояние по умолчанию:
Web-интерфейс включен

Режим ИКС:
Режим Общей настройки

ip http port

Команда используется для назначения TCP-порта для подключения через графический пользовательский интерфейс. Использование префикса **no** возвращает номер порта по умолчанию.

Синтаксис:
ip http port *port-number*
no ip http port

Параметры:
port-number – номер TCP-порта для HTTP-сервера (диапазон 1-65535).

Состояние по умолчанию:
Номер TCP-порта по умолчанию: 80

Режим ИКС:
Режим Общей настройки

ip http timeout-policy

Команда устанавливает интервал ожидания при использовании Web-интерфейса, после которого происходит автоматическое завершение сессии пользователя. Использование префикса **no** устанавливает значение интервала ожидания по умолчанию.

Синтаксис:
ip http timeout-policy *seconds*
no ip http timeout-policy

Параметры:
seconds – значение интервала ожидания в секундах (диапазон 0-86400).

Состояние по умолчанию:
600 секунд

Режим ИКС:
Режим Общей настройки

Пояснения:
Данная команда также устанавливает интервал ожидания для защищенного подключения к Web-интерфейсу по протоколу HTTPS.

ip http secure-server

Команда включает управление коммутатором и просмотр его состояния через защищенное подключение к Web-интерфейсу. Использование префикса no отключает данную функцию.

Синтаксис:
ip http secure-server
no ip http secure-server

Состояние по умолчанию:
Защищенное подключение не используется

Режим ИКС:
Режим Общей настройки

ip http secure-port

Команда используется для назначения TCP-порта для защищенного подключения к графическому пользовательскому интерфейсу. Использование префикса no возвращает номер порта по умолчанию.

Синтаксис:
ip http secure-port port-number
no ip http secure-port

Параметры:
`port-number – номер` TCP-порта для HTTPS-сервера (диапазон 1-65535)

Состояние по умолчанию:
Номер TCP-порта по умолчанию: 443

Режим ИКС:
Режим Общей настройки

`ip https certificate`
Команда используется для выбора активного сертификата для протокола HTTPS. Использование префикса no возвращает номер активного сертификата по умолчанию.

Синтаксис:
`ip https certificate number`
`no ip https certificate`

Параметры:
`number – номер сертификата` (1-2)

Состояние по умолчанию:
Номер сертификата по умолчанию: 1

Режим ИКС:
Режим Общей настройки

Пояснения:
Для генерации сертификата HTTPS необходимо использовать команду crypto certificate number generate.

`show ip http`
Команда используется для отображения текущей конфигурации HTTP-сервера.

Синтаксис:
`show ip http`

Режим ИКС:
Привилегированный режим

`show ip https`
Команда используется для отображения текущей конфигурации HTTPS-сервера.

Синтаксис:
`show ip https`

Режим ИКС:
Привилегированный режим

4. Контроль загрузки ресурсов и системных параметров коммутатора

В данном разделе описаны команды, с помощью которых можно просмотреть загрузку ресурсов устройства, существующих пользователей и их активных сессий, а также отобразить данные о встроенном ПО и других системных параметрах.

`service cpu-utilization`

Команда включает измерение уровня загрузки ресурсов центрального процессора коммутатора. Использование префикса **`no`** отключает измерение указанных ресурсов.

Синтаксис:
```
service cpu-utilization
no service cpu-utilization
```

Состояние по умолчанию:
Измерение уровня загрузки ресурсов центрального процессора отключено.

Режим ИКС:
Режим Общей настройки

Пояснения:
Для просмотра уровня загрузки ресурсов центрального процессора используйте команду **`show cpu utilization`** привилегированного режима.

`show cpu utilization`

Команда отображает статистику по уровню загрузки ресурсов центрального процессора.

Синтаксис:
```
show cpu utilization
```

Режим ИКС:
Привилегированный режим

Пояснения:
Для включения измерения уровня загрузки ресурсов центрального процессора используйте команду **`show cpu utilization`** Режима Общей настройки.

`clear cpu counters`

Команда обнуляет счетчики пакетов, проходящих через центральный процессор.

Синтаксис:
```
clear cpu counters
```

Режим ИКС:
Пользовательский режим

`service cpu-counters`

Команда включает счетчики пакетов, проходящих через центральный процессор. Использование префикса **no** отключает указанные счетчики.

Синтаксис:
service cpu-counters
no service cpu-counters

Режим ИКС:
Режим Общей настройки

Пояснения:
Для отображения счетчиков пакетов, проходящих через центральный процессор, используйте команду **show cpu counters** Пользовательского режима.

show cpu counters

Команда позволяет просмотреть счетчики пакетов центрального процессора.

Синтаксис:
show cpu counters

Режим ИКС:
Пользовательский режим

Пояснения:
Для включения счетчиков пакетов, проходящих через центральный процессор, используйте команду **service cpu-counters** Режима Общей настройки.

show users

Команда отображает информацию об активных пользователях.

Синтаксис:
show users

Режим ИКС:
Пользовательский режим

show sessions

Команда отображает информацию об открытых TELNET-сессиях к удаленным устройствам.

Синтаксис:
show sessions

Режим ИКС:
Пользовательский режим

Пояснения:
Команда отображает TELNET-подключения к удаленным устройствам, открытые текущей TELNET-сессией к локальному устройству. Она не отображает TELNET-подключения к удаленным устройствам, открытые другими TELNET-сессиями к локальному устройству.

show system

Команда отображает системную информацию о коммутаторе.

Синтаксис:
show system [**unit** *unit*]

Параметры:
unit – номер устройства в стеке (диапазон 1-8). Для коммутатора, работающего в автономном режиме, параметр не используется.

Режим ИКС:
Пользовательский режим

show system defaults

Команда отображает заводские настройки системы.

Синтаксис:
show system defaults [{**management** | **ipv6** | **802.1x** | **port** | **fdb** | **multicast** | **port-mirroring** | **spanning-tree** | **vlan** | **voice-vlan** | **network-security** | **dos-attacks** | **ip-addressing** | **qos-acl**}]

Параметры:
Ввод каждого из параметров указывает на отображение только соответствующих настроек.

Режим ИКС:
Привилегированный режим

show version

Команда отображает информацию о версии системного ПО, загрузочного ПО и аппаратного обеспечения устройства.

Синтаксис:
show version [**unit** *unit*]

Параметры:
unit – номер устройства в стеке (диапазон 1-8). Для коммутатора, работающего в автономном режиме, параметр не используется.

Режим ИКС:
Пользовательский режим

show version md5

Команда отображает MD5-дайджест программного обеспечения устройства.

Синтаксис:
show version md5 [unit unit]

Параметры:
unit – номер устройства в стеке (диапазон 1-8). Для коммутатора, работающего в автономном режиме, параметр не используется.

Режим ИКС:
Пользовательский режим

show system tcam utilization

Команда отображает загрузку ресурсов памяти TCAM (Ternary Content Addressable Memory - троичная ассоциативная память).

Синтаксис:
show system tcam utilization [**unit** *unit*]

Параметры:
– *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется).

Режим ИКС:
Пользовательский режим

show switch

Команда отображает информацию о состоянии стека или устройства в стеке.

Синтаксис:
show switch [*stack-member-number*]

Параметры:
– *stack-member-number* – номер устройства в стеке (диапазон 1-8).

Режим ИКС:
Пользовательский режим

Пояснения:
Команда активна только для устройства, работающего в режиме стекирования.

show interfaces

Команда используется для отображения сводной информации о текущем состоянии выбранного интерфейса или группы интерфейсов устройства.

Синтаксис:
show interfaces [*interface-id*]

Параметры:
– *interface-id* – номер интерфейса, информацию о котором необходимо отобразить.

Состояние по умолчанию:
Без указания номера интерфейса отображается сводная информация о текущем состоянии всех интерфейсов устройства.

Режим ИКС:
Пользовательский режим

Пояснения:
Для отображения сведений о средней скорости и пропускной способности интерфейса следует настроить для него параметры удаленного мониторинга на основе RMON с помощью команды **`rmon collection stats`**. По умолчанию функция сбора статистики RMON отключена.
Для отображения информации о Ethernet-параметрах выбранного интерфейса или всех интерфейсов устройства можно использовать команду **`show interfaces configuration`**.
Для отображения краткой информации о текущем состоянии выбранного интерфейса или всех интерфейсов устройства можно использовать команду **`show interfaces status`**.

5. Настройка времени, даты и других системных параметров

5.1 Настройка системного времени и даты

Система поддерживает установку системного времени и даты как вручную, так и в автоматическом режиме. Во втором случае пользователь может задать параметры подключения к одному или нескольким серверам времени, с которыми будет осуществляться синхронизация по протоколу SNTP. В системе реализована поддержка протокола SNTP v.4 в соответствии с документом RFC2030.

Если в системе определено несколько серверов времени, то один из них определяется в качестве «назначенного сервера». Им автоматически становится сервер с наименьшей ступенью (stratum) в иерархии эталонов времени. В случае, когда таковых оказывается несколько, то «назначенным сервером» выбирается тот из них, от которого раньше всего поступит временной пакет.

Если не обнаруживается ни один серверов времени, то система продолжает производить опрос подключенных устройств с заданным интервалом (poll interval). Коммутатор поддерживает назначение выбранных серверов времени доверенными, при этом только они могут быть источниками синхронизации. Для подключения к таким серверам можно настроить защищенное соединение.

Далее описаны команды, использующиеся для установки, изменения и просмотра системного времени и даты.

show clock

Команда отображает системное время и дату.

Синтаксис:
show clock [*detail*]

Параметры:
- *detail* – отображает параметры часового пояса и перехода на летнее время.

Режим ИКС:
Пользовательский режим

clock timezone

Команда устанавливает значение часового пояса. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:
clock timezone *zone hours-offset* [**minutes** *minutes-offset*]
no clock timezone

Параметры:
- *zone* – сокращенное описание часового пояса (от 1 до 4 символов),
- *hours-offset* – часовое смещение относительно нулевого меридиана UTC (от -12 до +13),

– *minutes-offset* – минутное смещение относительно нулевого меридиана UTC (от 0 до 59).

Состояние по умолчанию:
Нет описания часового пояса, часовое смещение – 0, минутное смещение – 0.

Режим ИКС:
Режим Общей настройки

clock summer-time

Команда используется для настройки автоматического перехода на летнее время. Использование префикса **no** отключает автоматический переход на летнее время.

Синтаксис:
clock summer-time *zone* **recurring** {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}}[*offset*]
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* [*offset*]
no clock summer-time

Параметры:
– *zone* – сокращенное описание часового пояса (от 1 до 4 символов),
– **recurring** – указывает на то, что начало и окончание летнего времени должны происходить в соответствующие дни ежегодно,
– **usa** – установить правила перехода на летнее время, используемые в США (переход во второе воскресенье марта, обратно в первое воскресенье ноября, в 2 часа утра по местному времени),
– **eu** – установить правила перехода на летнее время, используемые Евросоюзом (переход в последнее воскресенье марта, обратно в последнее воскресенье октября, в 1 час утра по Гринвичу),
– *week* – неделя месяца (может принимать значения: 1-4, первая, последняя),
– *day* – день недели (mon-sun),
– *month* – месяц (Jan-Dec),
– *hh:mm* – часы (0-23) и минуты (0-59),
– *offset* – количество добавляемых минут при переходе на летнее время (1-1440). По умолчанию – 60,
– **date** – указывает на то, что начало и окончание летнего времени должны происходить в соответствующие дни заданного года,
– *date* – день месяца (1-31),
– *year* – год (2000-2097).

Состояние по умолчанию:
Автоматический переход на летнее время отключено.

Режим ИКС:
Режим Общей настройки

Пояснения:

Во всех вариантах использования команды первая дата определяет начало летнего времени, а вторая – его окончание. Дата начала задается по стандартному времени, дата окончания – по летнему времени. Если месяц начала летнего времени хронологически находится после месяца окончания, то предполагается, что коммутатор используется в южном полушарии земного шара, поэтому сообщения об ошибке не появляется.

clock source

Команда включает использование внешнего источника для установки системного времени. Использование префикса **no** отключает использование внешнего источника времени.

Синтаксис:
clock source {**sntp**}
no clock source

Параметры:
- **sntp** – указывает, что SNTP-сервер является внешним источником для установки времени.

Состояние по умолчанию:
Внешний источник не используется.

Режим ИКС:
Режим Общей настройки

clock dhcp timezone

Команда разрешает получение данных о часовом поясе и переходе на летнее время от DHCP-сервера. Использование префикса **no** отключает получение указанных данных от DHCP-сервера.

Синтаксис:
clock dhcp timezone
no clock dhcp timezone

Состояние по умолчанию:
Использование DHCP-сервера для получения данных о часовом поясе и переходе на летнее время отключено.

Режим ИКС:
Режим Общей настройки

Пояснения:
Данные о часовом поясе и переходе на летнее время, полученные от DHCP-сервера, имеют приоритет над их установкой вручную. Они сохраняются после завершения периода аренды IP-адреса. Указанные данные обнуляются после перезагрузки системы.

sntp server

Команда задает адрес SNTP-сервера, который будет использоваться для синхронизации системного времени. Использование префикса **no** удаляет выбранный сервер из списка SNTP-серверов.

Синтаксис:
sntp server {*ipv4-address* | *ipv6-address* | *ipv6z-address* | *hostname*} [**poll**] [**key** *keyid*]
no sntp server {*ipv4-address* | *ipv6-address* | *ipv6z-address* | *hostname*}

Параметры:
- *ipv4-address* – IP-адрес сервера в формате IPv4,
- *ipv6-address* – IP-адрес сервера в формате IPv6,
- *ipv6z-address* – IP-адрес сервера в формате IPv6Z для команды `ping`. Формат IPv6Z-адреса: `{ipv6-link-local-address}%{interface-name}`, где:
  - `ipv6-link-local-address` – локальный IPv6 адрес канала,
  - `interface-name` – имя исходящего интерфейса, задается в следующем формате: `vlan {integer} | ch {integer} | isatap {integer} | {physicalport-name}`,
- *hostname* – доменное имя сервера (до 158 символов),
- **poll** – включает опрос,
- **key** – включает использования ключа аутентификации,
- *keyid* – идентификатор ключа (диапазон от 0 до 4294967295).

Состояние по умолчанию:
SNTP-серверы не заданы.

Режим ИКС:
Режим Общей настройки

Пояснения:
Система поддерживает до 8 SNTP-серверов.

sntp port

Команда задает UDP-порт SNTP-сервера. Использование префикса **no** устанавливает значение по умолчанию UDP-порт.

Синтаксис:
sntp port *port-number*
no sntp port

Параметры:
- *port-number* – номер UDP-порта SNTP-сервера (диапазон от 1 до 65535).

Состояние по умолчанию:
Номер UDP-порта SNTP-сервера по умолчанию – 123.

Режим ИКС:
Режим Общей настройки

show sntp configuration

Команда отображает конфигурацию протокола SNTP.

Синтаксис:
show sntp configuration

Режим ИКС:
Привилегированный режим

show sntp status

Команда отображает текущее состояние SNTP-серверов.

Синтаксис:
show sntp status

Режим ИКС:
Привилегированный режим

sntp client enable

Команда включает на выбранном интерфейсе SNTP-клиент, поддерживающий метод широковещательной (broadcast) рассылки пакетов и отправки их ближайшему устройству из группы получателей (anycast). Использование префикса **no** отключает на выбранном интерфейсе SNTP-клиент.

Синтаксис:
sntp client enable {**oob** |**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*| **vlan** *vlanID*}
no sntp client enable {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*| **vlan** *vlanID*}

Параметры:

- *oob* – порт управления
- *gi_port* – номер одногигового порта (1-24),
- *te _port* – номер десятигигового порта (1,2),
- *group* – номер группы агрегированных каналов (1-8),
- *vlanID* – номер виртуальной сети VLAN (1-4094).

Состояние по умолчанию:
SNTP-клиент на интерфейсе отключен.

Режим ИКС:
Режим Общей настройки

Пояснения:
После входа в Режим Настройки выбранного интерфейса (группы агрегированных каналов, виртуальной сети VLAN) данную команду можно использовать без указания параметров.
Для включения (отключения) одноадресных SNTP-клиентов используется команда:
(no) sntp unicast client enable.
Для включения (отключения) SNTP-клиентов, посылающих пакеты ближайшему устройству из группы получателей, используется команда:
(no) sntp anycast client enable.
Для включения (отключения) широковещательных SNTP-клиентов используется команда:
(no) sntp broadcast client enable.

sntp unicast client poll

Команда включает последовательный опрос заданных одноадресных SNTP-клиентов. Использование префикса **no** отключает опрос SNTP-клиентов.

Синтаксис:
sntp unicast client poll
no sntp unicast client poll

Состояние по умолчанию:
Опрос SNTP-клиентов отключен.

Режим ИКС:
Режим Общей настройки

sntp client poll timer

Команда устанавливает время опроса для SNTP-клиента. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:
sntp client poll timer *seconds*
no sntp client poll timer

Параметры:
– *seconds* – интервал опроса в секундах (60-86400).

Состояние по умолчанию:
Интервал опроса – 1024 секунды.

Режим ИКС:
Режим Общей настройки

sntp authentication-key

Команда устанавливает ключ проверки подлинности для протокола SNTP. Использование префикса **no** удаляет указанный ключ.

Синтаксис:
sntp authentication-key *key-number* **md5** *key-value*
no sntp authentication-key *key-number*

Параметры:
– *key-number* – номер ключа (1–4294967295),
– *key-value* – значение ключа(от 1 до 8 символов).

Состояние по умолчанию:
Проверка подлинности отключена.

Режим ИКС:
Режим Общей настройки

sntp authenticate

Команда включает проверку подлинности для SNTP-трафика, полученного от серверов. Использование префикса **no** отключает указанную проверку.

Синтаксис:
sntp authenticate
no sntp authenticate

Состояние по умолчанию:
Проверка подлинности отключена.

Режим ИКС:
Режим Общей настройки

sntp trusted-key

Команда осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. Использование префикса **no** отключает указанную проверку подлинности.

Синтаксис:
sntp trusted-key *key-number*
no sntp trusted-key *key-number*

Параметры:
key-number – номер проверяемого ключа (1–4294967295)

Состояние по умолчанию:
Проверка подлинности отключена.

Режим ИКС:
Режим Общей настройки

5.2 Базовые команды управления системой

Далее описаны базовые управляющие команды для формирования ICMP-запросов, определения маршрута трафика, установки имени системы, ее перезагрузки и т.д.

ping

Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети и для контроля поступающих ответов (ICMP Echo-Reply).

Синтаксис:
ping [**ip**] {*ipv4-address*|*hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

ping ipv6 {*ipv6-address*|*hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

Параметры:
– **ip** – для передачи запросов используется протокол IPv4,

- **ipv6** – для передачи запросов используется протокол IPv6,
- *ipv4-address* – IPv4-адрес узла сети,
- *ipv6-address* – IPv6-адрес узла сети,
- *hostname* – доменное имя узла сети (от 1 до 160 символов),
- *packet_size* – количество байт в пакете, включая тэг VLAN (64-1518), по умолчанию – 64 байт,
- *packet_count* – количество пакетов для передачи (0-65535), по умолчанию – 4 пакета. Если выбрать значение 0, то пакеты будут отправляться до принудительной остановки процесса,
- *time_out* – время ожидания ответа на каждый запрос в миллисекундах (50-65535), по умолчанию – 2000 миллисекунд.

Режим ИКС:
Пользовательский режим

Пояснения:
Для остановки передачи пакетов нажмите <**Esc**>.

traceroute

Команда служит для определения маршрута трафика до узла назначения.

Синтаксис:
traceroute ip {*ipv4-address*|*hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]

traceroute ipv6 {*ipv4-address*|*hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]

Параметры:
- **ip** – для определения маршрута используется протокол IPv4,
- **ipv6** – для определения маршрута используется протокол IPv6,
- *ipv4-address* – IPv4-адрес узла сети,
- *ipv6-address* – IPv6-адрес узла сети,
- *hostname* – доменное имя узла сети (от 1 до 160 символов),
- *packet_size* – количество байт в пакете (64-1518), по умолчанию – 64 байт,
- *max-ttl* – максимальное время жизни пакета (1-255), по умолчанию – 30,
- *packet_count* – количество попыток передачи пакета на каждом участке (1-10), по умолчанию – 3,
- *time_out* – время ожидания ответа на запрос в секундах (1-60), по умолчанию – 3,
- *ip-address* – IP-адрес интерфейса коммутатора, используемый для передачи пакетов,
- *tos* – тип сервиса, передаваемый в заголовке протокола IP (0-255).

Режим ИКС:
Пользовательский режим

Пояснения:
Команда отправляет запросы и строит маршрут путем определения времени прибытия на каждый участок маршрута до тех пор, пока не достигнет узла назначения или не истечет

время жизни пакета TTL. Кроме того, процесс определения маршрута остановится при нажатии клавиши <**Esc**>.

В таблице 5.1 описаны ошибки, которые могут появляться при выполнении команды.

Таблица 5.1. Описание ошибок команды `traceroute`

Символ ошибки	**Описание**
*	Таймаут при попытке передачи пакета
?	Неизвестный тип пакета
A	Административно недоступен. Обычно происходит при блокировании исходящего трафика по правилам в таблице доступа ACL
F	Требуется фрагментация и установка битов DF
H	Узел сети недоступен
N	Сеть недоступна
P	Протокол недоступен
Q	Источник подавлен
R	Истекло время повторной сборки фрагмента
S	Ошибка исходящего маршрута
U	Порт недоступен

`telnet`

Команда используется для подключения к устройству, которое поддерживает соединение по протоколу Telnet.

Синтаксис:
`telnet` {*`ip-address`* | *`hostname`*} [*`port`*] [*`keyword ...`*]

Параметры:
- *`ip-address`* – IP-адрес подключаемого устройства,
- *`hostname`* – доменное имя подключаемого устройства (от 1 до 160 символов),
- *`port`* – TCP-порт, по которому работает служба Telnet, по умолчанию – 23,
- *`keyword`* – ключевое слово или последовательность ключевых слов.

Режим ИКС:
Пользовательский режим

Пояснения:
Коммутатор поддерживает специальные Telnet-команды, которые выполняют функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш <**Ctrl-shift-6**>, после которой необходимо ввести соответствующий символ Telnet-команды. Получающиеся команды показаны в таблице 5.2. При этом нажатие указанной комбинации клавиш на экране отображается как «^^».

Специальные Telnet-команды

Команда	**Отображение на экране**	**Описание**
<Ctrl-shift-6> - b	`^^ b`	Передать по telnet разрыв соединения
<Ctrl-shift-6> - c	`^^ c`	Передать по telnet прерывание процесса (IP)
<Ctrl-shift-6> - h	`^^ h`	Передать по telnet удаление символа (EC)
<Ctrl-shift-6> - o	`^^ o`	Передать по telnet прекращение вывода (AO)
<Ctrl-shift-6> - t	`^^ t`	Передать по telnet сообщение «Are You There?» (AYT) для контроля подключения
<Ctrl-shift-6> - u	`^^ u`	Передать по telnet стирание строки (EL)
<Ctrl-shift-6> - x	`^^ x`	Возврат в режим командной строки

В таблице описаны ключевые слова, которые дополнительно можно использовать при открытии Telnet-сессии.

Ключевые слова при создании Telnet-сессии

Ключевое слово	**Описание**
`/echo`	Включение функци echo локально (без вывода на консоль)
`/quiet`	Запрет вывода всех сообщений службы Telnet
`/source-interface`	Интерфейс, являющийся источником
`/stream`	Включение обработки потока, который разрешает незащищенное TCP-соединение без контроля последовательностей Telnet. Потоковое соединение не обрабатывает Telnet-опции и может использоваться для подключения к портам, на которых запущены программы копирования UNIX-to-UNIX (UUCP) либо другие протоколы, не являющиеся Telnet-протоколами

`resume`

Команда используется для переключения на другую активную Telnet-сессию.

Синтаксис:
`resume` [*`connection`*]

Параметры:
– *`connection`* – номер активной Telnet-сессии (1-4)

Состояние по умолчанию:
Номер последней активной Telnet-сессии

Режим ИКС:

Пользовательский режим

hostname

Команда служит для установки или редактирования сетевого имени устройства. Использование префикса **no** удаляет существующее имя устройства.

Синтаксис:
hostname *name*
no hostname

Параметры:
– *name* – сетевое имя устройства (от 1 до 160 символов)

Состояние по умолчанию:
Сетевое имя устройства не определено.

Режим ИКС:
Режим Общей настройки

reload

Команда используется для перезагрузки устройства или стека устройств.

Синтаксис:
reload [**slot** *stack-member-number*]

Параметры:
– *stack-member-number* – номер устройства в стеке (1-8). Если в режиме стекирования указанный номер не задан, то перезагружается весь стек коммутаторов.

Режим ИКС:
Привилегированный режим

6. Использование буфера истории команд и журнала Syslog

6.1 Команды для работы с буфером истории команд

В интерфейсе командной строки реализован буфер истории команд, в котором хранятся до 207 последних команд, ранее введенных в течение текущей терминальной сессии. Этот буфер позволяет просмотреть действия, произведенные во время данного сеанса управления устройством, и повторно вызывать ранее веденные команды, не вводя их полностью заново.

Пользователь может отключить сохранение истории команд, а также установить необходимое количество сохраняемых в буфер команд. Далее описаны команды для настройки указанного буфера.

history

Команда включает функцию сохранения истории введенных команд. Использование префикса **no** отключает данную функцию.

Синтаксис:
history
no history

Состояние по умолчанию:
Функция сохранения истории введенных команд включена

Режим ИКС:
Режим Настройки соединения

Пояснения:
Данная команда включает/отключает функцию сохранения истории команд для конкретного вида подключения (console, telnet, SSH). Для включения/отключения данной функции для текущей терминальной сессии необходимо использовать команду **terminal history**.

history size

Команда устанавливает размер буфера истории введенных команд. Использование префикса **no** возвращает значение по умолчанию.

Синтаксис:
history size *number-of-commands*
no history size

Параметры:
– *number-of-commands* – количество команд, сохраняемых в буфере (10-197)

Состояние по умолчанию:
Размер буфера истории команд равен 10

Режим ИКС:
Режим Настройки соединения

Пояснения:
Данная команда задает размер буфера истории команд для конкретного вида подключения (console, telnet, SSH). Для установки размера буфера для текущей терминальной сессии необходимо использовать команду **`terminal history size`**.

`terminal history`

Команда включает функцию сохранения истории введенных команд для текущей терминальной сессии. Использование префикса **`no`** отключает данную функцию.

Синтаксис:
`history`
`no history`

Состояние по умолчанию:
Состояние по умолчанию данной функции для всех терминальных сессий определяется командой **`history`**.

Режим ИКС:
Пользовательский режим

`terminal history size`

Команда устанавливает размер буфера истории введенных команд для текущей терминальной сессии. Использование префикса **no** возвращает значение по умолчанию.

Синтаксис:
`terminal history size` *`number-of-commands`*
`no terminal history size`

Параметры:
– *`number-of-commands`* – количество команд, сохраняемых в буфере (10-207)

Состояние по умолчанию:
Значение по умолчанию данного параметра для всех терминальных сессий определяется командой **`history size`**.

Режим ИКС:
Пользовательский режим

`show history`

Команда отображает историю команд, введенных в текущей сессии управления устройством.

Синтаксис:
`show history`

Режим ИКС:
Пользовательский режим

Пояснения:
Буфер истории команд хранит как выполненные, так и не выполненные команда.

Команды отображаются в хронологической последовательности, начиная от самой ранней введенной команды.

Буфер продолжает работать при входе в режимы настройки и выходе из них.

6.2 Работа с системным журналом Syslog

В коммутаторе реализована поддержка регистрации событий с использованием протокола Syslog. Системный журнал позволяет вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся соответствующие сообщения о событиях, при этом каждое сообщение имеет свой уровень важности. В системе выделены события 8 типов важности, представленные в таблице 5.4 в порядке убывания их важности.

Типы сообщений журнала Syslog

Тип событий	**Условный номер**	**Сообщения**	**Описание**
`Emergencies`	нет	Чрезвычайные	Система функционирует неправильно
`Alerts`	1	Сигналы тревоги	Необходимо немедленное вмешательство в систему
`Critical`	2	Критические	В системе произошла критическая ошибка
`Errors`	3	Ошибки	В системе произошла ошибка
`Warnings`	4	Предупреждения	Предупреждение, неаварийное сообщение
`Notifications`	5	Уведомления	Уведомление системы, неаварийное сообщение
`Informational`	6	Информационные	Информационное сообщение системы
`Debugging`	7	Отладочные	Предоставляет пользователю информацию для корректной настройки системы

Система позволяет вести журнал регистрации событий как локально непосредственно на самом устройстве, так и использовать для этого внешний Syslog-сервер. При этом поддерживается подключение до 8 таких Syslog-серверов. В целом сообщения о событиях могут регистрироваться:

- на экране консоли (logging console),
- в буферной памяти коммутатора (logging bufer),
- в специальном файле, хранящемся в энергонезависимой памяти устройства (logging file),
- на внешнем Syslog-сервере (logging host).

Далее описаны команды, необходимые для работы с журналом Syslog для всех указанных вариантов его хранения.

logging on

Команда включает регистрацию отладочных сообщений и сообщений об ошибках. Использование префикса **no** отключает регистрацию указанных сообщений.

Синтаксис:
logging on
no logging on

Состояние по умолчанию:
Регистрация отладочных сообщений и сообщений об ошибках включена

Режим ИКС:
Режим Общей настройки

Пояснения:
Данная команда запускает процесс регистрации событий в целом, при этом для включения регистрации в конкретном журнале можно использовать соответствующие им команды, которые описаны ниже. Однако по команде **no logging on** отключается регистрация во всех журналах, за исключением вывода на консоль.

logging console

Команда включает вывод на консоль сообщений о событиях до выбранного уровня важности. Использование префикса **no** возвращает уровень важности по умолчанию.

Синтаксис:
logging console *level*
no logging console

Параметры:
– *level* – уровень важности регистрируемых событий. Возможные значения: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.

Состояние по умолчанию:
На консоль выводятся информационные сообщения (informational)

Режим ИКС:
Режим Общей настройки

logging buffered

Команда включает регистрацию сообщений о событиях до выбранного уровня важности во внутреннем буфере и устанавливает размер буфера. Использование префикса **no** отключает регистрацию сообщений во внутреннем буфере и возвращает для него уровень важности по умолчанию.

Синтаксис:
logging buffered [*buffer-size*] [*severity-level*]
no logging buffered

Параметры:
– *buffer-size* – максимальное число записываемых сообщений (20-400),

– *severity-level* – уровень важности регистрируемых событий. Возможные значения: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging. Уровень важности можно указать по условному номеру от 1 до 7, за исключением событий типа emergencies (см. таблицу 5.5).

Состояние по умолчанию:
Регистрируются информационные сообщения (informational)

Режим ИКС:
Режим Общей настройки

logging file

Команда включает регистрацию сообщений о событиях до выбранного уровня важности в файл журнала. Использование префикса **no** отключает регистрацию сообщений в файле журнала.

Синтаксис:
logging file *level*
no logging file

Параметры:
– *level* – уровень важности регистрируемых событий. Возможные значения: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.

Состояние по умолчанию:
Регистрируются сообщения об ошибках (errors)

Режим ИКС:
Режим Общей настройки

logging host

Команда включает передачу сообщений о событиях до выбранного уровня важности на удаленный Syslog-сервер. Использование префикса **no** удаляет сетевой узел с указанными параметрами из списка Syslog-серверов.

Синтаксис:
logging host {*address* | *hostname*} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]
no logging host {*address* | *hostname*}

Параметры:
– *address* – IP-адрес Syslog-сервера в формате IPv4 или IPv6,
– *hostname* – доменное имя Syslog-сервера (до 158 символов),
– *port* – номер UDP-порта для передачи сообщений по протоколу Syslog (1-65535, по умолчанию - 514),
– *level* – уровень важности регистрируемых событий. Возможные значения: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging,

- *facility* – параметр facility, передаваемый внутри сообщения. Возможные значения: local0, local1 , local2 , local3 , local4 , local5 , local 6, local7, по умолчанию - local7,
- *text* – текстовое описание Syslog-сервера (до 64 символов).

Состояние по умолчанию:
На внешние серверы Syslog сообщения не отправляются

Режим ИКС:
Режим Общей настройки

clear logging

Команда удаляет все сообщения из внутреннего буфера.

Синтаксис:
clear logging

Режим ИКС:
Привилегированный режим

clear logging file

Команда удаляет все сообщения из журнала файла.

Синтаксис:
clear logging file

Режим ИКС:
Привилегированный режим

show logging

Команда отображает состояние журнала и сообщения, записанные во внутреннем буфере.

Синтаксис:
show logging

Режим ИКС:
Привилегированный режим

show logging file

Команда отображает состояние журнала и сообщения, записанные в файле журнала.

Синтаксис:
show logging file

Режим ИКС:
Привилегированный режим

show syslog-servers

Команда отображает текущие настройки для удалённых Syslog-серверов.

Синтаксис:

show syslog-servers

Режим ИКС:
Привилегированный режим

aaa logging login

Команда включает регистрацию в журнале событий аутентификации, авторизации и учета (AAA). Использование префикса **no** отключает регистрацию указанных событий.

Синтаксис:
aaa logging login
no aaa logging login

Состояние по умолчанию:
Регистрация событий аутентификации, авторизации и учета (AAA) включена

Режим ИКС:
Режим Общей настройки

Пояснения:
Данная команда включает запись сообщений об успешной и не успешной аутентификации пользователей, а также другие событий, связанных с аутентификацией и авторизацией.

file-system logging

Команда включает регистрацию событий файловой системы. Использование префикса **no** отключает регистрацию событий файловой системы.

Синтаксис:
file-system logging {**copy** | **delete-rename**}
no file-system logging {**copy** | **delete-rename**}

Параметры:
- **copy** – регистрация сообщений, связанных с операциями копирования файлов,
- **delete-rename** – регистрация сообщений, связанных с операциями удаления и переименования файлов.

Состояние по умолчанию:
Регистрация событий файловой системы включена

Режим ИКС:
Режим Общей настройки

management logging deny

Команда включает регистрацию срабатывания правил, запрещающих доступ к управлению системой на основе списков контроля доступа по управлению (Management ACL). Использование префикса **no** отключает регистрацию срабатывания указанных правил.

Синтаксис:
management logging deny
no management logging deny

Параметры:
- **copy** – регистрация сообщений, связанных с операциями копирования файлов,
- **delete-rename** – регистрация сообщений, связанных с операциями удаления и переименования файлов.

Состояние по умолчанию:
Регистрация событий файловой системы включена

Режим ИКС:
Режим Общей настройки

logging aggregation on

Команда включает агрегацию Syslog-сообщений. Использование префикса **no** отключает агрегацию Syslog-сообщений.

Синтаксис:
logging aggregation on
no logging aggregation on

Состояние по умолчанию:
Агрегация сообщений отключена

Режим ИКС:
Режим Общей настройки

logging aggregation aging-time

Команда устанавливает время хранения сгруппированных Syslog-сообщений. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:
logging aggregation aging-time *sec*
no logging aggregation aging-time

Параметры:
- *sec* – время хранения сгруппированных сообщений в секундах (15-3600)

Состояние по умолчанию:
Время хранения сгруппированных сообщений равно 300 секунд.

Режим ИКС:
Режим Общей настройки

7. Работа с программным обеспечением и конфигурацией

7.1 Принцип хранения системного программного обеспечения

Исполняемое и загрузочное программное обеспечение, а также все настройки системы хранятся в виде файлов, расположенных во встроенной энергонезависимой памяти коммутатора. Система поддерживает загрузку и выгрузку указанных файлов, их резервное копирование, обновление, удаление и ряд других операций, необходимых для работы со встроенным программным обеспечением и настройками устройства.

Исполняемое программное обеспечение хранится в виде единого файла, представляющего собой образ ПО. При этом для обеспечения восстановления в энергонезависимой памяти устройства всегда хранятся 2 экземпляра, один из которых является активным и загружается при старте системы, а второй хранится в виде резервной копии. Если при старте системы образ, назначенный активным, по какой-либо причине не загружается, то система автоматически переключится на резервный образ с отправкой соответствующего сообщения в журнал регистрации событий Syslog.

Оба образа исполняемого ПО хранятся в энергонезависимой памяти в заархивированном виде, откуда один из них распаковывается в оперативную память при старте системы. Пользователь может переназначить активный образ в процессе работы устройства, при этом настройка вступит в силу после перезапуска системы. При обновлении ПО перед загрузкой новой версии производится его автоматическая проверка на целостность и правильность формата, после чего запускается загрузка, по завершении которой обновленный образ становится неактивным. После назначения его активным образом и перезагрузки коммутатора старый образ сохраняется в памяти в виде резервной копии, на которую можно вернуться в случае наличия ошибок в новой версии. Обновление системного ПО можно производить с помощью протоколов TFTP, HTTP или X-modem через последовательный интерфейс.

В режиме стекирования пользователь может скопировать образ с памяти «ведущего» устройства в память любого «ведомого» или на все «ведомые» одновременно.

7.2 Принцип хранения загрузочного программного обеспечения

Также в энергонезависимой памяти хранятся загрузочные файлы. Они содержат загрузочный код, который используется для инициализации аппаратной части и запуска системы. Он выполняет распаковку исполняемого программного обеспечения из ПЗУ в оперативную память и управляет несколькими образами системного ПО.

В системе хранятся 2 идентичные копии загрузочного файла, одна из которых используется при включении устройства, а вторая хранится в виде резервной копии для активации в случае сбоя первого экземпляра.

Обновление загрузочного ПО можно производить с помощью протокола TFTP или через последовательный консольный порт, при этом используется процедура, аналогичная обновлению системного программного обеспечения.

7.3 Работа с конфигурационными файлами

Все произведенные в системе настройки хранятся в конфигурационных файлах, которые записываются в энергонезависимую память. При этом коммутатор содержит следующие виды конфигурационных файлов:

- **Startup configuration file** – конфигурационный файл, содержащий все настройки системы и значения соответствующих параметров, которые активизируются при старте системы.
- **Running configuration file** – конфигурационный файл, в котором хранятся все настройки системы и значения соответствующих параметров, которые пользователь изменил в процессе работы устройства. Указанные настройки продолжают действовать до тех пор, пока система не будет перезапущена или пользователь не внесет новые изменения в настройки.
- **Backup configuration file** – конфигурационный файл, являющийся резервной копией файла startup-config. Загружается при старте системы в случае, когда по какой-либо причине не произошла загрузка файла startup-config. Также можно использовать для отката настроек при внесении изменений в стартовую конфигурацию, которые оказались нежелательными.
- **Factory-default configuration file** – конфигурационный файл, к которому пользователь не имеет доступа. Содержит заводские настройки и активизируется, если при включении/перезагрузке устройства система не обнаружит ни одну из вышеперечисленных конфигураций или все они окажутся поврежденными.

Примечание: Для сохранения изменений, внесенных в конфигурацию систему в процессе ее работа, рекомендуется файл Running configuration скопировать в файл Startup configuration. В противном случае после перезагрузки устройства все новые настройки будут утеряны.

Пользователь может производить следующие операции с конфигурационными файлами:

- резервирование: копирование стартовой конфигурации в резервную;
- восстановление: копирование резервной конфигурации в стартовую;
- загрузка стартовой, текущей или резервной конфигурации из внешнего источника;
- копирование текущей конфигурации в резервную;
- копирование текущей конфигурации в стартовую;
- удаление стартовой, текущей или резервной конфигурации из памяти.

Вносить изменения в настройки пользователь может как непосредственно на самом устройстве через ИКС, так и путем создания соответствующего файла на внешнем ПК и его последующей загрузки в коммутатор.

Резервных конфигурационных файлов может быть несколько, и их можно переименовывать, все остальные файлы конфигураций существуют в единственном экземпляре, названия которых пользователь не может менять.

Примечание: В энергонезависимой памяти также может храниться файл Mirror Configuration, являющийся резервной копией конфигурации при синхронизации настроек устройств в режиме стека. В версии программного обеспечения ROS 1.0.20 данный файл не поддерживается.

7.4 Команды для работы с ПО и конфигурационными файлами

При выполнении операций над файлами в аргументах соответствующих команд указываются URL-адреса местонахождения файлов, а также используются ключевые слова. В таблице описаны ключевые слова и префиксы адресов, которые используются в операциях над файлами.

Ключевые слова и префиксы адресов в командах над файлами

Ключевое слово, префикс	**Описание**
`flash://`	Исходный адрес или адрес места назначения в энергонезависимой памяти. Эта память используется по умолчанию, если URL-адрес определен без префикса.
`running-config`	Файл текущей конфигурации
`startup-config`	Файл стартовой конфигурации
`backup-config`	Резервный файл конфигурации
`image`	Файл образа системного ПО. Если образ указан в качестве файла-источника, то образ активный, если указан в качестве файла назначения, то образ не активный
`boot`	Загрузочный файл
`tftp://`	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: `tftp://host/[directory]/filename`. `host` – может быть IPv4-адресом, IPv6-адресом или сетевым именем устройства, `directory` – каталог, `filename` – имя файла.
`xmodem:`	Исходный адрес файла при использовании протокола X-modem по последовательному соединению.
`unit://member/ startup-config`	Файл стартовой конфигурации одного из устройств стека. `member` – номер устройства в стеке
`unit://member/ backup-config`	Резервный файл конфигурации одного из устройств стека. `member` – номер устройства в стеке
`unit://member/image`	Файл образа системного ПО одного из устройств стека. `member` – номер устройства в стеке
`unit://member/boot`	Загрузочный файл одного из устройств стека. `member` – номер устройства в стеке
`localization`	Второй языковой файл. Первый файл основного языка интерфейса недоступен для пользователя
`null:`	Пустой адрес назначения для файлов. Можно копировать файл на пустой адрес назначения для определения его размера
`logging`	Файл Syslog

Далее описаны команды, с помощью которых можно выполнять различные операции над файлами системного программного обеспечения, а также загрузочными и конфигурационными файлами.

copy

Команда используется для копирования файла из местоположения источника в местоположение назначения.

Синтаксис:

copy *source-url destination-url* [**snmp**]

Параметры:

- *source-url* – адрес местонахождения копируемого файла (от 1 до 160 символов),
- *destination-url* – адрес назначения файла, в который данные будут скопированы (от 1 до 160 символов),
- snmp – указывает на то, что адрес файл записан в формате SNMP. Параметр используется только в случае, когда команда связана с файлом startup-config.

Режим ИКС:
Привилегированный режим

Пояснения:
При указании адресов используются префиксы и ключевые слова, описанные в таблице 6.0. Процесс копирования может длиться до нескольких минут и зависит от используемого протокола и структуры сети между источником и назначением. Далее показаны шаблоны наиболее часто используемых схем копирования файлов.

1) Копирование файла образа системного ПО с сервера в энергонезависимую память:

copy *source-url* **image**

2) Копирование загрузочного файла с сервера в энергонезависимую память:

copy *source-url* **boot**

3) Копирование файла конфигурации с сервера в текущую конфигурацию:

copy *source-url* **running-config**

При этом команды из загруженной конфигурации добавляются к уже существующей текущей конфигурации так, что итоговая текущая конфигурация является комбинацией существующей и вновь загруженной экземпляров.

4) Копирование файла конфигурации с сервера в стартовую конфигурацию:

copy *source-url* **startup-config**

5) Сохранение текущей или стартовой конфигурации на сервере:

copy running-config *destination-url*
copy startup-config *destination-url*

6) Сохранение текущей конфигурации в стартовую конфигурацию:

copy running-config startup-config

7) Сохранение текущей или стартовой конфигурации в заданный резервный файл:

copy running-config *file*
copy startup-config *file*

8) Сохранение текущей или стартовой конфигурации в резервный файл конфигурации:

copy running-config backup-config
copy startup-config backup-config

Существуют недопустимые комбинации адресов источника и назначения, которые описываются следующими условиями:

- исходный файл и файл назначения не могут совпадать,
- xmodem: не может быть указан в адресе назначения, по данному протоколу можно загрузить данные только в файл системного ПО, загрузочный файл или в пустой адрес.
- TFTP-сервер не может быть одновременно указан в адресе исходного местонахождения и адресе назначения,
- копирование файлов с расширением *.prv, *.sys запрещено,

– копировать с/на устройства, являющиеся «ведомыми» в стеке можно только файлы системного ПО и загрузочные файлы.

Процесс копирования сопровождается отображением следующих вспомогательных символов:
! – отображение восклицательного знака свидетельствует об успешном процессе копирования. Появление каждого такого знака означает успешное копирование 10 пакетов данных размером по 512 байт.
. – отображение точки свидетельствует о прерывании процесса копирования. Появление нескольких точек подряд означает возникновение ошибки при копировании.

Пример:
В следующем примере производится копирование файла `ros1022` системного ПО с TFTP-сервера с адресом 10.0.0.125 в не активный образ в памяти устройства.

```
console# copy tftp:// 10.0.0.125/ros1020 image
Accessing file 'file1' on 10.0.0.125...
Loading file1 from 10.0.0.125:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:18 [hh:mm:ss]
```

dir

Команда отображает список файлов, хранящихся в энергонезависимой памяти коммутатора.

Синтаксис:
dir
dir [*directory-path*]

Параметры:
– *directory-path* – путь к папке в памяти

Режим ИКС:
Привилегированный режим

Пример:
В следующем примере отображается список файлов, хранящихся в энергонезависимой памяти коммутатора.

```
     console#dir
Directory of flash:

     File Name       Permission Flash Size Data Size        Modified
------------------- ---------- ---------- --------- ----------------------
aaafile.prv              --        65520       --      08-Jan-2014 15:35:58
dhcpsn.prv               --        65520       --      21-Dec-2014 11:38:22
directry.prv             --        65520       --      21-Dec-2014 11:38:22
image-1                  rw      11796480  11796480    08-Jan-2014 16:30:06
image-2                  rw      11796480  11796480    08-Jan-2014 16:10:14
startup-config           rw      1048320      5006     09-Jan-2014 19:58:04
syslog1.sys              r-       131072       --      09-Jan-2014 20:19:38
syslog2.sys              r-       131072       --      09-Jan-2014 20:19:38
```

```
Total size of flash: 33423360 bytes
     Free size of flash: 8323376 bytes
```

more

Команда отображает содержимое выбранного файла.

Синтаксис:
more {**flash:**//<file>|**startup-config**|**running-config** |<file>}

Параметры:
- **flash:**// – отображает файл в энергонезависимой памяти,
- <file> – имя файла (от 1 до 160 символов),
- **startup-config** – файл стартовой конфигурации,
- **running-config** – файл текущей конфигурации.

Режим ИКС:
Привилегированный режим

Пояснения:
Содержимое файлов отображается в формате ASCII, за исключением образов системного ПО, которые отображаются в шестнадцатеричном формате.
Содержимое файлов *.prv, *.sys не отображается.

write

Команда сохраняет текущую конфигурацию в файл стартовой конфигурации.

Синтаксис:
write [**memory**|**terminal**]

Параметры:
- **memory** – сохранение текущую конфигурацию в файл стартовой конфигурации,
- **terminal** – вывод текущей конфигурации на терминал.

Режим ИКС:
Привилегированный режим

delete

Команда удаляет выбранный файл из энергонезависимой памяти устройства.

Синтаксис:
delete *url*
delete startup-config

Параметры:
- *url* – адрес URL удаляемого файла (от 1 до 160 символов),
- **startup-config** – удаляется файл стартовой конфигурации.

Режим ИКС:

Привилегированный режим

Пояснения:
Файлы *.prv, *.sys, image-1, image-2 удалить нельзя.

rename

Команда используется для изменения имени файла.

Синтаксис:
rename *url new-url*

Параметры:
- *url* – текущий URL-адрес файла (от 1 до 160 символов),
- *new-url* – новый URL-адрес файла (от 1 до 160 символов).

Режим ИКС:
Привилегированный режим

Пояснения:
Файлы *.prv, *.sys, image-1, image-2 переименовать нельзя.

boot system

Команда используется для назначения активного файла системного ПО, который будет загружаться при старте системы.

Синтаксис:
boot system {**image-1** | **image-2**}

Параметры:
- **image-1** – при следующем старте системы загрузится образ image-1,
- **image-2** – при следующем старте системы загрузится образ image-2.

Режим ИКС:
Привилегированный режим

Пояснения:
Для определения, какой файл в текущий момент является активным, используется команда **show bootvar**.

show running-config

Команда отображает содержимое файла текущей конфигурации.

Синтаксис:
show running-config

Режим ИКС:
Привилегированный режим

show startup-config

Команда отображает содержимое файла стартовой конфигурации.

Синтаксис:
show startup-config

Режим ИКС:
Привилегированный режим

show bootvar

Команда показывает активный файл системного ПО, который загружается при старте системы.

Синтаксис:
show bootvar [**unit** *unit*]

Параметры:
unit – номер устройства в стеке (1-8). Для коммутатора, работающего в автономном режиме, параметр не используется.

Режим ИКС:
Пользовательский режим

Пример:
В следующем примере показано использование команды.

```
console#show bootvar
Image  Filename   Version     Date                    Status
-----  ---------  ---------   --------------------    -----------
1      image-1    2.0.10      14-Jul-2014  16:21:02   Not active
2      image-2    4.0.7       20-Jun-2014  18:17:00   Active*

"*" designates that the image was selected for the next boot
```

8. Настройка зеркалирования трафика

8.1 Поддержка функции зеркалирования трафика

Для анализа трафика и мониторинга устройств предполагается возможность определить порт, в который будет перенаправлена копия всего трафика, проходящего через заданные порты или виртуальные частные сети VLAN.

Пользователь может включить зеркалирование трафика на порту назначения. По умолчанию зеркалирование трафика не включено. Предусматривается только один порт назначения. Пользователь может зеркалировать один или несколько портов, а также одну или несколько виртуальных локальных сетей VLAN в порт назначения одновременно.

В случае если в качестве источника используется несколько портов, а также одна или несколько виртуальных локальных сетей VLAN, трафик, направляемый в порт назначения, помещается в его очередь и обслуживается по принципу «первый пришел, первым обслужен», а любой избыточный трафик будет отброшен без предупреждений. Это может означать, что на порт анализатора, подключенный к порту назначения, будет направлено произвольно выбранное подмножество фактического трафика, проходящего через порты или виртуальные частные сети VLAN источников.

При создании сессии зеркалирования следует учитывать следующие ограничения:

- Один порт не может быть одновременно и портом источника, и портом назначения.
- Порт назначения не может быть включенным в состав группы агрегированных портов.
- IP-адрес не может быть назначенным порту назначения.
- GVRP не может быть включен на порту назначения.
- Порт назначения не может быть членом ни одной сети VLAN, за исключением default VLAN.

8.2 Команды для настройки зеркалирования трафика

Далее описаны команды для зеркалирования трафика, проходящего через заданные порты или виртуальные частные сети VLAN, изменения режима и отображения состояния зеркалирования.

port monitor

Команда используется для создания сессии зеркалирования трафика.

Синтаксис:

```
port monitor src-interface-id [rx|tx]
no port monitor src-interface-id
port monitor vlan vlan-id
no port monitor vlan vlan-id
interface range interface-id-list
```

Параметры:

- *src-interface-id* – идентификатор интерфейса, которым может быть физический порт,
- *vlan-id* – номер сети VLAN (1-4094),
- **rx** – зеркалирование только полученных пакетов,
- **tx** – зеркалирование только отправленных пакетов.

Состояние по умолчанию:
Зеркалирование и полученных, и отправленных пакетов.

Режим ИКС:
Режим Настройки интерфейса (Ethernet). Не может быть настроен для группы или диапазона портов.

port monitor mode

Команда используется для определения режима зеркалирования трафика.

Синтаксис:
port monitor mode {*monitor-only* | *network*}
no port monitor mode

Параметры:
- **mode** *monitor-only* – указывает, что порт назначения работает только в режиме зеркалирования, любой другой трафик на нем отбрасывается,
- **mode** *network* – указывает, что порт назначения работает также в качестве сетевого порта.

Состояние по умолчанию:
Режим monitor-only.

Режим ИКС:
Режим Общей настройки

show ports monitor

Команда отображает текущее состояние сессии зеркалирования трафика.

Синтаксис:
show ports monitor

Режим ИКС:
Привилегированный режим

9. Работа с таблицей MAC-адресов

9.1 Принцип формирования таблицы MAC-адресов

Коммутация пакетов на 2-уровне сетевой модели OSI системой производится с использованием Базы Данных Пересылки (*Forwarding Data BASE, FDB*). Она хранится в троичной ассоциативной памяти, реализованной непосредственно в структуре пакетного процессора. В состав базы данных пересылки входит таблица MAC-адресов, в которой хранятся MAC-адреса сетевых устройств, которые пересылали пакеты через интерфейсы коммутатора. Аппаратная реализация таблицы MAC-адресов позволяет осуществлять коммутацию пакетов без участия ЦПУ, т.е. без потери скорости передачи данных.

В системе поддерживается привязка отдельной таблицы MAC-адресов к каждому интерфейсу, причем в совокупности в памяти можно хранить до 16000 записей. Заполнение таблицы MAC-адресов происходит как в динамическом, так и статическом режимах. В первом случае происходит «обучение» указанной таблицы, при котором в нее вносятся новые записи по мере прохождения через интерфейс пакета с не зафиксированным до этого MAC-адресом отправителя. После перезагрузки системы такие записи не сохраняются, и процесс «обучения» запускается по новому циклу. Кроме того, такие записи имеют заданное время действия (aging time), по истечении которого автоматически удаляются из таблицы.

Во втором случае отдельные записи в таблицу MAC-адресов можно внести вручную статически. Такие записи сохраняются после перезагрузки системы и не подвергаются устареванию, т.е не имеют времени действия (aging time). Они сохраняются в конфигурационном файле и могут быть удалены или отредактированы только в статическом режиме вручную.

9.2 Команды для работы с таблицей MAC-адресов

Далее описаны команды, с помощью которых можно создавать, редактировать и удалять таблицы MAC-адресов и отдельные записи в них, а также другие команды, необходимые для эффективной работы с указанными таблицами.

mac address-table static

Команда необходима для добавления заданного MAC-адреса отправителя в таблицу адресов. Использование префикса **no** удаляет заданный MAC-адрес отправителя из таблицы адресов.

Синтаксис:

mac address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-id* [**permanent**|**delete-on-reset**|**delete-on-timeout**|**secure**]

no mac address-table static [*mac-address*] **vlan** *vlan-id*

Параметры:

- *mac-address* – добавляемый MAC-адрес отправителя,
- *vlan-id* – номер сети VLAN (1-4094),
- *interface-id* – номер интерфейса, к которому прикрепляется таблица MAC-адресов,
- **permanent** – адрес можно удалить только с помощью команды **no bridge address**,
- **delete-on-reset** – адрес удаляется из таблицы при перезапуске системы,

- **delete-on-timeout** – адрес удаляется из таблицы по тайм-ауту,
- **secure** – адрес удаляется из таблицы после возвращения порта в режим «обучения» (по команде **no port security**).

Состояние по умолчанию:
Статические записи отсутствуют. По умолчанию новый адрес добавляется в таблицу с параметром **permanent**.

Режим ИКС:
Режим Общей настройки

clear mac address-table

Команда удаляет статические или динамические записи из таблицы MAC-адресов.

Синтаксис:
clear mac address-table dynamic [**interface** *interface-id*]
clear mac address-table secure interface *interface-id*

Параметры:
- **dynamic** – удаление динамических записей,
- **secure** – удаление статических записей,
- *interface-id* – удаление всех статических/динамических записей, привязанных к заданному интерфейсу: порту Ethernet или группе агрегированных портов.

Режим ИКС:
Привилегированный режим

mac address-table aging-time

Команда устанавливает время хранения адреса в таблице таблицы MAC-адресов. Использование префикса **no** возвращает указанному времени значение по умолчанию.

Синтаксис:
mac address-table aging-time *seconds*
no mac address-table aging-time

Параметры:
- *seconds* – время хранения MAC-адреса в таблице в секундах (от 10 до 630 с)

Состояние по умолчанию:
300 секунд

Режим ИКС:
Режим Общей настройки

show mac address-table

Команда отображает таблицу MAC-адресов для указанного интерфейса или всех интерфейсов.

Синтаксис:

show mac address-table [**count**|**dynamic**|**static**|**secure**] [**vlan** *vlan*] [**interface** *interface-id*] [**address** *mac-address*]

Параметры:

- **dynamic** – отображаются только динамические адреса,
- **static** – отображаются только статические адреса,
- **secure** – отображаются только «безопасные» адреса,
- *vlan* – номер сети VLAN (1-4094),
- *interface-id* – номер интерфейса: порт Ethernet или группа агрегированных портов,
- *mac-address* – MAC-адрес.

Режим ИКС:
Привилегированный режим

show mac address-table count

Команда отображает количество записей в таблице MAC-адресов для указанного интерфейса или для всех интерфейсов.

Синтаксис:
show mac address-table count [**vlan** *vlan* | **interface** *interface-id*]

Параметры:

- *vlan* – номер сети VLAN (1-4094),
- *interface-id* – номер интерфейса: порт Ethernet или группа агрегированных портов.

Режим ИКС:
Привилегированный режим

10. Настройка Агрегации каналов

10.1 Поддержка функции агрегации каналов

Система поддерживает механизм агрегации каналов, при котором можно несколько физических портов объединить в один логический интерфейс. Это увеличивает пропускную способность всего агрегированного соединения в тех случаях, когда возможности отдельных физических портов этого сделать не позволяет, а также повышает отказоустойчивость канала.

Коммутатор обеспечивает объединение до восьми интерфейсов Ethernet в одной группе агрегированных каналов (Link Aggregation Group, LAG) и до восьми групп LAG на устройстве или стеке устройств. Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в дуплексном режиме.

Устройство поддерживает два режима создания группы портов – статическая группа и группа, работающая по протоколу LACP (Link Aggregation Control Protocol). При этом если для интерфейса произведены настройки, то для добавления его в группу следует вернуть настройки по умолчанию.

Примечание: В зависимости от того в каком режиме работает коммутатор – автономно или в составе стека, изменяется вид записи для интерфейса Ethernet. При автономной работе запись для интерфейса имеет вид: 1/1/N, где N – номер интерфейса. При работе в составе стека запись для интерфейса имеет вид: K/1/N, где K – номер устройства в стеке, N – номер интерфейса. Средняя цифра указывает на номер слота в устройстве модульного типа.

10.2 Команды для настройки агрегированных каналов

Далее описаны команды, с помощью которых можно создавать группы агрегированных каналов в статическом режиме и по протоколу LACP, включать в них физические порты, управлять балансировкой нагрузки на него и просматривать информацию о существующих группах портов.

`interface range`

Команда используется для выбора группы интерфейсов или их диапазона, к которым будет применяться последующая команда.

Синтаксис:
`interface range` *`interface-id-list`*

Параметры:
– *`interface-id-list`* – группа или диапазон портов

Режим ИКС:
Режим Общей настройки

Пояснения:
Команды, выполняемые над группой интерфейсов, применяются к каждому из них независимо, т.е. если при выполнении команды над одним из интерфейсов появится

сообщение об ошибке, то выполнение этой команды над остальными интерфейсами будет продолжено.

channel-group

Команда используется для добавления выбранного интерфейса Ethernet в группу агрегированных каналов. Использование префикса **no** удаляет интерфейс Ethernet из группы агрегированных каналов.

Синтаксис:
channel-group *port-channel* **mode** {*on* | *auto*}
no channel-group

Параметры:
- *port-channel* – номер группы агрегированных портов, в который добавляется интерфейс,
- **mode** *on* – добавление интерфейса в статическом режиме, т.е. использования протокола LACP,
- **mode** *auto* – добавление интерфейса с. использованием протокола LACP.

Состояние по умолчанию:
Порт не принадлежит к группе агрегированных каналов.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet)

show interfaces port-channel

Команда отображает информацию о выбранном агрегированном канале или обо всех агрегированных каналах.

Синтаксис:
show interfaces port-channel [*interface-id*]

Параметры:
- *interface-id* – номер агрегированного канала

Режим ИКС:
Пользовательский режим

port-channel load-balance

Команда задает механизм балансировки нагрузки для группы агрегированных портов.

Синтаксис:
port-channel load-balance {*src-dst-mac-ip* | *src-dst-mac* | *src-dst-ip* | *src-dst-mac-ip-port*}

Параметры:
- *src-dst-mac-ip* – механизм балансировки основывается на MAC-адресе и IP-адресе,
- *src-dst-mac* – механизм балансировки основывается на MAC-адресе,
- *src-dst-ip* – механизм балансировки основывается на IP-адресе,

– *src-dst-mac-ip-port* – механизм балансировки основывается на MAC-адресе, IP-адресе и порте назначения.

Режим ИКС:
Режим Общей настройки

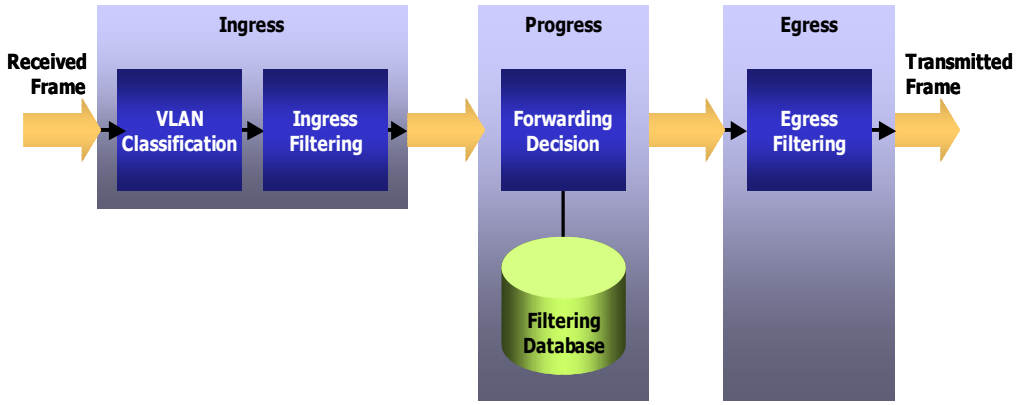
11. Настройка виртуальных локальных сетей VLAN

11.1 Поддержка виртуальных локальных сетей VLAN

Система поддерживает создание и обслуживание до 4094 виртуальных локальных сетей VLAN. Они широко используются для разделения пользователей на логические группы. Для коммутаторов, работающих на нескольких уровнях сетевой модели OSI, использование виртуальных локальных сетей VLAN обычно означает, что пользователи из разных сетей VLAN по-прежнему могут связываться, но должны для этого использовать IP-маршрутизацию.

Сеть VLAN может быть задана для отдельного коммутатора или она может занимать несколько коммутаторов путем определения сети VLAN на каждом из них, но при условии использования одного и того же тэга VLAN и соединения коммутаторов через порты, которые являются членами этой сети VLAN. При этом коммутация пакета системой производится в контексте отдельной сети VLAN. Каждый пакет классифицируется на входе в VLAN, причем такая классификация определяется на основе тэга VLAN в пакете (т.е. когда тэг задан внешне) или производится по некоторым установленным пользователем правилам на основе входного порта или каких-либо значений из заголовка пакета. Классификация VLAN является частью входной обработки пакета.

На рисунке показана последовательность обработки данных при прохождении кадра (frame) от входного порта коммутатора к выходному.



Поддержка виртуальных локальных сетей VLAN

Полученный кадр вначале классифицируется на принадлежность к той или иной сети VLAN следующим образом: если полученный кадр содержит тэг VLAN то он используется для классификации; в противном случае кадр классифицируется на основе параметра PVID порта. После классификации кадр может пройти через входную фильтрацию (если она включена), где кадр будет отброшен, если его VLAN ID не найден в списке сетей VLAN, к которым принадлежит входной порт. Далее принимается решение по пересылке (forwarding decision) на основе VLAN ID и MAC-адреса назначения. Наконец, выходные правила определяют, должен ли кадр быть отправлен с тэгом или без него. Членство в сети VLAN может быть сконфигурировано пользователем статически или посредством протоколов (GVRP и др.).

Пользователь может создавать/удалять в системе сети VLAN (кроме «Сети по умолчанию» Default VLAN, которая существует всегда). Каждый порт в VLAN может быть настроен как имеющий тэг (Tagged) и не имеющий его (Untagged), запрещенный и исключенный (не член VLAN). За исключением default VLAN, пользователь может настроить установку и снятие тэга (Tagged/Untagged) на выходном порту.

11.2 Команды для работы с сетями VLAN

Далее описаны команды для создания/редактирования/удаления виртуальных локальных сетей VLAN, включения в них интерфейсов и выполнения других необходимых действий.

`vlan database`

Команда используется для вхождения в режим конфигурирования сетей VLAN.

Синтаксис:
`vlan database`

Режим ИКС:
Режим Общей настройки

`vlan`

Команда используется для создания новой сети VLAN. Использование префикса **`no`** удаляет выбранную или все существующие сети VLAN.

Синтаксис:
`vlan` *`vlan-range`* [name *`vlan-name`*]
`no vlan` *`vlan-range`*

Параметры:
- *`vlan-range`* – список номеров создаваемых сетей VLAN (от 2 до 4094). Номера могут быть перечислены через запятую; если используются несколько номеров подряд, то их можно задать в виде диапазона через дефис,
- *`vlan-name`* – название сети VLAN (от 1 до 32 символов). Параметр активен, когда создается только одна сеть.

Режим ИКС:
Режим конфигурирования VLAN

`interface vlan`

Команда используется для вхождения в режим конфигурирования выбранной сети VLAN и настройки ее параметров.

Синтаксис:
`interface vlan` *`vlan-id`*

Параметры:
- *`vlan-id`* – номер конфигурируемой сети VLAN

Режим ИКС:

Режим Общей настройки

interface range vlan

Команда используется для однотипной настройки параметров нескольких сетей VLAN одновременно.

Синтаксис:
interface range vlan *vlan-range*

Параметры:
– *vlan-range* – список номеров настраиваемых сетей VLAN. Номера могут быть перечислены через запятую; если используются несколько номеров подряд, то их можно задать в виде диапазона через дефис

Режим ИКС:
Режим Общей настройки

Пояснения:
Команды, выполняемые над группой интерфейсов, применяются к каждому из них независимо, т.е. если при выполнении команды над одним из интерфейсов появится сообщение об ошибке, то выполнение этой команды над остальными интерфейсами будет продолжено.

name

Команда используется для присваивания имени выбранной сети VLAN. Использование префикса **no** удаляет название сети.

Синтаксис:
name *string*
no name

Параметры:
– *string* – уникальное название, ассоциированное с сетью VLAN (до 32 символов)

Состояние по умолчанию:
Нет названия сети

Режим ИКС:
Режимы Настройки интерфейса (VLAN)

show vlan

Команда отображает информацию о выбранной сети или обо всех сетях VLAN.

Синтаксис:
show vlan [**tag** *vlan-id* | **name** *vlan-name*]

Параметры:
– *vlan-id* – номер сети VLAN,
– *vlan-name* – имя сети VLAN.

Режим ИКС:
Привилегированный режим

`show default-vlan-membership`

Команда отображает членов специальной сети «VLAN по умолчанию» Default VLAN.

Синтаксис:
`show default-vlan-membership` [*`interface-id`*]

Параметры:

– *`interface-id`* – номер интерфейса: порт или группа агрегированных портов

Режим ИКС:
Привилегированный режим

12. Настройка многоадресной передачи (multicast bridge)

12.1 Поддержка многоадресной передачи

Многоадресная передача предполагает распространение трафика по принципу один-к-многим и многие-ко-многим – данные передаются на все активные порты коммутатора. Предусмотрена возможность блокирования распространение многоадресных данных в указанные порты, что позволяет сохранить пропускную способность и ресурсы устройства.

Для каждой виртуальной локальной сети VLAN система поддерживает списки групп многоадресной рассылки, на основании которых принимается решение в какой порт многоадресные данные должны быть переданы. Эти группы могут быть сконфигурированы пользователем статически или получены динамически с использованием протоколов IGMP для IPv4 или MLD для IPv6.

Команды для настройки многоадресной передачи

`ip igmp version`

Команда определяет версию протокола IGMP на интерфейсе. Использование префикса **`no`** восстановит установки по умолчанию.

Синтаксис:

```
ip igmp version {1 | 2 | 3}
no ip igmp version
```

Параметры:

- *1* – определяет, что протокол IGMP версии 1 используется на интерфейсе,
- *2* – определяет, что протокол IGMP версии 2 используется на интерфейсе,
- *3* – определяет, что протокол IGMP версии 3 используется на интерфейсе.

Состояние по умолчанию:
Версия протокола IGMP по умолчанию – 3

Режим ИКС:
Режимы Настройки интерфейса (VLAN)

`ipv6 mld version`

Команда определяет версию протокола MLD на интерфейсе. Использование префикса **`no`** восстановит установки по умолчанию.

Синтаксис:

```
ipv6 mld version {1 | 2}
no ipv6 mld version
```

Параметры:

- *1* – определяет, что протокол MLD версии 1 используется на интерфейсе,
- *2* – определяет, что протокол MLD версии 2 используется на интерфейсе.

Состояние по умолчанию:
Версия протокола MLD по умолчанию – 2

Режим ИКС:
Режимы Настройки интерфейса (VLAN)

ip igmp snooping (Global)

Команда включает групповую передачу на основе анализа IGMP пакетов (IGMP Snooping). Использование префикса **no** отключает групповую передачу на основе анализа IGMP пакетов.

Синтаксис:
ip igmp snooping
no ip igmp snooping

Состояние по умолчанию:
Групповая передача на основе анализа IGMP пакетов отключена

Режим ИКС:
Режим Общей настройки

ip igmp snooping vlan

Команда включает групповую передачу на основе анализа IGMP пакетов (IGMP Snooping) в указанной виртуальной локальной сети VLAN. Использование префикса **no** отключает групповую передачу на основе анализа IGMP пакетов в указанной VLAN.

Синтаксис:
ip igmp snooping vlan *vlan-id*
no ip igmp snooping vlan *vlan-id*

Параметры:
– *vlan-id* – номер сети VLAN (1-4094),

Состояние по умолчанию:
Групповая передача на основе анализа IGMP пакетов отключена

Режим ИКС:
Режим Общей настройки

Пояснения:
IGMP snooping может быть включен только в статических виртуальных локальных сетях VLAN. Для активации IGMP snooping команда **bridge multicast filtering** также должна быть выполнена.

ip igmp snooping vlan static

Команда статически регистрирует список групп многоадресной рассылки и добавляет порты к нему. Использование префикса **no** удаляет порт из списка групп.

Синтаксис:
ip igmp snooping vlan *vlan-id* **static** *ip-address* **[interface** *interface-list***]**
no ip igmp snooping vlan *vlan-id* **static** *ip-address* **[interface** *interface-list***]**

Параметры:
- *vlan-id* – номер сети VLAN (1-4094),
- *ip-address* – IP адрес многоадресной передачи
- *interface-list* – номер интерфейса: порт или группа агрегированных портов

Состояние по умолчанию:
IP адрес многоадресной передачи не определен

Режим ИКС:
Режим Общей настройки

Пояснения:
Статический IP адрес многоадресной передачи может быть включен только в статических виртуальных локальных сетях VLAN. Команда может быть выполнена до того, как создана сеть VLAN.

ipv6 mld snooping (Global)

Команда включает групповую передачу на основе анализа MLD пакетов (MLD Snooping). Использование префикса **no** отключает групповую передачу на основе анализа MLD пакетов.

Синтаксис:
ipv6 mld snooping
no ipv6 mld snooping

Состояние по умолчанию:
Групповая передача на основе анализа MLD пакетов отключена

Режим ИКС:
Режим Общей настройки

ipv6 mld snooping vlan

Команда включает групповую передачу на основе анализа MLD пакетов (MLD Snooping) в указанной виртуальной локальной сети VLAN. Использование префикса **no** отключает групповую передачу на основе анализа MLD пакетов в указанной VLAN.

Синтаксис:
ipv6 mld snooping vlan *vlan-id*
no ipv6 mld snooping vlan *vlan-id*

Параметры:
- *vlan-id* – номер сети VLAN (1-4094),

Состояние по умолчанию:
Групповая передача на основе анализа MLD пакетов отключена

Режим ИКС:
Режим Общей настройки

Пояснения:
MLD snooping может быть включен только в статических виртуальных локальных сетях VLAN. Для активации MLD snooping команда **`bridge multicast filtering`** также должна быть выполнена.

`ipv6 mld snooping vlan static`

Команда статически регистрирует список групп многоадресной рассылки и добавляет порты к нему. Использование префикса **`no`** удаляет порт из списка групп.

Синтаксис:
`ipv6 mld snooping vlan` *`vlan-id`* **`static`** *`ipv6-address`* **`[interface`** *`interface-list`***`]`**
`no ipv6 mld snooping vlan` *`vlan-id`* **`static`** *`ipv6-address`* **`[interface`** *`interface-list`***`]`**

Параметры:
- *`vlan-id`* – номер сети VLAN (1-4094),
- *`ipv6-address`* – IPv6 адрес многоадресной передачи
- *`interface-list`* – номер интерфейса: порт или группа агрегированных портов

Состояние по умолчанию:
IP адрес многоадресной передачи не определен

Режим ИКС:
Режим Общей настройки

Пояснения:
Статический IP адрес многоадресной передачи может быть включен только в статических виртуальных локальных сетях VLAN. Команда может быть выполнена до того, как создана сеть VLAN.

13. Настройка протокола Spanning Tree

13.1 Поддержка протокола Spanning Tree

Протокол Spanning Tree защищает широковещательный домен от петель и штормов пакетов, которые могут образоваться в результате, путем выборочного включения интерфейсов в режим ожидания, в котором они не передают пользовательские данные, но автоматически повторно активируются при изменении топологии. Коммутаторы периодически обмениваются конфигурационными сообщениями, используя специально отформатированные кадры, называемые BPDU, и выборочно включают и отключают передачу трафика на портах.

Система поддерживает 3 типа Spanning Tree протоколов: Spanning Tree protocol (IEEE802.1D – классический SPT), Rapid Spanning Tree Protocol (IEEE802.1w – RSTP), and Multiple Spanning Tree Protocol (IEEE802.1s –MSTP). По умолчанию используется RSTP. Поддерживается возможность фильтрации BPDU или отключения STP на указанных портах.

13.2 Команды для настройки протокола Spanning Tree

spanning-tree

Команда включает протокол Spanning Tree. Использование префикса **no** отключает протокол.

Синтаксис:
spanning-tree
no spanning-tree

Состояние по умолчанию:
Протокол Spanning Tree включен

Режим ИКС:
Режим Общей настройки

spanning-tree mode

Команда определяет режим работы протокола Spanning Tree на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
spanning-tree mode {*stp* | *rstp* | *mst*}
no spanning-tree mode

Параметры:
- *stp* – определяет, что протокол STP используется,
- *rstp* – определяет, что протокол Rapid STP используется,
- *mst* – определяет, что протокол Multiple STP используется.

Состояние по умолчанию:
По умолчанию используется RSTP

Режим ИКС:
Режим Общей настройки

spanning-tree priority

Команда определяет приоритет устройства, используемый для выбора корневого коммутатора. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
spanning-tree priority *priority*
no spanning-tree priority

Параметры:
– *priority* – значение приоритета коммутатора: (0-61440 с шагом в 4096).

Состояние по умолчанию:
32768

Режим ИКС:
Режим Общей настройки

Пояснения:
Коммутатор с наименьшим значением приоритета становится корневым. Если больше чем один коммутатор имеет наименьшее значение приоритета – коммутатор с наименьшим MAC адресом становится корневым.

spanning-tree cost

Команда определяет стоимость STP пути на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
spanning-tree cost *cost*
no spanning-tree cost

Параметры:
– *cost* – значение стоимости пути интерфейса: (1-200000000).

Состояние по умолчанию:
Значение стоимости пути по умолчанию зависит от скорости интерфейса и метода определения стоимости (быстрый или медленный):

Интерфейс	**Медленный**	**Быстрый**
Port-channel	20,000	4
TenGigabit Ethernet (10 Gbps)	2000	2
Gigibit Ethernet (1 Gbps)	20,000	4
Ethernet (10 Mbps)	2,000,000	100

Режим ИКС:
Режимы Настройки интерфейса

spanning-tree port-priority

Команда определяет стоимость STP пути на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
spanning-tree port-priority *priority*
no spanning-tree port-priority

Параметры:
– *priority* – значение приоритета интерфейса: (1-240 с шагом в 16).

Состояние по умолчанию:
128

Режим ИКС:
Режимы Настройки интерфейса

spanning-tree portfast

Команда включает режим portfast на интерфейсе. В режиме portfast интерфейс немедленно переходит в состояние передачи, используется на портах уровня доступа. Использование префикса **no** выключает режим portfast на интерфейсе.

Синтаксис:
spanning-tree portfast [*auto*]
no spanning-tree portfast

Параметры:
– *auto* – устройство устанавливает задержку в 3 секунды. Если до ее истечение не получено ниодного BPDU сообщения, порт переводится в режим portfast.

Состояние по умолчанию:
Режим portfast выключен

Режим ИКС:
Режимы Настройки интерфейса

spanning-tree bpduguard

Команда выключает интерфейс в случае получения BPDU сообщения. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
spanning-tree bpduguard {*enable* | *disable*}
no spanning-tree bpduguard

Параметры:
– *enable* – включить функцию BPDU-guard,
– *disable* – выключить функцию BPDU-guard

Состояние по умолчанию:
Режим bpduguard выключен

Режим ИКС:
Режимы Настройки интерфейса

14. Настройка IP-адресации и маршрутизации

IP-маршрутизация, т.е. обработка и передача данных на 3-уровне сетевой модели OSI, является одним из базовых сетевых сервисов системы. Для этого в ней реализована поддержка протоколов RIP, ARP, DNS, DHCP, а также сетей IP VLAN и групповой адресации IP multicast. При этом в системе можно прописать до 128 статических маршрутов и внести до 1024 записей в таблицу соответствий ARP.

Коммутатор может функционировать в следующих двух режимах обработки и передачи данных:

- Режим моста (**Bridging Mode**). При этом для пересылки пакетов используется адресная информация 2-уровня сетевой модели OSI (L2 Forwarding).
- Режим маршрутизации (**Routing Mode**). При этом для пересылки пакетов используется адресная информация 3-уровня сетевой модели OSI (L3 Forwarding).

Для переключения коммутатора в режим маршрутизации используется команда **`ip routing`**, подробное описание которой дано ниже.

Примечание: Далее описание всех настроек и команд в данном разделе приведено для случая использования IP-адресов формата IPv4. Вместе с тем в системе реализована полнофункциональная поддержка адресации на основе IPv6. При этом в синтаксисе или параметрах соответствующих команд, как правило, достаточно заменить **`ip`** на **`ipv6`**. Кроме того, система поддерживает функцию туннелирования трафика IPv6 на базе протокола ISATAP, который позволяет осуществлять передачу трафика IPv6 через сети с адресацией IPv4.

14.1 Назначение IP-адресов коммутатору и его интерфейсам

Самому коммутатору и его интерфейсам можно назначить от 1 до 30 IP-адресов. Если устройство работает в режиме моста, то можно назначить только один IP-адрес всей системе, если устройство работает в режиме маршрутизации, то можно назначить до 30 IP-адресов отдельным интерфейсам системы, под которыми здесь понимаются физические порты, агрегированные каналы и интерфейсы VLAN.

По умолчанию система запускается в режиме моста и ожидает назначения ей динамического IP-адреса от DHCP-сервера. Если в течение 60 секунд после старта ответа от DHCP-сервера не поступает, то системе назначается IP-адрес по умолчанию: `192.168.1.239/24`, где `24` – маска подсети, записанная в двоичном представлении.

Примечание: Значение маски может быть записано либо в формате `A.B.C.D`, либо в формате `/N`, где `N` – количество единиц в двоичном представлении маски.

Использование статической и динамической IP-адресации

Далее описаны команды, использующиеся для назначения, просмотра и настойки IP-адресов. При этом если IP-адрес настраивается для интерфейса физического порта или группы агрегированных портов, то этот интерфейс удаляется из сети VLAN, которой ранее принадлежал.

`ip address`

Команда назначает IP-адрес интерфейсу, которым может быть физический порт, агрегированный канал или VLAN. Использование префикса **no** удаляет назначенный ранее интерфейсу IP-адрес.

Синтаксис:
ip address *ip-address* {*mask* | *prefix-length*}
no ip address [*ip-address*]

Параметры:
- *ip-address* – назначаемый IP-адрес,
- *mask* – маска подсети записанная в формате IP-адреса,
- *prefix-length* – количество единиц в двоичном представлении маски (8-30). Перед указанием данного параметр должна стоять косая черта (/).

Состояние по умолчанию:
Интерфейсам IP-адреса не назначены.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel, VLAN). Команда не может быть применена к группе интерфейсов.

Пояснения:
а) Назначение интерфейсу статического IP-адреса автоматически отключает на нем DHCP-клиент.
б) Назначаемые отдельным интерфейсам IP-адреса должны принадлежать различным подсетям. Если коммутатор работает в режиме моста, то назначаемый ему единый IP-адрес привязывается к порту, через который в текущий момент разрешено управление системой.

ip address dhcp

Команда используется для получения IP-адреса для настраиваемого интерфейса от DHCP-сервера. Использование префикса **no** отключает динамическое присваивание интерфейсу IP-адреса и освобождает этот адрес. Интерфейсом может быть физический порт, агрегированный канал или VLAN.

Синтаксис:
ip address dhcp
no ip address dhcp

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel, VLAN). Команда не может быть применена к группе интерфейсов.

Пояснения:
Включение на интерфейсе DHCP-клиента автоматически удаляет назначенный ему статический IP-адрес.

ip default-gateway

Команда устанавливает для коммутатора шлюз по умолчанию. Использование префикса **no** удаляет шлюз по умолчанию.

Синтаксис:
ip default-gateway *ip-address*
no ip default-gateway

Параметры:
– *ip-address* – IP-адрес шлюза по умолчанию.

Режим ИКС:
Режим Общей настройки

Состояние по умолчанию:
Шлюз по умолчанию не установлен

renew dhcp

Команда отправляет запрос DHCP-серверу на обновление IP-адреса.

Синтаксис:
renew dhcp {*interface-id*} [**force-autoconfig**]

Параметры:
– *interface-id* – номер интерфейса (порт, агрегированный канал, VLAN),
– **force-autoconfig** – после обновления IP-адреса производится автоматическое внесение изменений в конфигурационный файл устройства.

Режим ИКС:
Привилегированный режим

Пояснения:
Команда не включает автоматически DHCP-клиент на интерфейсе, то есть если на интерфейсе DHCP-клиент не включен, то при вводе данной команды появится сообщение об ошибке.

show ip interface

Команда отображает текущую конфигурацию IP-адресации для всех интерфейсов или для указанного интерфейса.

Синтаксис:
show ip interface [*interface-id*]

Параметры:
– *interface-id* – номер интерфейса (порт, агрегированный канал, VLAN),

Режим ИКС:
Пользовательский режим

interface ip

Команда используется для входа в режим настройки IP-интерфейсов.

Синтаксис:
interface ip *ip-address*

Параметры:

– *ip-address* – настраиваемый адрес.

Режим ИКС:
Режим Общей настройки

Пояснения:
IP-адреса, назначенные каким-либо интерфейсам (порт, агрегированный канал, VLAN), далее можно настраивать в виде самостоятельных IP-интерфейсов, т.е. не указывая их принадлежность конкретному интерфейсу 2-го уровня.

ipv6 enable

Команда включает поддержку IPv6 на интерфейсе. Использование префикса **no** отключает поддержку IPv6 на интерфейсе.

Синтаксис:
ipv6 enable [no-autoconfig]
no ipv6 enable

Параметры:

– **no-autoconfig** – включение поддержки трафика IPv6 на интерфейсе без автоматической конфигурации адресов

Состояние по умолчанию:
Поддержка IPv6 отключена.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel, VLAN). Команда не может быть применена к группе интерфейсов.

Использование протокола DNS для трансляции адресов

В системе реализована поддержка протокола DNS, использующегося для определения IP-адреса сетевого устройства по его доменному имени и обратно. Коммутатор является полнофункциональным DNS-клиентом, поддерживающим до 8 DNS-серверов с базами данных соответствий доменных имен узлов сети и их IP-адресов. При этом один из таких серверов назначается «первичным» (primary), и к нему система обращается в первую очередь. Кроме того, пользователь может статически прописать до 64 записей таких соответствий непосредственно на самом устройстве. Далее описаны команды, использующиеся для настройки работы с использованием протокола DNS.

ip domain lookup

Команда включает трансляцию доменных имен сетевых устройств в их IP-адреса с использованием протокола DNS. Использование префикса **no** отключает трансляцию адресов.

Синтаксис:
ip domain lookup
no ip domain lookup

Состояние по умолчанию:
Поддержка DNS в системе включена

Режим ИКС:
Режим Общей настройки

ip domain name

Команда определяет доменное имя по умолчанию, которое будет использоваться программой для дополнения неполных доменных имен (доменных имен без точки). Для доменных имен без точки в конец имени будет добавляться точка и указанное в команде выражение. Использование префикса **no** удаляет доменное имя по умолчанию.

Синтаксис:
ip domain name *name*
no ip domain name

Параметры:
– *name* – доменное имя по умолчанию (от 1 до 158 символов)

Состояние по умолчанию:
Доменное имя по умолчанию не задано

Режим ИКС:
Режим Общей настройки

Пояснения:
При вводе доменного имени по умолчанию необходимо использовать только символы ASCII: буквы A-Z (с учетом регистра), цифры 0-9, символ подчеркивания и дефис. Точка используется для разделения слов.

ip name-server

Команда определяет IPv4/IPv6-адреса для доступных DNS-серверов. Использование префикса **no** удаляет IP-адрес DNS-сервера из списка доступных.

Синтаксис:
ip name-server {*server1-address*} [*server2-address … server8-address*]
no ip name-server [*server1-address … server8-address*]

Параметры:
– *server-address* – IPv4/IPv6-адрес DNS-сервера. В одной команде можно задать до 8 серверов.

Состояние по умолчанию:
DNS-сервера не заданы

Режим ИКС:
Режим Общей настройки

Пояснения:
Приоритет использования DNS-серверов определяется порядком их следования в команде. Сервера могут быть также заданы несколькими командами.

ip host

Команда определяет статические соответствия имен узлов сети IP-адресам и добавляет установленное соответствие в кэш-память коммутатора. Использование префикса **no** удаляет статическое соответствие.

Синтаксис:
ip host *name address* [*address2 address3 address4*]
no ip host *name*

Параметры:
- *name* – доменное имя (от 1 до 158 символов),
- *address* – ассоциированный с доменным именем IP-адрес. К одному доменному имени можно привязать до 4 IP-адресов.

Состояние по умолчанию:
Статические соответствия не заданы

Режим ИКС:
Режим Общей настройки

Пояснения:
При вводе доменного имени необходимо использовать только символы ASCII: буквы A-Z (с учетом регистра), цифры 0-9, символ подчеркивания и дефис. Точка используется для разделения слов.

clear host

Команда удаляет записи соответствия доменных имен узлов сети и их IP-адресов из кэш-памяти устройства.

Синтаксис:
clear host {*name* | *}

Параметры:
- *name* – доменное имя узла сети,
- * – удаление всех записей из таблицы соответствия.

Режим ИКС:
Привилегированный режим

show hosts

Команда отображает доменное имя по умолчанию, список DNS-серверов, статические и кэшированные соответствия имен узлов сети и IP-адресов.

Синтаксис:
show hosts [*name*]

Параметры:
– *name* – доменное имя узла сети, по которому отображается соответствующий ему IP-адрес

Режим ИКС:
Привилегированный режим

14.2 Настройка IP-маршрутизации

Коммутатор поддерживает работу системы в режиме маршрутизации проходящего трафика. При этом IP-маршруты можно прописать в таблице маршрутизации статически. Кроме того, поддерживается динамическая маршрутизация пакетов по протоколу RIP версий 1 и 2, OSPF версии 2. Далее описаны команды для настройки IP-маршрутизации проходящего трафика.

ip routing

Команда включает режим маршрутизации IPv4-пакетов. Использование префикса **no** отключает режим маршрутизации.

Синтаксис:
ip routing
no ip routing

Состояние по умолчанию:
Режим маршрутизации отключен

Режим ИКС:
Режим Общей настройки

ip route

Команда создает статическое правило маршрутизации. Использование префикса **no** удаляет статическое правило из таблицы маршрутизации.

Синтаксис:
ip route *prefix* {*mask* | *prefix-length*} *gateway* [**metric** *distance*] [**reject-route**]
no ip route prefix {*mask* | *prefix-length*} [*gateway*]

Параметры:
– *prefix* – IP-адрес для сети назначения,
– *mask* – маска подсети для сети назначения,
– *prefix-length* – маска подсети для сети назначения в двоичном представлении (0-32),
– *gateway* – IP-адрес шлюза для доступа к сети назначения,
– *distance* – вес маршрута (1-255),
– **reject-route** – запрещает маршрутизацию к сети назначения через все шлюзы.

Состояние по умолчанию:
Вес маршрута по умолчанию равен 1

Режим ИКС:
Режим Общей настройки

show ip route

Команда отображает текущее состояние таблицы маршрутизации или отдельных записей из нее.

Синтаксис:
show ip route [**connected** | **static** | {**address** *address* [*mask* | *prefix-length*] [**longer-prefixes**]}]

Параметры:
- **connected** – отображает только подключенные к интерфейсам и функционирующие маршруты,
- **static** – отображает только статически прописанные маршруты,
- *address* – отображает маршрут только до указанного IP-адреса,
- *mask* – маска подсети указанного IP-адреса,
- *prefix-length* – маска подсети указанного IP-адреса в двоичном представлении (0-32)
- **longer-prefixes** – отображает все маршруты, соответствующие введенным значениям параметров *mask* или *prefix-length*.

Режим ИКС:
Пользовательский режим

show ip protocols

Команда отображает текущее состояние и настройки активных протоколов маршрутизации.

Синтаксис:
show ip protocols

Режим ИКС:
Пользовательский режим

14.3 Настройка протокола маршрутизации RIP

RIP является дистанционно-векторным протоколом внутридоменной маршрутизации на основе алгоритма Беллмана-Форда. Этот алгоритм был использован для маршрутизации в компьютерных сетях с первых дней работы сети ARPANET и получил большую популярность через свою простоту. RIP выполняет выбор маршрута путем минимизации простой метрики, которая является числом переходов до места назначения. RIP посылает периодические обновления с заданной частотой. Каждое обновление содержит пары значений, состоящих из IP-адреса и расстояния до узла с этим IP-адресом.

В системе реализована поддержка протокола RIP версий 1 и 2 в соответствии с документами RFC2453, RFC2082, RFC1724. Пользователь может указать используемую версию на интерфейсе. По умолчанию RIP выключен на всех интерфейсах и в системе в целом. При включении по умолчанию используется RIP версии 1. Для передачи сообщений RIP версии 1 в адресе получателя используется широковещательный адрес 255.255.255.255, а RIP версии 2 — мультикаст адрес 224.0.0.9. RIP для транспорта обновлений использует протокол UDP порт 520.

router rip enable

Команда включает процесс маршрутизации RIP. Использование префикса **no** отключает процесс маршрутизации.

Синтаксис:
router rip enable
no router rip enable

Состояние по умолчанию:
Протокол маршрутизации RIP отключен

Режим ИКС:
Режим Общей настройки

rip

Команда включает процесс маршрутизации RIP на интерфейсе. Использование префикса **no** отключает процесс маршрутизации.

Синтаксис:
rip
no rip

Состояние по умолчанию:
Протокол маршрутизации RIP отключен на всех интерфейсах

Режим ИКС:
Режимы Настройки интерфейса (IP)

rip version

Команда определяет версию протокола RIP на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
rip version {*1* | *2*}
no rip version

Параметры:
- *1* – определяет, что протокол RIP версии 1 используется на интерфейсе,
- *2* – определяет, что протокол RIP версии 2 используется на интерфейсе.

Состояние по умолчанию:
Версия протокола RIP по умолчанию – 1

Режим ИКС:
Режимы Настройки интерфейса (IP)

rip passive-interface

Команда отключает отправку периодических обновлений на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
`rip passive-interface`
`no rip passive-interface`

Состояние по умолчанию:
Обновления маршрутизации отправляются периодически

Режим ИКС:
Режимы Настройки интерфейса (IP)

Пояснения:
Если отправка обновлений маршрутизации на интерфейсе отключена:
- подсеть, настроенная на интерфейсе, продолжает быть объявленной через другие интерфейсы, на которых запущен протокол маршрутизации RIP;
- обновления от других маршрутизаторов на этом интерфейсе поступают поступать и обрабатываться.

`show ip rip`
Команда отображает текущее состояние процесса маршрутизации RIP.

Синтаксис:
`show ip rip` [**`md5`** | **`statistics`** | **`peer`**]

Параметры:
- **`md5`** – отображает информацию об MD5 аутентификации,
- **`statistics`** – отображает статистическую информацию,
- **`peer`** – отображает информацию о соседних маршрутизаторах.

Режим ИКС:
Привилегированный режим

14.4 Настройка протокола маршрутизации OSPF

OSPF является внутридоменным протоколом динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры. OSPF характеризуется высокой скоростью сходимости по сравнению с дистанционно-векторными протоколами маршрутизации, а также оптимальным использованием пропускной способности интерфейсов с построением дерева кратчайших путей. При выборе кратчайшего маршрута анализируется не только расстояния до узла с этим IP-адресом, но и скорости интерфейсов на всем пути.

В системе реализована поддержка протокола OSPF версии 2 в соответствии с документом RFC2328. OSPF инкапсулируется в IP (номер протокола 89). Для передачи пакетов использует мультикаст адреса: 224.0.0.5 и 224.0.0.6.

`router ospf enable`
Команда включает процесс маршрутизации OSPF. Использование префикса **`no`** отключает процесс маршрутизации.

Синтаксис:
router ospf enable
no router ospf enable

Состояние по умолчанию:
Протокол маршрутизации OSPF отключен

Режим ИКС:
Режим Общей настройки

router ospf area

Команда определяет OSPF зону – логическую совокупность сетей и интерфейсов маршрутизаторов, имеющих один и тот же идентификатор. Использование префикса **no** удаляет OSPF зону с процесса маршрутизации.

Синтаксис:
router ospf area *area-id*
no router ospf area *area-id*

Параметры:
– *area-id* – номер OSPF зоны. Должна быть указана в формате IP-адреса.

Состояние по умолчанию:
Только магистральная зона (area 0) определена

Режим ИКС:
Режим Общей настройки

router ospf area stub

Команда определяет OSPF зону тупиковой. Использование префикса **no** определяет OSPF зону нормальной.

Синтаксис:
router ospf area *area-id* **stub**
no router ospf area *area-id* **stub**

Параметры:
– *area-id* – номер OSPF зоны. Должна быть указана в формате IP-адреса.

Состояние по умолчанию:
Тупиковая зона не определена

Режим ИКС:
Режим Общей настройки

Пояснения:
Если зона тупиковая, она должна быть определена тупиковой на всех маршрутизаторах этой зоны.

router ospf router-id

Команда определяет уникальный идентификатор для OSPF маршрутизатора. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
router ospf router-id *ip-address*
no router ospf router-id

Параметры:
– *ip-address* – уникальный идентификатор для OSPF маршрутизатора

Состояние по умолчанию:
IP-адрес первого IP интерфейса

Режим ИКС:
Режим Общей настройки

Пояснения:
Router ID – это уникальное имя маршрутизатора, по которому он известен в сети. Его совпадение на нескольких маршрутизаторах может вызвать сбой в работе маршрутизации во всей сети. После изменения Router ID, для корректной работы процесс OSPF должен быть перезагружен.

ospf enable

Команда включает процесс маршрутизации OSPF на интерфейсе. Использование префикса **no** отключает процесс маршрутизации.

Синтаксис:
ospf enable
no ospf enable

Состояние по умолчанию:
Включен

Режим ИКС:
Режимы Настройки интерфейса (IP)

ospf area

Команда включает процесс маршрутизации OSPF на интерфейсе в заданной зоне. Использование префикса **no** отключает процесс маршрутизации.

Синтаксис:
ospf area *area-id*
no ospf area

Параметры:
– *area-id* – номер OSPF зоны. Должна быть указана в формате IP-адреса.

Состояние по умолчанию:
0.0.0.0

Режим ИКС:
Режимы Настройки интерфейса (IP)

ospf cost

Команда определяет стоимость пересылки данных по каналу на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
ospf cost *interface-cost*
no ospf cost

Параметры:
– *interface-cost* – значение стоимости интерфейса: (1-65535).

Состояние по умолчанию:
10^8 разделенная на скорость интерфейса, но не менее чем 1.

Режим ИКС:
Режимы Настройки интерфейса (IP)

ospf priority

Команда определяет приоритет маршрутизатора, используемый для выбора выделенного (DR) и резервного выделенного (BDR) маршрутизаторов. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
ospf priority *number-value*
no ospf priority

Параметры:
– *number-value* – значение приоритета маршрутизатора: (0-255).

Состояние по умолчанию:
1

Режим ИКС:
Режимы Настройки интерфейса (IP)

Пояснения:
В сетях со множественным доступом отношения соседства должны быть установлены между всеми маршрутизаторами. Это приводит к тому, что рассылается большое количество OSPF обновлений. Для предотвращения проблемы рассылки в сетях со множественным доступом выбираются DR и BDR. Маршрутизатор с большим значением приоритета становится DR. Если значение приоритета равно нулю – маршрутизатор не может стать DR или BDR.

show ip ospf

Команда отображает текущее состояние процесса маршрутизации OSPF.

Синтаксис:
show ip ospf

Режим ИКС:
Привилегированный режим

15. Настройка списков контроля доступа (ACL)

Правила фильтрации трафика, проходящего через коммутатор, реализованы на основе применения списков контроля доступа (Access Control List - ACL) к интерфейсам устройства. Данные списки позволяют фильтровать проходящие пакеты по IP-адресу или MAC-адресу отправителя и получателя, типу протокола, параметрам портов и других характеристикам.

Списки контроля доступа ACL применяются к отдельным интерфейсам и обрабатывают входящий трафик. Система в целом поддерживает до 2048 списков ACL. При этом каждый список ACL может состоять из одного или несколько правил доступа (Access Control Element - ACE). Если список ACL состоит из нескольких правил доступа ACE, то проверка пакета начинается последовательно по этим правилам до первого совпадения, после чего проверка на соответствие остальным правилам не производится. Поэтому порядок следования правил в списке ACL имеет большое значение.

В случае соответствия пакета какому-либо правилу производится указанное в этом правиле действие над пакетом – пересылка по адресу назначения, отбрасывание и т.д. Один и тот же список ACL можно применить к нескольким интерфейсам, при этом сами списки контроля доступа можно сконфигурировать на ПК и затем при необходимости загрузить их в устройство и применить к интерфейсам. Списки ACL можно применять к физическим портам или агрегированным каналам.

При создании списков ACL следует учитывать следующие ограничения:

- Списки ACL на базе IPv6, IPv4 и MAC-адресов не должны иметь одинаковые названия.
- Списки ACL на базе IPv4 и IPv6 могут работать вместе на одном физическом интерфейсе. Но список ACL на базе MAC-адресации не может совмещаться со списками для IPv4 или IPv6. Для их совместного использования необходимо создавать списки критериев классификации трафика на основе QoS.
- Два списка одинакового типа не могут быть применены к одному и тому же интерфейсу.

15.1 Настройка списков ACL на базе IP

Далее в данном разделе описаны команды для создания, удаления и редактирования списков контроля доступа ACL на базе IP-адресов отправителя и получателя фильтруемого трафика.

Примечание: Далее описание всех настроек и команд в данном разделе приведено для случая использования IP-адресов формата IPv4. Вместе с тем в системе реализована полнофункциональная поддержка списков ACL на базе IPv6. При этом в синтаксисе или параметрах соответствующих команд, как правило, достаточно заменить **ip** на **ipv6**.

ip access-list extended

Команда используется для создания нового списка контроля доступа на основе адресов формата IPv4 или для входа в режим редактирования существующего списка с указанным названием. Использование префикса **no** удаляет существующий список контроля доступа с указанным названием.

Синтаксис:

ip access-list extended *access-list-name*
no ip access-list extended *access-list-name*

Параметры:

– *access-list-name* – название списка контроля доступа (от 0 до 32 символов).

Состояние по умолчанию:
Списков на основе IP не существует.

Режим ИКС:
Режим Общей настройки

Пояснения:
Для создания списка ACL на базе IPv6 необходимо использовать команду **ipv6 access-list** режима Общей настройки.

permit

Команда используется для создания разрешающего правила фильтрации в списке контроля доступа ACL.

Синтаксис:
permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*dscp number*| *precedence number*] [**time-range** *time-range-name*] [**log-input**]

Для протоколов ICMP, IGMP, а также групп протоколов TCP и UDP данная команда имеет специальный синтаксис:

permit icmp {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*] [*dscp number* | *precedence number*] [**time-range** *time-range-name*] [**log-input**]

permit igmp {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*igmp-type*] [*dscp number* | *precedence number*] [**time-range** *time-range-name*] [**log-input**]

permit tcp {**any** | *source source-wildcard*} {**any** | *source-port*} {**any** | *destination destination-wildcard*} {**any** | *destination-port*} [*dscp number* | *precedence number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input**]

permit udp {**any** | *source source-wildcard*} {**any** | *source-port*} {**any** | *destination destination-wildcard*} {**any** | *destination-port*} [*dscp number* | *precedence number*] [*match-all list-of-flags*] [**time-range** *time-range-name*] [**log-input**]

Параметры:

– *protocol* – название или номер IP-протокола. Доступные названия протоколов: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis.
– *source* – IP-адрес отправителя пакета,
– *source-wildcard* – битовая маска, применяемая к IP-адресу отправителя пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы,
– *destination* – IP-адрес получателя пакета,

- *destination-wildcard* – битовая маска, применяемая к IP-адресу получателя пакета,
- *dscp number* – значение DSCP-поля diffserv в заголовке пакета. Возможные коды сообщений поля dscp: (0 – 63),
- *precedence number* – значение приоритета IP-трафика: (0-7),
- *precedence number* – значение приоритета IP-трафика: (0-7),
- *time-range-name* – имя профиля конфигурации временных интервалов действия правила (от 1 до 32 символов),
- **log-input** – отправка информационного сообщения в журнал Syslog при получении пакета, который соответствует правилу,
- *icmp-type* – тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Необходимо ввести номер типа (0-255) или одно из следующих значений: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris
- *icmp-code* – код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов (0-255),
- *igmp-type* – тип сообщений протокола IGMP, используемый для фильтрации IGMP-пакетов (0-255). Необходимо ввести номер типа (0-255) или одно из следующих значений: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3.
- *source-port* – UDP/TCP-порт отправителя. Необходимо указать номер порта (0-65535) или одно из следующих значений: для TCP: chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); для UDP: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds(49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Можно указать диапазон портов через дефис,
- *destination-port* – UDP/TCP-порт назначения. Параметры аналогичны *source-port*,
- *list-of-flags* – Списков флажков протокола TCP. Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin. При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку без пробелов, например: +fin-ack.

Состояние по умолчанию:
Весь трафик разрешен.

Режим ИКС:
Режим настройки Списков контроля доступа по IP-адресу

Пояснения:
После включения первого правила доступа ACE в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **permit**. Т.е. если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к

дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.
При включении параметра **log-input** система при каждом получении пакета, который соответствует правилу, отправляет в журнал Syslog информационное сообщение об этом. Генерация такого сообщения производится с участием ЦПУ, который работает с частотой, значительной меньшей частоты сетевого процессора, т.е. регистрация пакетов по установленному правилу фильтрации может привести к значительному снижению пропускной способности порта коммутатора, к которому это правило применено. Поэтому при использовании данного правила фильтрации с включенным параметром **log-input** рекомендуется ограничить скорость входящего трафика с помощью команды **rate-limit**.

deny

Команда используется для создания запрещающего правила фильтрации в списке контроля доступа ACL.

Синтаксис:
deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*dscp number*| *precedence number*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

Для протоколов ICMP, IGMP, а также групп протоколов TCP и UDP данная команда имеет специальный синтаксис:

deny icmp {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*] [*dscp number* | *precedence number*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

deny igmp {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*igmp-type*] [*dscp number* | *precedence number*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

deny tcp {**any** | *source source-wildcard*} {**any** | *source-port*} {**any** | *destination destination-wildcard*} {**any** | *destination-port*} [*dscp number* | *precedence number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

deny udp {**any** | *source source-wildcard*} {**any** | *source-port*} {**any** | *destination destination-wildcard*} {**any** | *destination-port*} [*dscp number* | *precedence number*] [*match-all list-of-flags*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

Параметры:
- параметры команды аналогичны параметрам команды **permit**,
- **disable-port** – отключение порта, с которого был принят пакет, удовлетворяющий условиям запрещающего правила.

Состояние по умолчанию:
Весь трафик разрешен.

Режим ИКС:
Режим настройки Списков контроля доступа по IP-адресу

Пояснения:
После включения первого правила доступа в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **permit**. Т.е. если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.
При включении параметра **log-input** система при каждом получении пакета, который соответствует правилу, отправляет в журнал Syslog информационное сообщение об этом. Генерация такого сообщения производится с участием ЦПУ, который работает с частотой, значительной меньшей частоты сетевого процессора, т.е. регистрация пакетов по установленному правилу фильтрации может привести к значительному снижению пропускной способности порта коммутатора, к которому это правило применено. Поэтому при использовании данного правила фильтрации с включенным параметром **log-input** рекомендуется ограничить скорость входящего трафика с помощью команды **rate-limit**.

15.2 Настройка списков ACL на базе MAC

Далее в данном разделе описаны команды для создания, удаления, редактирования и просмотра списков контроля доступа ACL на базе MAC-адресов отправителя и получателя фильтруемого трафика.

mac access-list extended

Команда используется для создания нового списка контроля доступа на основе MAC-адресов или для входа в режим редактирования существующего списка с указанным названием. Использование префикса **no** удаляет существующий список контроля доступа с указанным названием.

Синтаксис:
mac access-list extended *access-list-name*
no mac access-list extended *access-list-name*

Параметры:
– *access-list-name* – название списка контроля доступа (от 0 до 32 символов).

Состояние по умолчанию:
Списков на основе MAC не существует.

Режим ИКС:
Режим Общей настройки

permit (MAC)

Команда используется для создания разрешающего правила фильтрации в списке контроля доступа ACL на базе MAC.

Синтаксис:
permit {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**eth-type** *eth-type*] [**vlan** *vlan-id*] [**cos** *cos-wildcard*] [**time-range** *time-range-name*]

Параметры:

- *source* – MAC-адрес отправителя пакета,
- *source-wildcard* – маска, применяемая к MAC-адресу отправителя пакета для определения битов адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, для адресов 00:00:02:AA.xx.xx необходимо задать значение маски 0.0.0.0.FF.FF,
- *destination* – MAC-адрес получателя пакета,
- *destination-wildcard* – маска, применяемая к MAC-адресу получателя пакета,
- *eth-type* – Ethernet-тип фильтруемых пакетов в шестнадцатеричной записи (0-0xFFFF),
- *vlan-id* – номер VLAN,
- *cos* – класс обслуживания (CoS) фильтруемых пакетов (0-7),
- *cos-wildcard* – Битовая маска, применяемая к классу обслуживания (CoS), определяет биты CoS, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы,
- *time-range-name* – имя профиля конфигурации временных интервалов действия правила (от 1 до 32 символов).

Состояние по умолчанию:
Весь трафик разрешен.

Режим ИКС:
Режим настройки Списков контроля доступа по MAC-адресу

Пояснения:
После включения первого правила доступа ACE в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **permit**. Т.е. если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.

deny (MAC)

Команда используется для создания разрешающего правила фильтрации в списке контроля доступа ACL на базе MAC.

Синтаксис:
deny {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**eth-type** *eth-type*] [**vlan** *vlan-id*] [**cos** *cos-wildcard*] [**time-range** *time-range-name*] [**disable-port** | **log-input**]

Параметры:

- параметры команды аналогичны параметрам команды **permit** (MAC),
- **disable-port** – отключение порта, с которого был принят пакет, удовлетворяющий условиям запрещающего правила,
- **log-input** – отправка информационного сообщения в журнал Syslog при получении пакета, который соответствует правилу.

Состояние по умолчанию:
Весь трафик разрешен.

Режим ИКС:
Режим настройки Списков контроля доступа по MAC-адресу

Пояснения:
После включения первого правила доступа ACE в список контроля доступа ACL в его конец в неявном виде автоматически добавляется запрещающее правило на весь остальной трафик, не соответствующий данному правилу **permit**. Т.е. если в списке не окажется ни одного правила, которому пакет будет соответствовать, то такой пакет будет запрещен к дальнейшей пересылке. До тех пор, пока в список не включено ни одного запрещающего или разрешающего правила, все пакеты считаются разрешенными.

15.3 Применение списков ACL и установка временных параметров

Далее в данном разделе описаны команды для просмотра и применения списков контроля доступа ACL на базе IP-адресов и MAC-адресов к проходящему через коммутатор трафику, а также для установки временных интервалов действия правил фильтрации.

service-acl input

Команда применяет указанный список контроля доступа к физическому интерфейсу. Использование префикса **no** удаляет список контроля доступа с физического интерфейса.

Синтаксис:
service-acl input *acl-name1* [*acl-name2*]
no service-acl input

Параметры:
– *acl-name* – название применяемого списка контроля доступа ACL

Состояние по умолчанию:
К интерфейсам списки ACL не применены.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, VLAN, Port-channel)

Пояснения:
Списки ACL на базе IPv4 и IPv6 могут работать вместе на одном физическом интерфейсе.

Два списка одинакового типа не могут быть применены к одному и тому же интерфейсу.

К интерфейсу, к которому уже применен список ACL, нельзя добавить другой список ACL. Для этого нужно вначале удалить с интерфейса уже существующий список ACL, а затем применить два списка ACL совместно.

show access-lists

Команда отображает все списки контроля доступа, существующие в системе, или список ACL с указанными параметрами.

Синтаксис:
show access-lists [**time-range-active**] [*name*]

Параметры:
– **time-range-active** – отображать только те списка ACL, которые в текущий момент активны,
– *name* – название отображаемого списка ACL.

Режим ИКС:
Привилегированный режим

show interfaces access-lists

Команда отображает все списки контроля доступа ACL, примененные к интерфейсам коммутатора к выбранному интерфейсу.

Синтаксис:
show interfaces access-lists [*interface-id*]

Параметры:
– *interface-id* – идентификатор интерфейса, которым может быть физический порт, агрегированный канал или VLAN.

Режим ИКС:
Привилегированный режим

clear access-lists counters

Команда обнуляет все счетчики списков ACL, либо счетчики для списков ACL заданного интерфейса.

Синтаксис:
clear access-lists counters [*interface-id*]

Параметры:
– *interface-id* – идентификатор интерфейса, которым может быть физический порт или агрегированный канал

Режим ИКС:
Привилегированный режим

show interfaces access-lists counters

Команда отображает счетчики списков контроля доступа ACL.

Синтаксис:
show interfaces access-lists counters [*interface-id*]

Параметры:
– *interface-id* – идентификатор интерфейса, которым может быть физический порт или агрегированный канал

Режим ИКС:

Привилегированный режим

time-range

Команда используется для входа в режим конфигурирования временных интервалов действия правил фильтрации и определения временных интервалов для списков контроля доступа ACL. Использование префикса **no** удаляет временные интервалы.

Синтаксис:
time-range *time-range-name*
no time-range *time-range-name*

Параметры:
– *time-range-name* – имя профиля настроек временных интервалов

Состояние по умолчанию:
Временные интервалы не заданы

Режим ИКС:
Режим Общей настройки

Пояснения:
Активные профили временных интервалов удалить нельзя.
Все параметры задаются в значениях локального времени.
Профиль может как из абсолютных, так и из нескольких относительных (периодических) временных интервалов.

absolute

Команда устанавливает абсолютные время и дату начала и завершения действия списка контроля доступа ACL. Использование префикса **no** удаляет ограничение по времени

Синтаксис:
absolute start *hh:mm day month year*
no absolute start

absolute end *hh:mm day month year*
no absolute end

Параметры:
– **start** – абсолютное время и дата вступления в действие правила доступа,
– **end** – абсолютное время и дата завершения действия правила доступа,
– *hh*:*mm* – часы (0-23), минуты (0-59),
– *day* – день месяца (1-31),
– *month* – месяц года (*Jan-Dec*),
– *year* – год (2000-2097).

Состояние по умолчанию:
Временные интервалы не заданы

Режим ИКС:
Режим настройки Временных интервалов

periodic

Команда устанавливает время и день недели действия списка контроля доступа ACL. Использование префикса **no** удаляет ограничение по времени.

Синтаксис:

periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*
no periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*
periodic list *hh:mm* **to** *hh:mm day-of-the-week1* [*day-of-the-week2* … *day-of-the-week7*]
no periodic list *hh:mm* **to** *hh:mm day-of-the-week1* [*day-of-the-week2* … *day-of-the-week7*]
periodic list *hh:mm* **to** *hh:mm* **all**
no periodic list *hh:mm* **to** *hh:mm* **all**

Параметры:

– *day-of-the-week* – день недели (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday),
– *hh*:*mm* – часы (0-23), минуты (0-59),

Состояние по умолчанию:
Временные интервалы не заданы

Режим ИКС:
Режим настройки Временных интервалов

show time-range

Команда используется для отображения выбранных временных интервалов действия правил фильтрации.

Синтаксис:

show time-range *time-range-name*

Параметры:

– *time-range-name* – имя профиля настроек временных интервалов

Режим ИКС:
Пользовательский режим

16. Настройка механизмов контроля качества обслуживания (QoS)

16.1 Поддержка механизмов QoS

Система позволяет пользователю разделять и приоритезировать транспортные потоки в зависимости от конкретных услуг, для которых они предназначены. Такое поведение устройства достигается за счет двух механизмов:

Классификация – пользователь указывает некоторые значения определенным полям внутри пакета. Все пакеты, у которых значения этих полей соответствуют, соответствуют одному и тому же потоку/классу.

Действия – пользователь может установить различные действия, такие как манипуляции поля в пакете (например, VPT, DSCP), ограничение пропускной способности (policing) интерфейса, планирование и сглаживание (scheduling and shaping) трафика на выходе интерфейса. Те же действия применяются ко всем пакетам определенного потока.

Основной механизм, поддерживающий большинство действий, связанных с управление полосой пропускания и контроль – управление очередями. После того, как пакет был классифицирован, он направляется в одну из выходных очередей интерфейса. Система поддерживает 8 очередей на порт. Система обслуживает очереди (отправляет пакеты из очереди) в соответствии с текущими настройками планирования очереди, которые определяются пользователем. Эти параметры определяют, какая очередь обрабатывается и сколько пакетов из этой очереди будет обрабатываться раньше других очередей.

16.2 Настройка механизмов QoS

qos

Команда включает механизмы QoS и определяет режим их работы. Использование префикса **no** отключения механизмов QoS.

Синтаксис:
qos [*basic* | *advanced [ports-not-trusted* | *ports-trusted]*]
no qos

Параметры:
- *basic* – основной режим работы QoS,
- *advanced*– расширенный режим работы QoS,
- *ports-not-trusted* – применимо только для расширенного режима работы QoS. Указывает, что пакеты, которые не были классифицированы, отправляются в очередь 0. Это значение по умолчанию в расширенном режиме,
- *ports-trusted* – применимо только для расширенного режима работы QoS. Указывает, что пакеты, которые не были классифицированы, отображаются в очереди выхода на основе полей пакета.

Состояние по умолчанию:
Если команда **qos** введена без аргументов, включается основной режим работы QoS.
Если команда **qos advanced** введена без аргументов, по умолчанию используется режим **ports-not-trusted.**

Режим ИКС:
Режимы Режим Общей настройки.

class-map

Команда используется для создания и модификации классовой карты, которая позволяет реализовать классификацию и маркировку пакетов. Состоит из одного или нескольких ACL и определяет одному или всем полям ACL должен совпадать пакет, чтобы быть промаркированным. Использование префикса **no** удаляет существующую классовую карту с указанным названием. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
class-map *class-map-name* [*match-all* | *match-any*]
no class-map *class-map-name*

Параметры:
- *class-map-name* – название классовой карты,
- *match-all* – выполнять логическое И всех полей ACL. Пакет должен соответствовать всем полям ACL чтобы быть промаркированным,
- *match-any* – выполнять логическое ИЛИ всех полей ACL. Пакет должен соответствовать одному из полей ACL чтобы быть промаркированным.

Состояние по умолчанию:
Если не аргумент не указан *match-all* используется по умолчанию.

Режим ИКС:
Режим Общей настройки

Пояснения:
До двух *match* команд может быть использовано в одной классовой карде. Каждая определяет ACL разных типов (IP ACL и MAC ACL).

match

Команда используется для привязки ранее созданного ACL с class-map. Использование префикса **no** дает возможность удалить привязку. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
match access-group *acl-name*
no match access-group *acl-name*

Параметры:
- *acl-name* – название IP ACL или MAC ALC.

Состояние по умолчанию:
Привязки ACL с class-map не существуют

Режим ИКС:
Режим настройки Class-map

policy-map

Команда используется для создания и модификации карты политик, которая состоит из одной или нескольких классовых карт и описывает действие над трафиком, соответствующим этим картам. Использование префикса **no** удаляет существующую карту политик с указанным названием. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
policy-map *policy-map-name*
no policy-map *policy-map-name*

Параметры:
– *policy-map-name* – название карты политик (1-32 символ).

Состояние по умолчанию:
Карты политик не созданы.

Режим ИКС:
Режим Общей настройки

Пояснения:
Команда *service-policy* привязывает карту политик к интерфейсу (используется для входящего направления).

class

Команда используется для привязки class-map к policy-map. Использование префикса **no** удаляет существующую привязку с указанными названиями. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
class *class-map-name* [**access-group** *alc-name*]
no class *class-map-name*

Параметры:
– *class-map-name* – название классовой карты,
– *acl-name* – название IP ACL или MAC ALC.

Состояние по умолчанию:
Привязки не созданы.

Режим ИКС:
Режим настройки карты политик

trust

Команда используется для настройки состояния доверия, в котором трафик отправляется в очередь в соответствии с его изначальными значениями параметров QoS. Использование префикса **no** восстановит установки по умолчанию. Команда доступна только в расширенном режиме работы QoS, в состоянии ports-not-trusted.

Синтаксис:
trust
no trust

Состояние по умолчанию:
Определяется при включении механизма QoS

Режим ИКС:
Режим настройки карты политик

Пояснения:
Команда *set* и *trust* взаимоисключающиеся в пределах одной карты политик.

set

Команда устанавливает значения, которое QoS использует в качестве значения DSCP для определения приоритета трафика. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}
no set

Параметры:
- *new-dscp* – значение DSCP для класифицированного трафика (0-63),
- *queue-id* – номер исходящей очереди (1-8),
- *new-cos* – значение приоритета пакета (0-7).

Режим ИКС:
Режим настройки карты политик

Пояснения:
Команда *set* и *trust* взаимоисключающиеся в пределах одной карты политик.

police

Команда устанавливает ограничение скорости для классифицированного трафика. Использование префикса **no** снимает ограничение скорости классифицированного трафика. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
police *committed-rate-kbps committed-burst-byte* [**exceed-action** *{drop | policed-dscp-transmit}*]
no police

rate-limit *vlan-id committed-rate committed-burst-byte*
no rate-limit *vlan-id*

Параметры:
- *committed-rate-kbps* – средняя скорость трафика в кбит/сек (от 3 до 10485760 кбит/сек),

- *committed-burst-byte* – размер сдерживающего порога (ограничение скорости) в байтах (от 3000 до 19173960 кбит/с),
- *drop* – удалить пакет,
- *policed-dscp-transmit* – изменит значение DSCP пакета в соответствии с policed-DSCP map.

Режим ИКС:
Режим настройки карты политик

service-policy

Команда применяет указанную карту политик к физическому интерфейсу. Использование префикса **no** удаляет карту политик с физического интерфейса. Команда доступна только в расширенном режиме работы QoS.

Синтаксис:
service-policy input *policy-map-name*
no service-policy input

Параметры:
- *policy-map-name* – название карты политик (1-32 символ).

Состояние по умолчанию:
К интерфейсам карты политик не применены.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel)

Пояснения:
Две карты политик не могут быть применены к одному и тому же интерфейсу в одном направлении.

show qos

Команда отображает текущее состояние механизмов контроля качества QoS.

Синтаксис:
show qos

Режим ИКС:
Привилегированный режим

rate-limit

Команда устанавливает ограничение скорости для входящего трафика на порту или VLAN. Использование префикса **no** снимает ограничение скорости входящего трафика.

Синтаксис:
rate-limit *committed-rate-kbps* [**burst** *committed-burst-byte*]
no rate-limit

rate-limit *vlan-id committed-rate committed-burst-byte*
no rate-limit *vlan-id*

Параметры:

- *committed-rate-kbps* – максимально допустимая скорость входящего трафика на порту в кбит/с (от 3 до 10485760 кбит/с),
- *committed-burst-byte* – размер сдерживающего порога (ограничение скорости) в байтах (от 3000 до 19173960 кбит/с), по умолчанию 128 кбайт,
- *vlan-id* – номер VLAN,
- *committed-rate* – средняя скорость входящего трафика в VLAN в кбит/с (от 3 до 57982058 кбит/с).

Состояние по умолчанию:
Ограничения скорости трафика нет.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet) или Режим Общей настройки (для VLAN).

17. Настройка механизмов обеспечения безопасности

17.1 Настройка MAC-based Port Security

Функция используется для повышения безопасности путем ограничения MAC адресов, связанных с определенным портом. Порт может работать в следующих режимах:

- Регулярный небезопасный – количество хранимых динамических MAC-адресов на порту ограничено размером таблицы MAC-адресов,
- Ограниченный небезопасный – количество хранимых динамических MAC-адресов на порту ограничено конфигурацией,
- Безопасный – адреса, связанные с портом, зарезервированы статически, динамическое обучение отключено.

port security

Команда включает механизм обеспечения безопасности Port Security и определяет режим их работы. Использование префикса **no** отключает механизм Port Security.

Синтаксис:

port security [*forward* | *discard* | *discard-shutdown*][**trap** *seconds*]
no port security

Параметры:

- *forward* – пересылать пакеты с неизвестным MAC-адресом отправителя, но не изучать этот адрес,
- *discard* – отбросить пакеты с неизвестным MAC-адресом отправителя,
- *discard-shutdown* – отбросить пакеты с неизвестным MAC-адресом отправителя и выключить порт, с которого они получены,
- *seconds* – минимальный интервал времени между последовательными SNMP сообщениями (1-1000000).

Состояние по умолчанию:

Функционал выключен по умолчанию.

Режим по умолчанию *discard*.

Последовательными SNMP сообщениями по умолчанию отправляются без задержки (интервал времени равен 0 секунд)

Режим ИКС:

Режимы Настройки интерфейса (Ethernet, Port-channel)

port security mode

Команда определяет режим работы механизма Port Security на интерфейсе. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:

port security mode {*max-addresses* | *lock* | *secure permanent* | *secure delete-on-reset*}
no port security mode

Параметры:

- *max-addresses* – небезопасный режим с ограничением динамического изучения MAC-адресов, статические адреса могут быть добавлены дополнительно командой **bridge unicast unknown,**
- *lock* – безопасный режим, не предусматривающий возможность динамического изучения MAC-адресов, статические адреса могут быть добавлены командой **bridge unicast unknown,**
- *secure permanent* – безопасный режим с ограниченным динамического изучения безопасных MAC-адресов с постоянным временем хранения,
- *secure delete-on-reset* – безопасный режим с ограниченным динамического изучения безопасных MAC-адресов, которые удаляются после перезагрузки.

Состояние по умолчанию:
Режим по умолчанию *lock*.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel)

port security max

Команда определяет максимальное количество MAC-адресов, которое может изучить интерфейс, находящийся в режиме *max-addresses*. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
port security max *max-addr*
no port security max

Параметры:

- *max-addr* – максимальное количество адресов, которое может изучить интерфейс (0-256)

Состояние по умолчанию:
1

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel)

show port security

Команда отображает информацию о состоянии механизма Port Security.

Синтаксис:
show port-security [*interface-id* | **detailed**]

Параметры:

- *interface-id* – номер интерфейса, информацию о котором необходимо отобразить,
- *detailed* – отобразить подробную информацию о состоянии механизма обеспечения безопасности Port Security.

Режим ИКС:
Пользовательский режим

17.2 Контроль доступа на основе проверки подлинности по стандарту IEEE 802.1x

Контроль доступа к сети по стандарту IEEE 802.1x использует физические характеристики сетевой инфраструктуры для обеспечения аутентификации и авторизации устройств, подключенных к портам устройства.

Согласно протоколу 802.1X доступ к сети получают только клиенты прошедшие аутентификацию, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен. 802.1X предполагает использование модели точка-точка. То есть он не может быть применен в ситуациях когда несколько хостов соединяются с коммутатором (на котором настроена аутентификация 802.1X) через хаб или через другой коммутатор. В качестве сервера аутентификации должен использоваться предварительно развернутый внешний RADIUS сервер.

dot1x system-auth-control

Команда включает протокол 802.1x на устройстве. Использование префикса **no** отключает протокол 802.1x.

Синтаксис:

```
dot1x system-auth-contr
no dot1x system-auth-contr
```

Состояние по умолчанию:
Протокол выключен по умолчанию.

Режим ИКС:
Режим Общей настройки

radius-server host

Команда определяет внешний RADIUS сервер. Использование префикса **no** удалит настройки RADIUS сервера.

Синтаксис:

```
radius-server host {ip-address | hostname}[auth-port auth-port-number]
[acct-port acct-port-number][timeout timeout][retransmit retries]
[deadtime deadtime][key key-string][source source-ip][priority priority]
[usage {login | 802.1x | all}]
no radius-server host {ip-address | hostname}
```

Параметры:

- *ip-address* – IPv4, IPv6 или IPv6Z адрес RADIUS сервера,
- *hostname* – доменное имя сервера (до 158 символов),
- *auth-port-number* – номер порта для аутентификации (0-65535), по умолчанию – 1812.
- *acct-port-number* – номер порта для авторизации (0-65535), по умолчанию – 1813.
- *timeout* – время ожидания ответа в секундах (1-30),
- *retries* – количество попыток доступа к серверу (1-15),
- *deadtime* – время ожидания завершения транзакции в минутах (0-2000),
- *key-string* – ключ (0-128 символов),
- *source-ip* – IP-адрес источника,
- *priority* – приоритет сервера (0-65535) ,
- *login* – сервер используется только для аутентификации пользователей,

- *802.1x* – сервер используется только для 802.1x аутентификации портов,
- *all* – сервер используется для аутентификации пользователей и 802.1x аутентификации портов.

Состояние по умолчанию:
Функционал выключен по умолчанию.

Режим ИКС:
Режим Общей настройки

dot1x port-control

Команда настройки 802.1x аутентификации на порту.

Синтаксис:
dot1x system-auth-contr {auto | *force-authorized* | *force-unauthorized*}
[**time-range** *time-range-name*]

Параметры:
- auto – 802.1x аутентификация включена,
- *force-authorized* – 802.1x аутентификация выключена, порт в состоянии авторизован,
- *force-unauthorized* – 802.1x аутентификация выключена, порт в состоянии не авторизован,
- *time-range-name* – имя профиля конфигурации временных интервалов действия правила (от 1 до 32 символов).

Состояние по умолчанию:
Порт в состоянии *force-authorized*.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet, Port-channel)

dot1x mac-authentication

Команда настройки 802.1x аутентификации на порту на основании MAC-адреса клиента. Использование префикса **no** отключит функционал.

Синтаксис:
dot1x mac-authentication {mac-only | *mac-and-802.1x*}
no dot1x mac-authentication

Параметры:
- mac-only –аутентификация только на основе MAC-адреса клиента,
- *mac-and-802.1x* – 802.1x аутентификация и аутентификация на основе MAC-адреса клиента включены.

Состояние по умолчанию:
Аутентификации на порту на основании MAC-адреса клиента отключена.

Режим ИКС:
Режимы Настройки интерфейса (Ethernet)

Пояснения:
Гостевой VLAN должен быть включен для использования аутентификации на основе MAC-адреса.
Статические MAC-адреса не могут быть авторизированными.
Реаутентификация должна быть включена для работы аутентификации на основе MAC-адреса.

aaa authentication dot1x

Команда определяет какие сервера должны быть использованы для 802.1x аутентификации. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
aaa authentication dot1x default {radius | *none* | {*radius none*}}
no aaa authentication dot1x default

Параметры:
- radius –совокупность всех определенных RADIUS серверов,
- *none* – аутентификация не используется,
- *radius none* – в случае если сервер аутентификации недоступен, аутентификация пройдет успешно.

Состояние по умолчанию:
RADIUS сервер

Режим ИКС:
Режим Общей настройки

show dot1x

Команда отображает информацию о состоянии протокола 802.1X на интерфейсах.

Синтаксис:
show dot1x [**interface** *interface-id* | **detailed**]

Параметры:
- *interface-id* – номер интерфейса, информацию о котором необходимо отобразить,
- *detailed* – отобразить подробную информацию о состоянии протокола 802.1X на интерфейсах.

Режим ИКС:
Привилегированный режим

18. Настройка протокола SNMP

18.1 Поддержка протокола SNMP

Система управляется с помощью комбинации базы данных MIB (Management Information Base) переменных, чьи комбинации значений представляют все аспекты состояния системы, и протокола SNMP, предназначенного для изучения и изменения этих значений.

SNMP является базовым объектом системы. Все функции и также опции ее конфигурации отражаются в какой-то переменной MIB, и, как правило, во многих. Существуют обширные стандарты, охватывающие различные аспекты, касающиеся организации базы MIB, ее функционирования и взаимодействия с протоколом SNMP.

В системе реализована поддержка протокола SNMP версий 1, 2c и 3 в соответствии с документом RFC3410.

18.2 Настройка протокола SNMP

snmp-server server

Команда включает протокол SNMP на устройстве. Использование префикса **no** отключения протокола Open Flow.

Синтаксис:
snmp-server server
no snmp-server server

Состояние по умолчанию:
Протокол SNMP включен

Режим ИКС:
Режимы Режим Общей настройки.

snmp-server server community

Команда определяет пароль, разрешающий доступ к устройству по протоколу SNMP версий 1 и 2c. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
snmp-server server community *community-string* [*ro* | *rw* | *su*][*ip-address* | *ipv6-address*][**mask** *mask* | **prefix** *prefix-length*][**view** *view-name*]
no snmp-server server community *community-string* [*ip-address*]

Параметры:
- *community-string* – строка пароля, разрешающего доступ к устройству (1-20 символов),
- *ro* – доступ только для чтения, используется по умолчанию,
- *rw* – доступ для чтения и записи,
- *su* – доступ SNMP администратора,
- *ip-address* – IP-адрес управляющего устройства. По умолчанию – все IPv4, IPv6, IPv6Z адреса,
- *mask* – IPv4 маска подсети,

- *prefix-length* – IPv4 префикс подсети,
- *view-name* – список MIB объектов доступных для указанного пароля.

Состояние по умолчанию:
Пароль не определен

Режим ИКС:
Режим Общей настройки

snmp-server server user

Команда определяет пользователей протокола SNMP. Использование префикса **no** удалит пользователя протокола SNMP.

Синтаксис:
snmp-server user *username groupname* {*v1*|*v2c*|[**remote** *host*]v3[**auth**{*md5*|sha} auth-password[**priv** *priv-password*]]}
no snmp-server user *username* [**remote** *host*]

Параметры:
- *username* – имя пользователя (до 20 символов),
- *groupname* – имя группы, к которой принадлежит пользователя (до 30 символов),
- *host* – IP-адрес или доменное имя управляющего устройства,
- *v1* – пользователь SNMP версии 1,
- *v2c* – пользователь SNMP версии 2c,
- *v3* – пользователь SNMP версии 3,
- *md5* – уровень аутентификации HMAC-MD5-96,
- *sha* – уровень аутентификации HMAC-SHA-96,
- *auth-password* – строка пароля аутентификации (до 32 символов),
- *priv-password* – строка пароля шифрования (до 64 символов).

Состояние по умолчанию:
Пользователи не определены

Режим ИКС:
Режим Общей настройки

show snmp

Команда отображает информацию о состоянии протокола SNMP.

Синтаксис:
show snmp

Режим ИКС:
Привилегированный режим

19. Настройка протокола Open Flow (OF)

19.1 Поддержка протокола Open Flow

Протокол Open Flow предназначен для управления трафиком между маршрутизаторами и коммутаторами, созданными разными производителями. Он дает возможность отделить программное обеспечение устройства от его аппаратной реализации.

Open Flow позволяет программе контроллера, работающие на удаленной станции, классифицировать входящие на устройство пакеты по потоках. Она осуществляет это путем сопоставления заголовков пакетов с образцом, и указания необходимых действий (например, установка определенных VLAN тегов или отправка по определенному направлению) для пакетов, которые либо соответствуют, либо не соответствуют указанным образцам. Это означает, что коммутатор можно настраивать с помощью OpenFlow контроллера или с помощью обычных каналов управления коммутаторов (ИКС, графический интерфейс или оба). Таким образом, для функционирования подсистемы для каждого потока, имеются два канала управления, которые работают параллельно.

19.2 Настройка протокола Open Flow

`openflow enable`

Команда включает протокол Open Flow на устройстве. Использование префикса **`no`** отключения протокола Open Flow.

Синтаксис:
`openflow enable`
`no openflow enable`

Состояние по умолчанию:
Протокол Open Flow включен

Режим ИКС:
Режимы Режим Общей настройки.

Пояснения:
Команда вступает в силу только после перезагрузки устройства.

`openflow ip-address`

Команда определяет IP адрес Open Flow контроллера. Использование префикса **`no`** восстановит установки по умолчанию.

Синтаксис:
`openflow ip-addres` *`ip-address`*
`no openflow ip-addres` *`ip-address`*

Параметры:
- *`ip-address`* – IP-адресс Open Flow контроллера,

Состояние по умолчанию:
10.10.10.10

Режим ИКС:
Режим Общей настройки

Пояснения:
Команда вступает в силу только после перезагрузки устройства.

openflow protocol

Команда определяет протокол и номер порта для подключения к Open Flow контроллеру. Использование префикса **no** восстановит установки по умолчанию.

Синтаксис:
openflow protocol tcp {**tcp-port** [port-id]}
no openflow protocol

Параметры:
– port-id – TCP порт Open Flow контроллера,

Состояние по умолчанию:
TCP порт 6633

Режим ИКС:
Режим Общей настройки

Пояснения:
Команда вступает в силу только после перезагрузки устройства.

show openflow

Команда отображает информацию о состоянии протокола Open Flow на устройстве.

Синтаксис:
show openflow

Режим ИКС:
Привилегированный режим

20. Функциональная спецификация

В таблице приведен перечень основных функций, поддерживаемых коммутатором.

Функциональная спецификация

Раздел	**Функция**	**Описание**
Функции портов	Auto Negotiation	Автоматическое согласование скорости, дуплексного режима, управления потоком
	Auto MDI/MDIX	Автоматическое определение прямого и перекрестного типов кабеля
	Head of Line (HOL) Blocking Prevention	Защита от блокировки нескольких потоков на одном порту
	Flow Control Support (IEEE802.3X)	Управление потоком в полном дуплексном режиме для предотвращения потери пакетов
	Back Pressure Support	Механизм обратного давления для предотвращения переполнения буфера, в полудуплексном режиме
	Jumbo Frame	Полнофункциональная поддержка сверхдлинных пакетов размером до 9 Кбайт
	Optical Transceiver Analysis	Проверка подключенного оптического трансивера: напряжение, сила тока, входная и выходная мощность, температура, потеря сигнала, отказы трансивера.
	Manual Port Control and Identification	Ручная настройка порта: символьное описание, статус, параметры и др.
	Port Profiles	Поддержка макросов, т.е. сохраненных наборов консольных команд, содержащих конфигурацию порта
	Port Mirroring	Поддержка полного зеркалирования (дублирования) трафика портов для анализа и мониторинга. Поддерживается зеркалирование до 8 портов на 1 контролирующий порт
	VLAN Mirroring	Поддержка полного зеркалирования (дублирования) трафика сети VLAN для анализа и мониторинга
	Protected Ports	Изоляция интерфейсов друг от друга на 2-сетевом уровне
	Green Ethernet	Поддержка энергосберегающей технологии: отключение питания не использующегося порта, подстройка мощности под длину кабеля
MAC-адресация	MAC Table	Талица MAC-адресов размерностью до 16384

Раздел	Функция	Описание
		записей
	MAC Learning	Автоматическое «обучение» – формирование таблицы MAC-адресов
	VLAN-Aware MAC-BASEd Switching	Коммутация пакетов на основе MAC-адреса с учетом принадлежности к сети VLAN. Поддержка отдельной базы данных пересылки (Forwarding Data BASE,FDB) для каждой сети VLAN
	MAC Address Aging	Автоматическое удаление MAC-адресов, не активных в течение заданного времени, для предотвращения переполнения таблицы пересылки
	Static MAC Entries	Ручной (статический) ввод в таблицу пересылки MAC-адресов, не «устаревающих» и не удаляющихся после перезагрузки
Виртуальные локальные сети VLAN	VLAN Support	Поддержка до 4096 виртуальных локальных сетей VLAN
	Default VLAN	Сеть VLAN, существующая в коммутаторе по умолчанию при любых настройках.
	GVRP	Поддержка протокола GVRP для динамического создания сетей VLAN
	Port BASEd VLAN	Распределение по группам VLAN на основе портов
	Protocol BASEd VLANs	VLAN по признаку протокола L2, для изоляции трафика от уровня L3. Поддерживается до 8 таких сетей
	IPv4 Subnet-BASEd VLANs	Трансляция (mapping) трафика в сеть VLAN на основе подсети IP-адреса источника
	MAC-BASEd VLANs	Трансляция (mapping) трафика в сеть VLAN на основе MAC-адреса источника
	Voice VLAN	Автоматическое добавление VoIP-оборудования в сеть Voice VLAN на основе OUI для приоритезации трафика. Поддерживается до 128 OUI
	Multicast TV VLAN	Выделенные сети VLAN групповой передачи L2-трафика
	Triple Play, MVR	Вложенные сети VLAN (Q-in-Q) для передачи данных, голоса и видео с изоляцией на уровне L2. Поддержка протокола MVR
	Q-in-Q, Selective Q-in-Q	Поддержка вложенных сетей VLAN (стандарт IEEE 802.1Q , IEEE 802.1ad)

Раздел	Функция	Описание
Многоадресная передача уровня L2 (Multicast)	Multicast Bridging Mode	Поддержка различных режимов пересылки в базах FDB, независимо для IPv4 и IPv6
	Static Multicast Groups	Ручная настройка таблиц групповых адресов, когда не поддерживается IGMP. Поддерживается до 256 групп
	IGMP Snooping	Групповая передача на основе анализа IGMP-пакетов. Поддержка IGMP v1, v2, v3
	MLD Snooping	Групповая передача на основе анализа MLD-пакетов в сетях IPv6. Поддержка MLD v1, v2
	Flooding of Unregistered Multicast Frames	Настройка работы с пакетами, которые принадлежат незарегистрированным группам многоадресной рассылки
	IGMP Querier	Работа в режиме Querier в отсутствии в сети multicast-маршрутизатора
Spanning Tree	Per-device Spanning Tree	Поддержка протокола STP для построения древовидной топологии сети (802.1d)
	Rapid Spanning Tree	Поддержка "быстрого" протокола STP (IEEE802.1w)
	Multiple Spanning Tree	Поддержка протокола MSTP (IEEE802.1s) для привязки сетей VLAN к элементам в древовидной топологии (до 16 элементов)
	STP Root Guard	Защита от назначения несанкционированного устройства на роль «корневого элемента» древовидной топологии сети
	BPDU Filtering	Фильтрация BPDU-данных для разделения "деревьев" двух подсетей
	STP BPDU Guard	Автоматическое отключение порта при получении сообщения BPDU для защиты от неправильной конфигурации сети
	Per-device Loopback Detection (LBD)	Определение петель пересылки в L2-топологии сети, дополнительно к STP
Агрегирование каналов (Link Aggregation)	Link Aggregation Groups	Поддержка агрегирования нескольких физических каналов в один логический. Объединение до 8 портов в один канал, поддерживается до 8 объединенных каналов
	LACP	Поддержка протокола LACP для автоматического объединения отдельных связей в единый канал. Объединение до 16 портов-кандидатов
	LAG Balancing	Настройка баланса загрузки пропускной способности агрегированного канала на основе

Раздел	Функция	Описание
		MAC, IP или порта назначения
Качество обслуживания (Quality of Service)	QoS Basic mode (802.1p)	Поддержка приоритезации до 8 очередей на каждый порт, до 8 уровней приоритетов
	QoS Advanced Mode	Создание правил приоритезации (фильтрации) на основе классификации потоков
	Output Scheduling scheme	Выделение очередей с эксклюзивным приоритетом
	QoS Across the Stack	Распространение правил QoS на весь стэк устройств
	QoS statistics	Сбор статистики QoS на каждом порту по: очередям, классу трафика, примененным политикам
	Egress Rate Limiting (Shaping)	Ограничение скорости передачи пакетов заданного типа при сохранении параметров QoS на порту
	Ingress Rate Limiting	Ограничение скорости входящего трафика на порту на основе политик
	Packet Storm Control	Контроль скорости передачи широковещательных и многоадресных пакетов на входе порта
IP адресация	Static and DHCP/BootP	Статическое назначение коммутатору IP-адреса и его получение по протоколам DHCP/BootP. Одновременно поддерживается до 32 IP-адресов на коммутатор
	DNS Client	Поддержка до 8 DNS-серверов, до 64 статических назначений доменных имен
Поддержка IPv6	IPv6 Host	Работа в режиме хоста IPv6. Приложения IPv6: ICMPv6, Telnet, RADIUS, MACL, SNTP, Syslog, DNS
	Dual Stack	Реализация двойного стека протоколов IPv4 и IPv6
	ISATAP Tunneling	Туннелирование - инкапсуляция пакета IPv6 в пакет IPv4
IPv4 Routing	Static Routes and ARP Entries	Поддержка до 128 статических IPv4-маршрутов и 1024 записей ARP
	Proxy ARP	Поддержка ответа на ARP-запросы с IP-адреса, не входящего в сеть
	Routing and Bridging modes	Переключение между режимами работы в режиме маршрутизации (L3 forwarding) и коммутации (L2 forwarding)

Раздел	Функция	Описание
	RIP	Поддержка протокола динамической маршрутизации RIPv1, v2
Relay -Server	UDP Relay	Перенаправление широковещательного UDP-трафика на указанный IP-адрес, поддерживается до 128 записей переадресации
	IP Helper	Перенаправление широковещательного UDP-трафика на все IP-интерфейсы
	DHCP Relay	Работа в режиме DHCP-ретранслятора между клиентами и DHCP-сервером (с поддержкой опции 82)
	DHCP Server	Работа в режиме DHCP-сервера, поддерживается до 512 клиентов
Функции обеспечения безопасности	MAC-BASEd Port Security (Locked Port)	Предоставление доступа к порту коммутатора только для устройств, MAC-адреса которых закреплены за этим портом, до 256 адресов
	802.1x Port-BASEd Authentication	Контроль доступа на основе проверки подлинности по стандарту IEEE 802.1x. До 512 одновременных проверенных пользователей
	Time BASEd 802.1x	Настройка времени действия проверки подлинности по стандарту IEEE 802.1x. До 20 временных диапазонов
	Guest VLAN	Предоставление пользователю, не прошедшему проверку подлинности, доступа к ограниченной гостевой сети VLAN
	Unauthenticated VLANs	Предоставление доступа к назначенным сетям VLAN, не требующим проверки подлинности портов (например, в IP-телефонии)
	802.1x - MAC Authentication	Проверка подлинности на основе MAC-адреса для устройств, не поддерживающих 802.1x
	Action-on-Violation	Настройка действий порта при попытке доступа к нему устройства с неразрешенным MAC-адресом
	Dynamic VLAN Assignment	Динамическое присоединение прошедшего проверку клиента к сети VLAN на основе данных RADIUS о нем
	L2–L3–L4 ACL (Access Control List)	Контроль доступа на основе правил фильтрации трафика. Поддержка до 2048 списков ACL на основе заголовков пакетов уровней 2, 3 и 4
	IPv6 ACL	Поддержка правил фильтрации для пакетов IPv6
	Time-BASEd ACL	Настройка времени действия правил фильтрации. Поддержка до 10 временных

Раздел	Функция	Описание
		диапазонов и до 10 периодических правил
	Dynamic ACL (DACL)	Динамическое внесение записи с прошедшим проверку MAC-адресом в ACL-список порта
	Flow Monitoring (sFlow)	Мониторинг трафика через выбранные интерфейсы со сбором статистики и анализом
	RADIUS Remote Authorization and Authentication	Клиент RADIUS. Поддержка протокола удаленной авторизации, аутентификации и учета. Поддерживается до 8 RADIUS-серверов
	RADIUS Accounting	Регистрация сессий по управлению/настройке коммутатора, до 128 сессий на отдельный коммутатор и до 1024 сессий на стэк
	TACACS+	Поддержка протокола проверки подлинности TACACS+. Поддерживается до 8 TACACS-серверов
	DHCP Snooping	Фильтрация DHCP сообщений, поступивших с ненадежных портов
	IP Source Address Guard	Защита от подмены IP-адресов, записанных в таблице на основе DHCP Snooping
	ARP Inspection	Защита от атак с использованием протокола ARP на основе проверки IP-адреса
	DoS Attack Prevention	Защита от DoS-атак (защита от полной загрузки процессора и переполнения буфера)
	SSL	Шифрование удаленного доступа к Web-интерфейсу по HTTPS. Поддержка SSL v2, v3
	SSH	Сервер SSH для удаленного доступа к консоли управления, до 4 одновременных сессий. Поддержка SSH v1, v2
Функции управления	Web Server	Встроенный Web-сервер для доступа к настройкам через Web-интерфейс. Поддерживается до 5 одновременных сессий
	Multi-Session Telnet	Поддержка до 5 одновременных Telnet-сессий, включая доступ через консоль
	CLI, RS-232	Полнофункциональный интерфейс командной строки. Доступ к управлению через консольный порт RS-232
	Switch Users	Поддержка до 15 уровней привилегий для доступа к коммутатору
	Management ACL	Поддержка до 128 специализированных ACL для настройки правил доступа к управлению

Раздел	Функция	Описание
	TFTP	Запись и чтение файлов настройки и образа программного обеспечения по протоколу TFTP
	LLDP	Поддержка протокола LLDP для построения топологии сети. Поддержка 802.1ab – LLDP-MED
	Auto Configuration backup	Автоматическое периодическое сохранение конфигурации
	SNMP	Мониторинг и управление коммутатором по протоколу SNMP (v1, v2, v3). Поддерживается до 8 сообществ
	Syslog	Регистрация событий и ошибок на внешних серверах. Поддерживается до 8 Syslog-серверов
	SNTP	Синхронизация системного времени по протоколу SNTP. Поддерживается до 4 SNTP-серверов
	ICMP	Передачи ICMP-сообщений об ошибках и других исключительных ситуациях
	Traceroute	Определение маршрутов передачи данных в IP-сетях
	Monitoring	Сбор статистики по: интерфейсам, типам пакетов
	RMON	Поддержка удаленного мониторинга на основе RMON
	CPU utilization mechanism	Контроль загрузки центрального процессора
	Power Supply Status	Мониторинг состояния блока питания коммутатора
	Fan Status	Мониторинг состояния вентиляторов
	Temperature	Мониторинг температуры
Стекирование	Stacking Topology	Стекирование до 8 коммутаторов. Топология: кольцо, линейная.

21. Поиск неисправностей Troubleshooting

Неисправность	Возможная причина	Решение
Сбой во время загрузки приводящий к fatal error	Некорректное определение типа пакетного процессора	В логе загрузки должна присутствовать строка dev type=dd7411ab [BobCat] если она отличается от приведенной выше - это скорее всего проблемы с аппаратурой. Необходимо обратиться в сервисный центр.
	Некорректная стартовая конфигурация	Подключить к устройству флешь-накопитель, перезагрузить устройство, сделать резервную копию cdb-файла из загрузочной консоли (при необходимости) . Изъять флешь-накопитель, удалить cdb-файл перезагрузить устройство. Во время загрузки будет создан новый пустой cdb-файл. Таким образом можно подтвердить/опровергнуть корректность конфигурации в устройстве.
	Попытка загрузки некорректного образа	Подключить к устройству флешь-накопитель, перезагрузить устройство, сделать резервную копию прошивки командой update с ssd на флешь-накопитель (при необходимости). Используя флешь-накопитель, с заведомо рабочим ПО, обновить ПО на устройстве и перезагрузить устройство. Таким образом можно подтвердить/опровергнуть корректность прошивки в

		устройстве.
	Проблемы с аппаратурой	Если сообщения об ошибках явно говорят о неисправности оборудования, и/или предыдущие варианты уже исключены следует обратиться в сервисный центр. При обращении желательно сообщить о условия эксплуатации устройства в момент сбоя (сведения об электропитании, температуре помещения, количестве задействованных портов и т.д.) и предоставить лог загрузки.
Отсутствие/некорректный вывод в консоль при подаче питания	Неправильно настроена консоль	Удостовериться что ПО для работы с консолью на ПК настроены согласно настройкам в устройстве (стандартные настройки 115200, 8n1, аппаратное управление потоком отключено). Подробнее см. руководство администратора. **Примечание:** настройка параметров консоли в загрузчике и основном образе могут отличаться **Примечание:** для связи с устройством следует использовать нуль-модемный кабель Для проверки целостности кабеля его нужно отключить от устройства и закоротить между собой линии RX и TX в кабеле (контакты 2 и 3). В консоли должно отображаться эхо вводимых команд.
	Отсутствует загрузчик	Попробовать загрузить устройство с флешь-накопителя с заведомо рабочим ПО. В случае успеха обновить ПО на ssd.
Не поднимается линк на свитче даже на заведомо	Устройство, подключаемое к свитчу не	**Примечание:** свитч работает только на скоростях

рабочей линии связи	поддерживает нужную скорость	1G/10G (за исключением oob-порта). **Примечание:** При необходимости 10G порты должны быть соотв. командой переведены в 1G режим. Если необходимо подключить устройство, которое поддерживает только 10M/100M скорости рекомендуется использовать промежуточные неуправляемые свитчи.
Устройство недоступно через oob-порт, несмотря на то что линк поднимается	oob-порт настроен на работу с другой физической средой	**Примечание:** настройка физической среды не влияет на способность поднимать линк Поменять режим работы oob-порта можно из загрузочной консоли.

Спасибо, что используете оборудование Симанитрон!