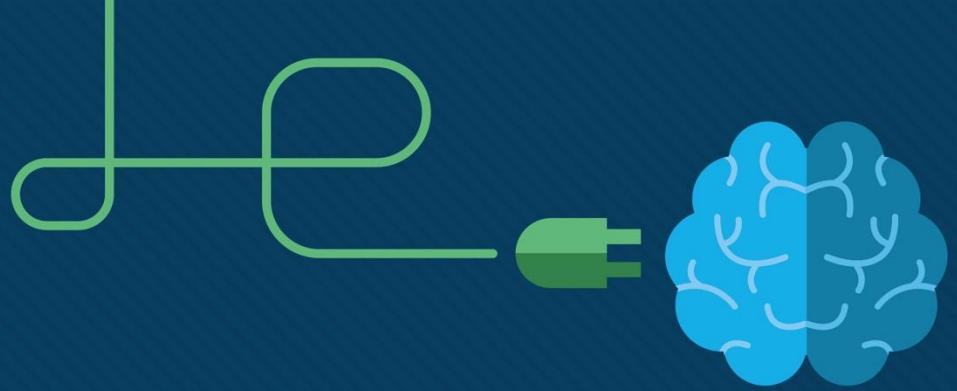


Модуль 1. Базовая настройка устройств

Задачи модуля

Заголовок модуля: Базовая настройка устройств
Цели модуля: Выполнять настройку устройств с учетом практических рекомендаций по обеспечению безопасности.

Заголовок темы	Цель темы
Первоначальная настройка коммутатора	Выполнить первоначальную настройку коммутатора Cisco.
Настройка портов коммутатора	Настройка портов коммутатора в соответствии с требованиями сети.
Удаленный защищенный доступ	Выполнить на коммутаторе настройку защищенного доступа для управления.
Базовая конфигурация маршрутизатора	С помощью интерфейса командной строки настроить на маршрутизаторе основные параметры для маршрутизации трафика между двумя сетями, подключенными напрямую.
Проверка связи между подключенными напрямую сетями	Выполнить проверку связи между двумя сетями, которые подключены к маршрутизатору напрямую.

1.1. Первоначальная настройка коммутатора

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Последовательность загрузки коммутатора

После включения коммутатор Cisco проходит следующие стадии загрузки:

Шаг 1. Во-первых, коммутатор загружает программу самотестирования питания (POST), хранящуюся в ПЗУ. POST проверяет подсистему CPU. Он проверяет процессор, DRAM и часть флэш-устройства, которая составляет файловую систему флэш-памяти.

Шаг 2: После этого на коммутаторе запускается программное обеспечение начального загрузчика. Начальный загрузчик — это небольшая программа, которая хранится в ПЗУ и запускается сразу после успешного завершения проверки POST.

Шаг 3: Начальный загрузчик выполняет низкоуровневую инициализацию центрального процессора. Он инициализирует регистры ЦП, которые контролируют место отображения физической памяти, количество памяти и ее скорость.

Шаг 4:Затем программа запускает файловую систему флеш-памяти на материнской плате.

Шаг 5: Наконец, начальный загрузчик находит и загружает образ операционной системы IOS по умолчанию и передает ей управление коммутатором.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Команда загрузочной системы - boot system

Он пытается выполнить автоматическую загрузку, используя информацию из переменной для среды BOOT. Если эта переменная не установлена, коммутатор пытается загрузить и выполнить первый исполняемый файл, который он может найти.

Затем операционная система IOS инициализирует интерфейсы, используя команды Cisco IOS из файла загрузочной конфигурации, который хранится в энергонезависимом ОЗУ (NVRAM). Файл startup-config называется **config.text** и находится во флэш-памяти.

В примере переменная среды BOOT задается с помощью команды режима глобальной конфигурации **boot system** . Обратите внимание, что IOS находится в отдельной папке и указан путь к папке. Используйте команду **show boot**, чтобы узнать, как настроен файл текущей загрузки IOS.

```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

Команда	Определение
boot system	Основная команда
flash:	Устройство хранения
c2960-lanbasek9-mz.150-2.SE/	Путь к файловой системе
c2960-lanbasek9-mz.150-2.SE.bin	Имя файла IOS

ры, 2016 г. Все права защищены.
Информация Cisco

Начальная настройка параметров коммутатора
Светодиодные индикаторы коммутатора

Системный индикатор показывает, есть ли питание системы и функционирует ли она должным образом.
Индикатор RPS. Индикатор резервного источника питания (RPS), который указывает состояние этой источника.
Индикатор состояния порта (STAT): зеленый цвет указывает, что выбран режим состояния порта, который является значением по умолчанию. Статус порта может быть понятен светом, связанным с каждым портом.
Светодиодный индикатор дуплекса порта (DUPLX):зеленый цвет указывает, что выбран режим дуплекса порта. Дуплекс порта может быть понятен светом, связанным с каждым портом.
Индикатор скорости порта (SPEED):зеленый цвет указывает, что выбран режим скорости порта. Скорость порта может быть понята светом, связанным с каждым портом.
Power over Ethernet LED (PoE):Присутствует, если коммутатор поддерживает PoE. Указывает состояние PoE портов коммутатора.
Кнопка Mode используется для перемещения между различными режимами — STAT, DUPLX, SPEED и PoE

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Светодиодные индикаторы коммутатора (продолжение)

	Выкл.	Зеленый	Часто мигающий зеленый	Желтый	Часто мигающий оранжевый	Мигающий зеленый и оранжевый
RPS	Выкл/Нет RPS	RPS готов	RPS включен, но недоступен	Резервный или неисправный RPS	Внутренняя PS не удалось, RPS обеспечивает питание	Нет
PoE	Не выбрано, проблем нет	Выбранный	—	—	Не выбран, проблемы с портом присутствуют	Нет
При выборе именованного режима свет, связанный с каждым физическим портом, указывает:						
STAT	Нет связи или выключения	Соединение установлено	Действие	Порт блокирует петлю	Порт блокирует петлю	Ошибка соединения.
Дуплексный режим	Полудуплекс	Полный дуплекс	—	—	—	—
SPEED	10 Мбит/с	100 Мбит/с	1000 Мбит/с	—	—	—
PoE	PoE выключен	PoE включен	Нет	PoE отключен	Питание PoE отключено из-за ошибки.	PoE отклонено (сверх бюджета)

© Cisco и/или партнеры, 2014. Все права защищены.
Конфиденциальная информация Cisco

Восстановление после сбоя системы

Загрузчик предоставляет доступ к коммутатору, если операционная система не может быть использована из-за отсутствия или повреждения системных файлов. Загрузчик имеет командную строку, которая обеспечивает доступ к файлам, хранящимся во флэш-памяти. Доступ в начальный загрузчик можно получить через консольное подключение, выполнив следующие действия:

Шаг 1. Подключите ПК через консольный кабель к консольному порту коммутатора. Настройка программы эмуляции терминала и подключение ПК к консольному порту

Шаг 2. Отсоедините кабель питания коммутатора.

Step 3. Повторно подключите шнур питания к коммутатору и в течение 15 секунд нажмите и удерживайте кнопку Mode, пока индикатор системы все еще мигает зеленым цветом.

Step 4. Продолжайте нажимать кнопку « Режим», пока системный светодиод не станет желтым, а затем сплошным зеленым; затем отпустите кнопку «Режим».

Step 5. В эмуляторе терминала на ПК появится запрос switch: начального загрузчика.

Командная строка начального загрузчика поддерживает команды для форматирования файловой флеш-системы, переустановки операционной системы и восстановления утерянного или забытого пароля. Например, команду **dir** можно использовать для просмотра списка файлов в указанном каталоге, как показано на рисунке.

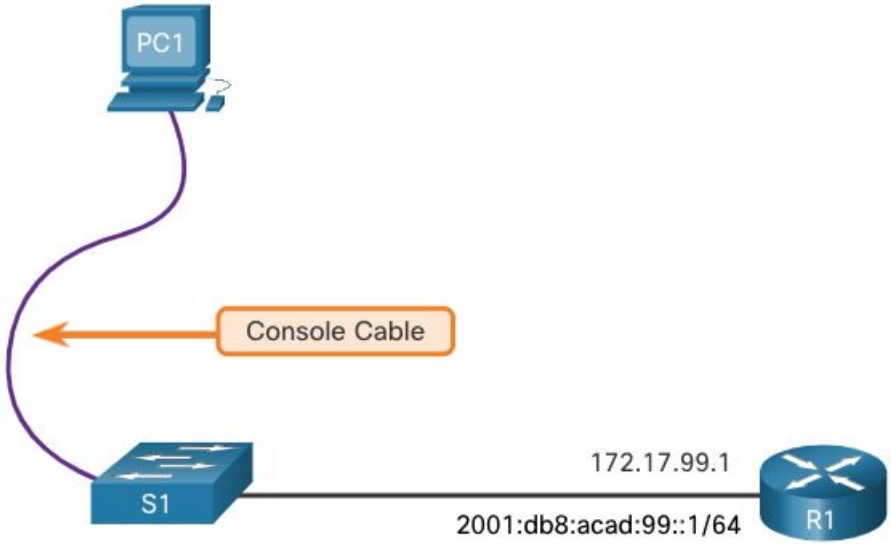
© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Настройка доступа для управления коммутатором

Чтобы подготовить коммутатор для доступа к удаленному управлению, он должен быть настроен с IP-адресом и маской подсети.

Имейте в виду, что для управления коммутатором из удаленной сети на коммутаторе должен быть настроен на шлюз по умолчанию. Это очень похоже на настройку информации об IP-адресах на хост-устройствах.

На рисунке виртуальный интерфейс коммутатора (SVI) на S1 должен быть назначен IP-адрес. SVI — это виртуальный интерфейс, а не физический порт коммутатора. Кабель консоли используется для подключения к ПК, так что коммутатор может быть изначально настроен.



© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Базовая настройка коммутатора

По умолчанию управляющий виртуальный интерфейс коммутатора управляется и настраивается через VLAN 1. По умолчанию все порты назначены во VLAN 1. В целях безопасности рекомендуется использовать VLAN, отличную от VLAN 1, для управляющей VLAN, например, в данном примере VLAN 99.

Шаг 1. Настройте интерфейс управления. В режиме конфигурации интерфейса VLAN IPv4-адрес и маска подсети применяются к SVI управления коммутатора.

Примечание. SVI для VLAN 99 не будет отображаться как «up/up», пока не будет создана VLAN 99 и не будет подключено устройство к порту коммутатора, связанному с VLAN 99.

Примечание. Возможно, коммутатор необходимо настроить для IPv6. Например, перед настройкой адресации IPv6 на Cisco Catalyst 2960 под управлением IOS версии 15.0 необходимо ввести команду глобальной конфигурации sdm prefer dual ipv4-and-ipv6 по умолчанию, а затем **перезагрузить** коммутатор.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Базовая настройка коммутатора

Задача	Команды IOS
Войдите в режим глобальной настройки.	S1# **configure terminal**
Войдите в режим конфигурации интерфейса для SVI.	S1(config)# **interface vlan 99**
Настройте IPv4-адрес интерфейса управления.	S1(config-if)# **ip address 172.17.99.11 255.255.255.0**
Настройте IPv6-адрес интерфейса управления.	S1(config-if)# **ipv6 address 2001:db8:acad:99::1/64**
Включите интерфейс управления.	S1(config-if)# **no shutdown**
Вернитесь в привилегированный режим.	S1(config-if)# **end**
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# **copy running-config startup-config**

Базовая настройка коммутатора

Шаг 2: Настройте шлюз по умолчанию для коммутатора

Если требуется удаленное управление коммутатором из сетей без прямого подключения, на коммутаторе следует настроить шлюз по умолчанию.

- Примечание. Поскольку коммутатор получит информацию о шлюзе по умолчанию из сообщения объявления маршрутизатора (RA), коммутатору не требуется шлюз по умолчанию IPv6.

Задача	Команды IOS
Войдите в режим глобальной настройки.	S1# **configure terminal**
Настройте шлюз по умолчанию для коммутатора.	S1(config)# **ip default-gateway 172.17.99.1**
Вернитесь в привилегированный режим.	S1(config-if)# **end**
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# **copy running-config startup-config**

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Базовая настройка коммутатора

Шаг 3. Проверка конфигурации.

Команды **show ip interface brief** и **show ipv6 interface brief** полезны для определения состояния физических и виртуальных интерфейсов. Приведенные выходные данные подтверждают, что интерфейс VLAN 99 настроен с IPv4-адресом и маской подсети.

Примечание. IP-адрес, применяемый к SVI, предназначен только для удаленного управления доступом к коммутатору; это не позволяет коммутатору маршрутизировать пакеты уровня 3.

```
S1# show ip interface brief
Interface      IP-Address      OK? Method   Status     Protocol
Vlan99         172.17.99.11    YES manual   down       down
(output omitted)
S1# show ipv6 interface brief
Vlan99                  [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::1
(output omitted)
```

и Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Лабораторная работа - Базовая настройка коммутатора

В этой лабораторной работе вы выполните следующие задачи:

- Часть 1. Проверка конфигурации коммутатора по умолчанию
- Часть 2. Создание сети и настройка основных параметров устройства
- Часть 3. Проверка сетевых подключений
- Часть 4. Управление таблицей MAC-адресов

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

1.2. Настройка портов коммутатора

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Связь в дуплексном режиме

Полнодуплексная связь повышает эффективность использования полосы пропускания, позволяя обоим сторонам канала одновременно передавать и принимать данные. Данный вид связи также называют двунаправленной связью и это требуется для микросегментации.

Микросегментированная локальная сеть создается, когда к коммутационному порту подключено только одно устройство, а порт работает в полнодуплексном режиме. Когда коммутационный порт работает в полнодуплексном режиме, то коллизионные домены, связанные с портом, отсутствуют.

В отличие от полнодуплексной связи, полудуплексная связь является однонаправленной. Полудуплексная связь создает проблемы с производительностью, поскольку данные могут поступать только в одном направлении одновременно, что часто приводит к столкновениям.

Для работы полнодуплексных соединений требуются сетевые интерфейсные платы, поддерживающие Gigabit Ethernet и 10Gb Ethernet. В полнодуплексном режиме схема обнаружения столкновений на сетевой плате отключена. Полнодуплексный режим Fast Ethernet обеспечивает эффективность 100% в обоих направлениях. Это приводит к удвоению потенциального использования указанной полосы пропускания.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Настройка портов коммутатора на физическом уровне

Порты коммутатора можно настроить вручную с помощью определенных параметров дуплекса и скорости. Соответствующие команды конфигурации интерфейса — **duplex** и **speed** .

По умолчанию для дуплексного режима и скорости портов коммутаторов на коммутаторах Cisco Catalyst 2960 и 3560 используется автоматически. Порты 10/100/1000 работают в полудуплексном или полнодуплексном режиме, если они установлены на 10 или 100 Мбит/с, и работают только в полнодуплексном режиме, если установлено значение 1000 Мбит/с (1 Гбит/с).

Автосогласование полезно, если параметры скорости и дуплексного режима устройства, подключенного к порту, неизвестны или могут измениться. При подключении к известным устройствам, таким как серверы, выделенные рабочие станции или сетевые устройства, рекомендуется вручную задать параметры скорости и дуплекса.

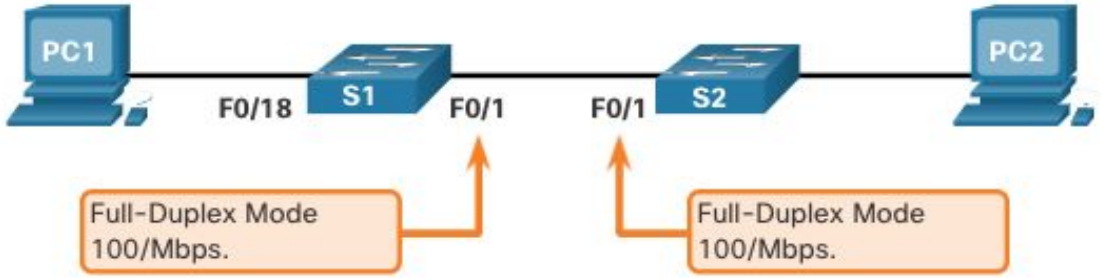
При устранении проблем с портами коммутатора важно проверить параметры дуплекса и скорости.

Примечание Несоответствие настроек дуплексного режима или скорости может привести к проблемам с подключением. Ошибка автосогласования создает несовпадающие параметры.

Все порты оптоволоконных кабелей, например порты 1000BASE-SX, работают только на предустановленной скорости и всегда в полнодуплексном режиме.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Настройка портов коммутатора на физическом уровне



Задача	Команды IOS
Войдите в режим глобальной настройки.	S1# **configure terminal**
Войдите в режим конфигурации интерфейса.	S1(config)# **interface FastEthernet 0/1**
Настройте дуплексный режим интерфейса.	S1(config-if)# **duplex full**
Настройте скорость интерфейса.	S1(config-if)# **speed 100**
Вернитесь в привилегированный режим.	S1(config-if)# **end**
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# **copy running-config startup-config**

Функция Auto-MDIX

Когда включено автоматическое пересечение интерфейса, зависящее от среды (auto-MDIX), интерфейс коммутатора автоматически определяет требуемый тип кабельного соединения (прямой или перекрестный) и соответствующим образом конфигурирует соединение.

При подключении к коммутаторам без функции auto-MDIX необходимо использовать прямые кабели для соединения с устройствами, такими как серверы, рабочие станции или маршрутизаторы. Перекрестные кабели должны использоваться для подключения к другим коммутаторам или ретрансляторам.

Включенная функция auto-MDIX позволяет использовать любой тип кабеля для подключения к другим устройствам, а интерфейс автоматически настраивается для успешного взаимодействия.

На новых коммутаторах Cisco эту функцию включает команда режима интерфейсной настройки **mdix auto**. При использовании функции auto-MDIX на интерфейсе необходимо задать для его скорости и режима дуплекса значение **auto** (Автоопределение).

Примечание. Функция auto-MDIX включена по умолчанию на коммутаторах Catalyst 2960 и Catalyst 3560, но недоступна на старых коммутаторах Catalyst 2950 и Catalyst 3550.

Чтобы проверить настройку auto-MDIX для конкретного интерфейса, используйте команду **show controllers ethernet-controller** с ключевым словом **phy** . Чтобы ограничить выходные данные строками, ссылающихся на автоматическое MDIX, используйте фильтр **include Auto-MDIX** .

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Команды проверки коммутатора

Задача	Команды IOS
Отобразите состояние и конфигурацию интерфейса.	S1# **show interfaces** [*interface-id*]
Отобразите текущую загрузочную конфигурацию.	S1# **show startup-config**
Отобразите текущую конфигурацию.	S1# **show running-config**
Отобразите данные о файловой системе флеш-памяти.	S1# **show flash**
Отобразите состояние системного оборудования и программного обеспечения.	S1# **show version**
Отобразите историю введенных команд.	S1# **show history**
Отобразите данные IP для интерфейса.	S1# **show ip interface** [*interface-id*] ИЛИ S1# **show ipv6 interface** [*interface-id*]
Отобразите таблицу MAC-адресов.	S1# **show mac-address-table** ИЛИ S1# **show mac address-table**

Проверка конфигурации портов коммутатора

Для проверки правильности настройки коммутатора можно использовать команду **show running-config**. Из выборки сокращенного вывода по S1 на рисунке показана некоторая важная информация:

- Интерфейс Fast Ethernet 0/18 настроен с сетью управления VLAN 99.
- VLAN 99 назначен IPv4-адрес 172.17.99.11 с маской подсети 255.255.255.0.
- Задайте шлюз по умолчанию 172.17.99.1

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
(output omitted)
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка конфигурации портов коммутатора (продолжение)

Команда **show interfaces** — это еще одна часто используемая команда, которая отображает сведения о состоянии и статистике сетевых интерфейсов коммутатора. Команда **show interfaces** часто используется при настройке и мониторинге сетевых устройств.

Первая строка выходных данных для команды **show interfaces fastEthernet 0/18** указывает на то, что интерфейс FastEthernet 0/18 работает. Следующие данные вывода показывают, что включен полнодуплексный режим и установлена скорость 100 Мбит/с.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

Проблемы на уровне сетевого доступа

Выходные данные команды **show interfaces** полезны для обнаружения распространенных проблем с носителями. Одной из наиболее важных частей этого вывода является отображение состояния протокола линии и канала передачи данных, как показано в примере.

Первый параметр (FastEthernet0/18 is up) относится к аппаратному уровню. Он указывает, получает ли интерфейс сигнал обнаружения несущей. Второй параметр (line protocol is up) относится к уровню линии. Он указывает, принимаются ли сообщения keepalive протокола уровня линии. На основе выходных данных команды **show interfaces** возможные проблемы могут быть устранены следующим образом:

- Если интерфейс включен, а протокол линии не функционирует, возникает проблема. Может быть несоответствие типа инкапсуляции, интерфейс на другом конце может быть отключен, или может быть аппаратная проблема.
- Если протокол линии и интерфейс отключены, кабель не подключается или возникает другая проблема с интерфейсом. Например, во встречно-параллельном включении мог быть административно отключен другой конец подключения.
- Если интерфейс отключен административно, он был отключен вручную (была выдана команда **shutdown**) в активной конфигурации.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW
100000 Kbit/sec, DLY 100 usec,
```

Проблемы на уровне сетевого доступа (продолжение)

Выходные данные команды **show interfaces** отображают счетчики и статистику для интерфейса FastEthernet0/18, как показано ниже:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2295197 packets input, 305539992 bytes, 0 no buffer
     Received 1925500 broadcasts (74 multicasts)
     0 runts, 0 giants, 0 throttles
     3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 74 multicast, 0 pause input
     0 input packets with dribble condition detected
     3594664 packets output, 436549843 bytes, 0 underruns
     8 output errors, 1790 collisions, 10 interface resets
     0 unknown protocol drops
     0 babbles, 235 late collision, 0 deferred
```

Проблемы на уровне сетевого доступа (продолжение)

Некоторые ошибки носителя недостаточно серьезны, чтобы привести к сбою цепи, но вызывают проблемы с производительностью сети. В таблице объясняются некоторые из этих распространенных ошибок, которые можно обнаружить с помощью команды **show interface**.

Тип ошибки	Описание
Ошибки ввода	Общее количество ошибок. Включает «карликовые» и «гигантские» кадры, отсутствие буфера, CRC, ошибки в кадрах, переполнение и проигнорированные пакеты.
Runts (ошибки типа «карликовый кадр»)	Пакеты, отброшенные из-за того, что они меньше минимального размера пакета для среды. Например, любой кадр Ethernet размером менее 64 байтов считается карликовым (runt).
Гигантские кадры (giant)	Пакеты, которые отброшены из-за превышения максимального размера пакета для среды. Например, любой кадр Ethernet размером более 1 518 байтов считается слишком большим (giant).
CRC	Ошибки CRC создаются, когда рассчитанная контрольная сумма не соответствует полученной контрольной сумме.
Ошибки вывода	Сумма всех ошибок, которые мешали окончательной передаче дейтаграмм из анализируемого интерфейса.
Коллизии	Количество сообщений, повторно переданных из-за коллизий Ethernet.
Поздние коллизии	Коллизия, которая случается после передачи 512 бит кадра.

Ошибки ввода вывода

«Входные ошибки» — это сумма всех ошибок в датаграммах, полученных на исследуемом интерфейсе. Включает «карликовые» и «гигантские» кадры, отсутствие буфера, CRC, ошибки в кадрах, переполнение и проигнорированные пакеты. К ошибкам вывода, которые можно обнаружить с помощью команды **show interfaces**, относятся следующие.

- **Runt Frames** - фреймы Ethernet, которые короче, чем 64-байтовая минимально допустимая длина, называются runts. Обычно причиной большого числа карликовых кадров являются неисправные сетевые интерфейсные платы, но они также могут быть вызваны коллизиями.
- Гигантские кадры (giants) **— кадры Ethernet, размер которых превышает максимально допустимый.**
- Ошибки CRC — в Ethernet и последовательных интерфейсах ошибки CRC обычно свидетельствуют о неполадках в среде передачи или кабеле. Частыми причинами ошибок являются электрические помехи, плохо закрепленные или поврежденные разъемы, а также неверно выбранный тип кабеля. Большое количество ошибок CRC приводит к шуму на канале, поэтому следует проверить кабель. Также следует найти и устранить источники электромагнитного шума.

© Cisco и/или партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Настройкаошибок ввода и выводаинтерфейса портов коммутатора (продолжение)

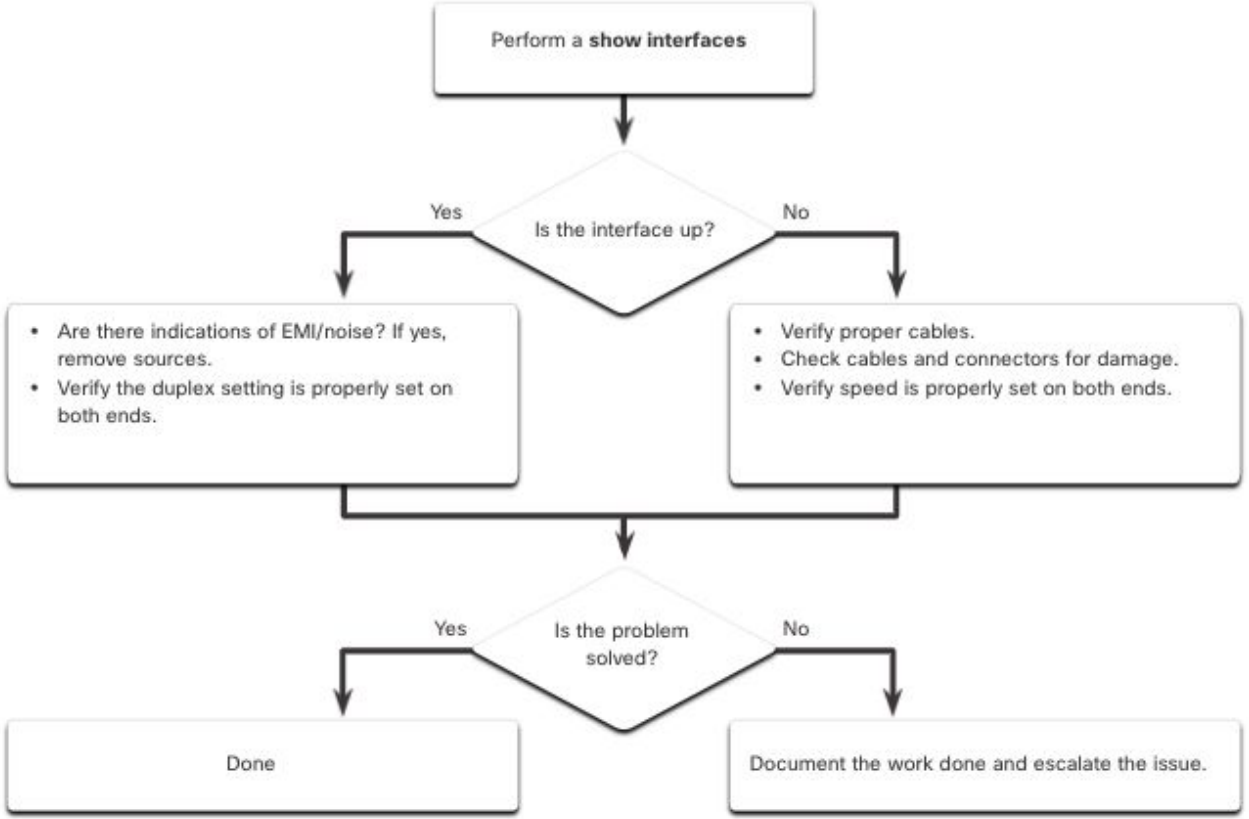
«Ошибки вывода» — это сумма всех ошибок, которые препятствовали окончательной передаче датаграмм из проверяемого интерфейса. К ошибкам вывода, которые можно обнаружить с помощью команды **show interfaces**, относятся следующие.

- Коллизии являются обычным явлением при работе в полудуплексном режиме. Однако они никогда не должны возникать на интерфейсе, настроенном для полнодуплексного режима связи.
- Поздние коллизии — это коллизии, которые происходят после передачи 512 бит кадра. Чрезмерная длина кабеля является наиболее распространенной причиной последних столкновений. Другой распространенной причиной является неправильная конфигурация дуплекса.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Поиск и устранение неполадок на уровне сетевого доступа

Для поиска и устранения неполадок при отсутствии или плохом качестве соединения коммутатора с другим устройством следуйте данному алгоритму действий:



© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

1.3. Удаленный защищенный доступ

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Принцип работы протокола Telnet

Telnet использует TCP-порт 23. Telnet является более ранним протоколом, использующим небезопасную незашифрованную передачу как данных, так и идентификационной информации (имя пользователя и пароль) между взаимодействующими устройствами.

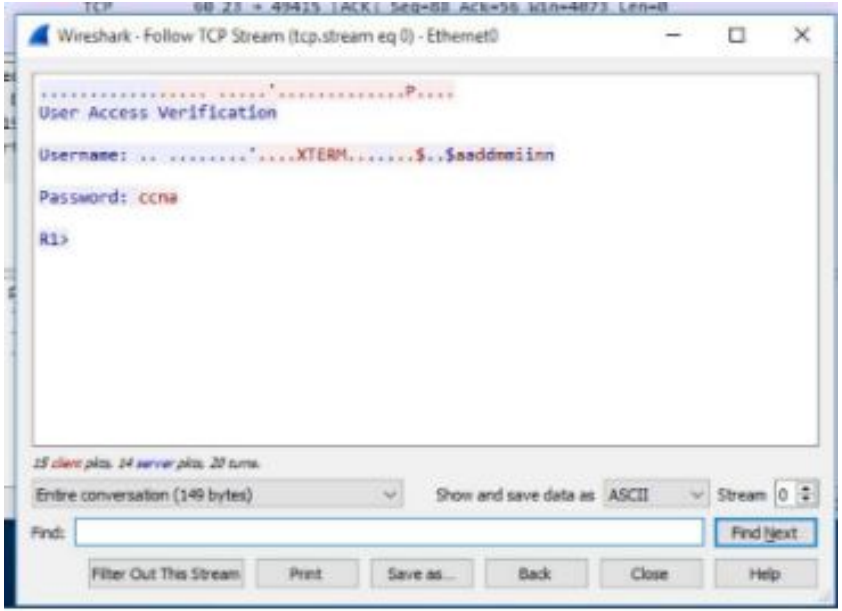
Злоумышленник может отслеживать пакеты с помощью Wireshark. Например, на рисунке актер угрозы захватил имя пользователя **admin** и пароль **ccna** из сеанса Telnet.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Принцип работы протокола SSH

Secure Shell (SSH) — это безопасный протокол, который использует TCP-порт 22. Протокол Secure shell (SSH) — это протокол, который обеспечивает безопасное (зашифрованное) подключение для управления удаленным устройством. Для безопасного управления удаленными подключениями Cisco рекомендует заменить протокол Telnet протоколом SSH. SSH обеспечивает защиту удаленных подключений, предоставляя надежное шифрование данных аутентификации устройства (имя пользователя и пароль), а также данных, передаваемых между устройствами.

Например, на рисунке показан захват с помощью Wireshark сеанса SSH. Актер угрозы может отслеживать сеанс, используя IP-адрес устройства администратора. Однако, в отличие от Telnet, с SSH имя пользователя и пароль шифруются.



© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверьте, что коммутатор поддерживает SSH

Для использования протокола SSH на коммутаторах Catalyst 2960 требуется версия операционной системы Cisco IOS с функциями и возможностями криптографии (шифрования). Используйте команду **show version** на коммутаторе, чтобы увидеть, какое IOS работает коммутатор в данный момент. Имя файла IOS, которое включает комбинацию «k9» поддерживает криптографические (зашифрованные) функции и возможности.

В примере показаны выходные данные команды **show version** .

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE
(fc1)
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Удаленный защищенный доступ Настройка протокола SSH

Перед настройкой протокола SSH на коммутаторе нужно настроить уникальное имя хоста и соответствующие параметры сетевого подключения.

Шаг 1. Проверка поддержки SSH. Используйте команду show ip ssh, чтобы убедиться, что коммутатор поддерживает SSH. Если на коммутаторе не работает IOS, поддерживающая криптографические функции, эта команда не распознается.

Шаг 2. Настройка IP-домена — настройка IP-имени домена сети с помощью команды ip domain-name domain-name domain-name global configuration mode.

Шаг 3: Создание пар ключей RSA - Создание пары ключей RSA автоматически включает SSH. Используйте команду crypto key generate rsa global configuration mode, чтобы включить сервер SSH на коммутаторе и создать пару ключей RSA.

Примечание. Чтобы удалить пару ключей RSA, используйте команду crypto key zeroize rsa global configuration mode. После удаления пары ключей RSA сервер SSH автоматически отключается.

Шаг 4: Настройка аутентификации пользователя - SSH сервер может аутентифицировать пользователей локально или с помощью сервера аутентификации. Для использования метода локальной аутентификации создайте имя пользователя и пароль с помощью команды режима глобальной настройки _username_ _password_.

Шаг 5. Настройка строк vty — включите протокол SSH на линиях vty с помощью команды transport input ssh line configuration mode. Используйте команду line vty global configuration mode, а затем команду login local line configuration mode, чтобы требовать локальную аутентификацию для SSH-соединений из локальной базы данных имени пользователя.

Шаг 6: Включить SSH версии 2 - По умолчанию SSH поддерживает обе версии 1 и 2. При поддержке обеих версий это отображается в выходных данных show ip ssh как поддерживающая версия 2. Включите SSH версию с помощью глобальной команды конфигурации ip ssh версии 2.

© Cisco и/или партнеры, 2020 г. Все права защищены.

Принцип работы протокола SSH

Для подключения к серверу SSH на ПК используется SSH-клиент, например PuTTY. Например, предположим следующее:

- SSH включен на коммутаторе S1
- на коммутаторе S1 интерфейсу VLAN 99 (SVI) присвоен IPv4-адрес 172.17.99.11;
- компьютеру PC1 присвоен IPv4-адрес 172.17.99.21.

С помощью эмулятора терминала инициируйте SSH-соединение с IPv4-адресом SVI VLAN S1 от PC1.

При подключении пользователю будет предложено ввести имя пользователя и пароль, как показано в примере. Используя конфигурацию из предыдущего примера, вводятся имя пользователя **admin** и пароль **ccna** . После ввода правильной комбинации пользователь подключается через SSH к интерфейсу командной строки (CLI) коммутатора Catalyst 2960.

```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка работы протокола SSH

Для отображения используемой версии и конфигурации для протокола SSH на устройстве, который вы настроили в качестве сервера SSH, используйте команду **show ip ssh**. В примере включена версия SSH 2.

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started       admin
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started       admin
S1#
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Удаленный защищенный доступ Packet Tracer. Настройка протокола SSH

В этом трассировщике пакетов вы будете делать следующее:

- Безопасность всех паролей
- Шифрование передачи данных
- Проверка реализации SSH

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

1.4 – Базовая конфигурация маршрутизатора

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Примеры базовой настройки маршрутизатора

Маршрутизаторы и коммутаторы Cisco во многом похожи. Они поддерживают сходные модальные операционные системы, используют одинаковые структуры команд и команды. Кроме того, для начальной настройки этих устройств требуются схожие действия. Например, следующие параметры должны быть всегда настроены. Назовите устройство, чтобы отличить его от других маршрутизаторов, и настройте пароли, как показано в примере.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

© Cisco и/или Партнеры, 2019 г. Все права защищены.
Конфиденциальная информация Cisco

Настройка основных параметров маршрутизатора (продолжение)

Настройте баннер для предоставления юридического уведомления о несанкционированном доступе, как показано в примере.

```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

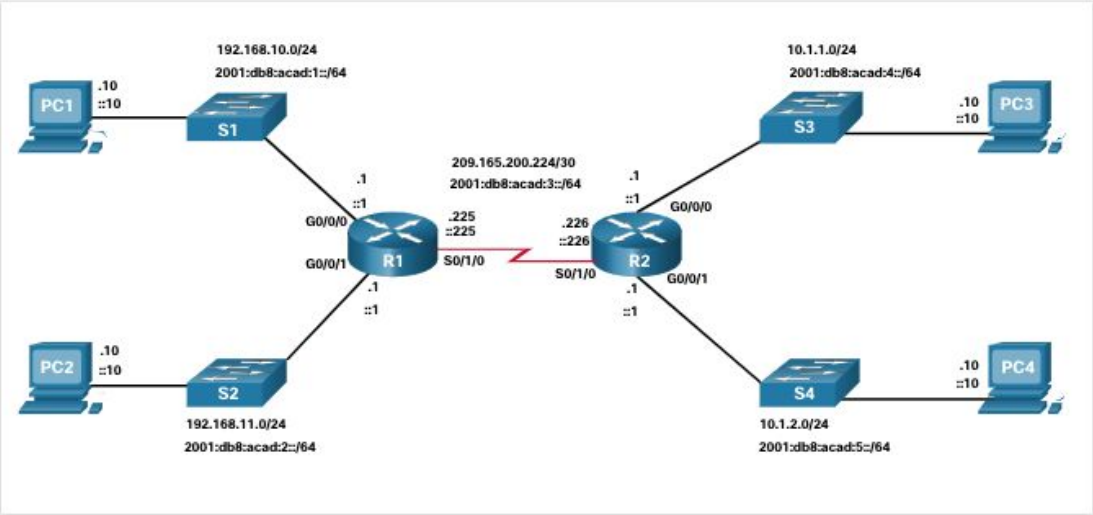
Сохраните изменения на маршрутизаторе, как показано в примере.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Тополога двойного стека

Одним из существенных различий между коммутаторами и маршрутизаторами являются поддерживаемые устройствами типы интерфейсов. Например, коммутаторы 2-го уровня поддерживают локальные сети, в связи с чем они оснащены несколькими портами FastEthernet или Gigabit Ethernet. Топология двойного стека на рисунке используется для демонстрации конфигурации интерфейсов IPv4 и IPv6 маршрутизатора.



© Cisco и/или партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Настройка интерфейсов маршрутизатора

Маршрутизаторы поддерживают локальные и глобальные сети, и могут обеспечивать соединение между разными типами сетей. Таким образом, они поддерживают множество типов интерфейсов. Например, маршрутизаторы семейства Cisco G2 SR используют один или два интегрированных интерфейса Gigabit Ethernet и разъемы для высокоскоростных интерфейсных карт WAN (HWIC) для поддержания разных типов сетевых интерфейсов, включая последовательный, DSL и кабельный интерфейсы.

Чтобы обеспечить доступность интерфейса, его необходимо:

- **Настроено по крайней мере с одним IP-адресом** . Используйте команды конфигурации интерфейса интерфейса *IPv6 ipv6-address/prefixip-address* .
- Активировать**: по умолчанию интерфейсы сетей LAN и WAN не активированы (**shutdown). Для включения интерфейса используйте команду активации **no shutdown** (Это действие аналогично подаче питания на интерфейс.) Для активации физического уровня интерфейс должен быть также подключен к другому устройству (концентратору, коммутатору или другому маршрутизатору).
- При необходимости для интерфейса можно настроить короткое описание длиной до 240 символов. Рекомендуется настраивать описание на каждом интерфейсе. В производственных сетях быстро оценили преимущества описания интерфейсов, поскольку это очень удобно при устранении неполадок, а также для определения стороннего подключения и поиска контактной информации.

© Cisco и/или партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Базовая конфигурацияМаршрутизатораНастройка интерфейсов маршрутизатора (продолжение)

Пример показывает настройку для интерфейсов на R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

ы, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Интерфейсы обратной петли IPv4

Другая распространенная конфигурация маршрутизаторов Cisco IOS — задействование интерфейса loopback.

Интерфейс обратной петли предоставляет собой логический, внутренний по отношению к маршрутизатору интерфейс. Он не назначается физическому порту и не может быть подключен к другому устройству. Он считается программным интерфейсом, который автоматически переводится в состояние up (активен) во время работы маршрутизатора.

Применение интерфейса loopback может быть целесообразным при тестировании и управлении устройством Cisco IOS, поскольку он обеспечивает доступность хотя бы одного интерфейса. Его можно использовать в целях тестирования — например, для тестирования внутренних процессов маршрутизации, путем имитации сетей за пределами маршрутизатора.

Интерфейсы обратной связи также широко используются в лабораторных средах для создания дополнительных интерфейсов. Например, можно создать несколько интерфейсов обратной связи на маршрутизаторе, чтобы имитировать большее количество сетей для практики настройки и тестирования. IPv4-адрес для каждого интерфейса loopback должен быть уникальным и не должен быть задействован другим интерфейсом. В этой учебной программе мы часто используем интерфейс обратной связи для имитации ссылки на Интернет.

Включение интерфейса и назначение loopback-адресов выполняется с помощью простого набора команд:

Packet Tracer— Настройка интерфейсов маршрутизатора

В этом упражнении Packet Tracer вам нужно:

- Настройка адресации IPv4 и проверка подключения
- Настройка адресации IPv6 и проверка подключения

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

1.5 Проверка связи между подключенными напрямую сетями

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Команды проверки

Для проверки работы и настройки интерфейса можно использовать несколько команд **show**.

Для того чтобы быстро определить состояние интерфейса, рекомендуется использовать следующие три команды:

- **Команда show ip interface brief** и **show ipv6 interface brief** отображает краткую информацию обо всех интерфейсах, в том числе IPv4-адрес интерфейса и текущее рабочее состояние.
- **show running-config interface** *идентификатор интерфейса* — отображает команды, настроенные на указанном интерфейсе.
- show ip route — отображает содержимое таблицы маршрутизации IPv4, которая хранится в ОЗУ; В Cisco IOS 15 активные интерфейсы должны быть указаны в таблице маршрутизации с двумя связанными с ними записями, которые определены кодом **«C»** (подключен) или **«L»** (локальный). В предыдущих версиях IOS появляется только запись с кодом **«C».**

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Команды проверки

Выходные данные команд **show ip interface brief** и **show ipv6 interface brief** можно использовать для быстрого отображения состояния всех интерфейсов на маршрутизаторе. Вы можете проверить, что интерфейсы активны и работают, как указано в состоянии «вверх» и протоколе «вверх», как показано в примере. Получение других выходных данных указывает на проблему с конфигурацией или

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::7279:B3FF:FE92:3131
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]     Unassigned
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка локальных и многоадресных адресов связи IPv6

В выходных данных **show ipv6 interface brief** отображаются два настроенных IPv6-адреса на каждый интерфейс. Один из адресов — глобальный индивидуальный адрес IPv6, который был введен вручную. Другой адрес, который начинается с FE80, это локальный индивидуальный адрес канала для интерфейса. Локальный адрес канала автоматически добавляется на интерфейс при назначении глобального индивидуального адреса. Для сетевого интерфейса с IPv6-настройками требуется локальный адрес канала, но необязателен глобальный индивидуальный адрес.

Результат выполнения команды **show ipv6 interface gigabitethernet 0/0**, представленный на рис. 2, отображает состояние интерфейса и все IPv6-адреса, принадлежащие этому интерфейсу. Кроме локального адреса канала и глобального индивидуального адреса, выходные данные содержат групповые адреса, назначенные интерфейсу и начинающиеся с префикса FF02.

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка конфигурации интерфейса

Выходные данные команды **show running-config interface** отображают текущие команды, примененные к указанному интерфейсу, как показано на рисунке.

Для получения дополнительной информации об интерфейсе используются следующие две команды:

- **Команда** show interfaces **отображает информацию об интерфейсе и счетчик потока пакетов для всех интерфейсов на устройстве.**
- show ip interface — отображает информацию, связанную с IPv4, для всех интерфейсов маршрутизатора.

```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка маршрутизации

Выходные данные команд **show ip route** и **show ipv6 route** показывают три непосредственно подключенных сетевых элемента и три записи интерфейса локального узла маршрута, как показано в примере.

Административное расстояние маршрута локального узла равно 0. Его маска для IPv4 равна /32, а для IPv6 — /128. Маршрут локального узла относится к маршрутам на маршрутизаторе с IP-адресом. Он используется для того, чтобы маршрутизатор мог обрабатывать пакеты, предназначенные для этого IP.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка маршрутизации

В таблице маршрутизации символ «**C**» рядом с маршрутом означает, что это сеть с прямым подключением. Когда интерфейс маршрутизатора настраивается с глобальным индивидуальным адресом и находится в активном состоянии (up/up), IPv6-префикс и длина префикса добавляются в таблицу IPv6-маршрутизации в качестве подключенного маршрута.

Глобальный индивидуальный адрес IPv6, настраиваемый на интерфейсе, также заносится в таблицу маршрутизации в качестве локального маршрута. Локальный маршрут имеет префикс /128. Локальные маршруты используются таблицами маршрутизации для эффективной обработки пакетов с адресом интерфейса маршрутизатора в качестве назначения.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Проверка обмена данными между сетями, подключенными напрямую Фильтрация выходных данных команды Show

Команды, которые производят несколько экранов выходных данных, по умолчанию приостанавливаются после 24 строк. В конце приостановленных выходных данных отображается текст --More--. Для вывода следующей строки нажмите **ВВОД**, а для отображения набора строк нажмите ПРОБЕЛ. Для указания количества отображаемых строк используйте команду **terminal length**. Значение 0 (ноль) позволяет просмотреть выходные данные без приостановки в процессе вывода данных на экран.

Удобство работы с интерфейсом командной строки также можно повысить с помощью фильтрации выходных данных команды **show**. Для отображения определенных разделов выходных данных можно использовать команды фильтрации. Чтобы включить фильтрацию, введите вертикальную черту (|) после команды **show**, а затем введите параметр и выражение фильтрации.

К параметрам фильтрации, которые следует указывать после вертикальной черты, относятся:

- section — показать целый раздел, который начинается с заданного фильтра.
- include — включить все строки выходных данных, которые соответствуют заданному фильтру.
- exclude — исключить все строки выходных данных, которые соответствуют заданному фильтру.
- begin — показать все строки выходных данных от конкретного места, начиная с линии, которая соответствует заданному фильтру.

© Cisco и/или Партнеры, 2016 г. Все права защищены.

Проверка обмена данными между сетями, подключенными напрямую Функция журнала команд

Функция истории команд обеспечивает возможность временного хранения списка выполненных команд для последующего просмотра.

Для вызова команды из буфера команд нажмите комбинацию клавиш **Ctrl+P** или клавишу **СТРЕЛКА ВВЕРХ**. Отображение команд начинается с последней выполненной команды. Повторяйте это сочетание клавиш для вызова каждой последующей, более старой команды. Для возврата к последним выполненным командам нажмите комбинацию клавиш **Ctrl+N** или клавишу **СТРЕЛКА ВНИЗ**. Повторяйте это сочетание клавиш для вызова каждой последующей, более новой команды.

Функция истории команд включена по умолчанию; система записывает последние десять командных строк в своем буфере. Чтобы отобразить содержимое буфера, используйте команду привилегированного режима **show history**.

На время текущего сеанса можно увеличить количество командных строк, записываемых в буфер. Для того чтобы увеличить или уменьшить размер буфера, используйте команду пользовательского режима **terminal history size**.

Packet Tracer - Проверка связи между подключенными напрямую сетями

В рамках данного упражнения Packet Tracer необходимо решить следующие задачи.

- Проверка связи IPv4 между подключенными напрямую сетями
- Проверка связи IPv6 между подключенными напрямую сетями
- Поиск и устранение неполадок подключения

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

1.6 Практика и контрольная работа модуля

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Packet Tracer - Реализация небольшой сети

В этом упражнении Packet Tracer вам нужно:

- Создание топологии сети
- Настройка устройств и проверка подключения

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

— настройка основных параметров маршрутизатора

В этой лабораторной работе вы выполните следующие задачи.

- Настройка топологии и инициализация устройств
  - Подключите кабели к оборудованию в соответствии с топологией сети.
  - Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.
- Настройка устройств и проверка подключения
  - Назначение статической информации IPv4 и IPv6 интерфейсу ПК
  - Настройка основных параметров маршрутизатора
  - Настройте на маршрутизаторе протокол SSH.
  - Проверка сетевого подключения

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Что я изучил в этом модуле?

- После включения коммутатор Cisco проходит следующие стадии загрузки:
- Переменная среды BOOT устанавливается с помощью команды режима глобальной конфигурации boot system.
- Индикаторы коммутатора и его портов служат для контроля его работы и характеристик.
- Загрузчик предоставляет доступ к коммутатору, если операционная система не может быть использована из-за отсутствия или повреждения системных файлов.
- Чтобы подготовить коммутатор для доступа к удаленному управлению, он должен быть настроен с IP-адресом и маской подсети.
- Имейте в виду, что для управления коммутатором из удаленной сети на коммутаторе должен быть настроен на шлюз по умолчанию.
- Полнодуплексная связь повышает эффективность использования полосы пропускания, позволяя обоим сторонам канала одновременно передавать и принимать данные.
- Порты коммутатора можно настроить вручную с помощью определенных параметров дуплекса и скорости.
- Используйте автосогласование, если параметры скорости и дуплексного режима устройства, подключенного к порту, неизвестны или могут измениться.
- Интерфейс с функцией auto-MDIX автоматически определяет требуемый тип кабельного соединения (прямой или перекрестный) и соответствующим образом настраивает подключение.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Что я изучил в этом модуле? (продолжение)

- Существует несколько команд show, которые можно использовать при проверке конфигураций коммутатора.
- Telnet является более ранним протоколом, использующим небезопасную незашифрованную передачу как данных, так и идентификационной информации (имя пользователя и пароль) между взаимодействующими устройствами.
- SSH обеспечивает защиту удаленных подключений, предоставляя надежное шифрование данных аутентификации устройства (имя пользователя и пароль), а также данных, передаваемых между устройствами.
- Имя файла IOS, которое включает комбинацию «k9», поддерживает криптографические функции и возможности.
- Чтобы настроить SSH, необходимо убедиться, что коммутатор поддерживает его, настроить IP-адрес домена, создать пары ключей RSA, настроить аутентификацию с использованием, настроить линии VTY и включить SSH версии 2.
- Чтобы убедиться, что SSH работает, используйте команду , чтобы отобразить данные о версии и конфигурации SSH на устройстве.
- Всегда должны выполняться следующие задачи начальной настройки: присвоить устройству имя, чтобы отличить его от других маршрутизаторов и настроить пароли, настроить баннер для предоставления юридического уведомления о несанкционированном доступе и сохранить изменения на маршрутизаторе.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

Что я изучил в этом модуле? (продолжение)

- Одним из существенных различий между коммутаторами и маршрутизаторами являются поддерживаемые устройствами типы интерфейсов.
- Маршрутизаторы поддерживают локальные и глобальные сети, и могут обеспечивать соединение между разными типами сетей. Таким образом, они поддерживают множество типов интерфейсов.
- Интерфейс обратной петли предоставляет собой логический, внутренний по отношению к маршрутизатору интерфейс. Он не назначается физическому порту и не может быть подключен к другому устройству.
- Для быстрого определения состояния интерфейса используйте следующие команды:
  - **показать краткое описание IP-интерфейса** и **показать краткое описание интерфейса ipv6** , чтобы увидеть сводку всех интерфейсов (адреса IPv4 и IPv6 и рабочее состояние),
  - **показать running-config интерфейс *interface-id***, чтобы увидеть команды, применяемые к указанному интерфейсу, и
  - show ip route — **отображает содержимое таблицы маршрутизации IPv4, которая хранится в ОЗУ.**
- Фильтруйте вывод команды show, используя символ (|). Использовать выражения фильтра: раздел, включить, исключить и начать.
- По умолчанию журнал команд включен и в его буфере хранятся последние 10 команд.
- Чтобы отобразить содержимое буфера, используйте команду привилегированного режима **show history**.

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

New Terms and Commands

- **boot system flash**
- Power over Ethernet (PoE)
- **duplex**
- **speed**
- auto-mdix
- **show controllers ethernet controller X**
- **phy**
- **show flash**
- **show history**
- **show ip ssh**
- **ip ssh version 2**
- Loopback Interface
- **interface loopback x**
- **include**
- **exclude**
- **section**
- **show history**
- **terminal history size**

© Cisco и/или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

CISCO