МОДУЛЬ 1. БАЗОВАЯ НАСТРОЙКА УСТРОЙСТВ

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

1.1 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

1.1.1 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.

1.1.2 ЗАГРУЗКА СИСТЕМЫ

Коммутатор 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

1.1.3 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 его состояние.

Индикатор состояния порта (STAT). Зеленый цвет указывает, что выбран режим состояния порта, который является значением по умолчанию. Статус порта может быть обозначен светом, связанным с каждым портом.

Светодиодный индикатор дуплекса порта (DUPLX). Зеленый цвет указывает, что выбран режим дуплекса порта. Дуплекс порта может быть обозначен светом, связанным с каждым портом.

Индикатор скорости порта (SPEED). Зеленый цвет указывает, что выбран режим скорости порта. Скорость порта может быть обохначена светом, связанным с каждым портом.

Power over Ethernet (PoE). Присутствует, если коммутатор поддерживает PoE. Указывает состояние PoE портов коммутатора.

Кнопка Mode используется для перемещения между различными режимами — STAT, DUPLX, SPEED и PoE

1.1.4 РАСШИФРОВКА ИНДИКАТОРОВ

	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	RPS обеспечивает питание	—
PoE	Не выбрано, проблем нет	Выбранный	—	—	Не выбран, проблемы с портом присутствуют	—
При выборе именованного режима свет, связанный с каждым физическим портом, указывает:						
STAT	Нет связи или выключен	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	—	PoE отключен	Питание PoE отключено из-за ошибки.	PoE отклонено (сверх бюджета)

1.1.5 ВОССТАНОВЛЕНИЕ ПОСЛЕ СБОЯ СИСТЕМЫ

Начальный загрузчик обеспечивает доступ к коммутатору, если ОС нельзя использовать из-за недостающих или повреждённых системных файлов. В начальном загрузчике есть командная строка, обеспечивающая доступ к файлам, которые хранятся во флеш-памяти.

Доступ в начальный загрузчик можно получить через консольное подключение, выполнив следующие действия:

Шаг 1. Подсоедините ПК с помощью консольного кабеля к консольному порту коммутатора. Настройте программу эмуляции терминала для подключения к коммутатору.

Шаг 2. Отсоедините кабель питания коммутатора.

Шаг 3. Заново подключите провод питания к коммутатору и по истечении 15 секунд нажмите и удерживайте кнопку **Mode**, пока системный индикатор мигает зелёным светом.

Шаг 4. Удерживайте кнопку **Mode**, пока системный индикатор не мигнёт желтым, а затем загорится зелёным. После этого отпустите кнопку **Mode**.

Шаг 5. В программе эмуляции терминала появится командная строка начального загрузчика **switch:**.

Командная строка **boot loader** поддерживает команды для форматирования файловой системы флеш-памяти, переустановки операционной системы и восстановления утерянного или забытого пароля. Например, команду **dir** можно использовать для просмотра списка файлов в указанном каталоге.

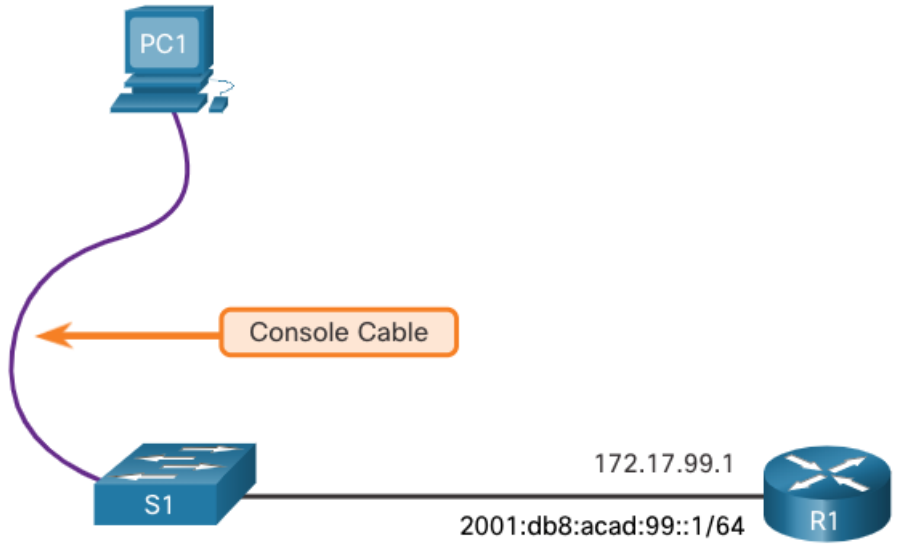
1.1.6 НАСТРОЙКА ДОСТУПА ДЛЯ УПРАВЛЕНИЯ КОММУТАТОРОМ

Чтобы настроить на коммутаторе возможность для удалённого управления, на коммутаторе нужно настроить IP-адрес и маску подсети. Помните, что для управления коммутатором из удалённой сети для него необходимо настроить шлюз по умолчанию. Подобная настройка мало чем отличается от настройки информации об IP-адресах на физических узлах. На данном рисунке IP-адрес следует назначить интерфейсу SVI коммутатора S1. SVI — это виртуальный интерфейс, а не физический порт коммутатора.

Понятие SVI относится к сетям VLAN. Сети VLAN— это пронумерованные логические группы, которым можно присвоить физические порты. Конфигурации и настройки, которые применены к VLAN, также применяются ко всем портам, назначенным для этой VLAN.

По умолчанию коммутатор настроен для управления через VLAN 1. По умолчанию все порты ассоциируются с VLAN 1. В целях безопасности не рекомендуется использовать сеть VLAN 1 в качестве сети управления VLAN.

Обратите внимание, что эти параметры IP применимы только для доступа к удалённому управлению коммутатором; параметры IP не позволяют коммутатору маршрутизировать пакеты на 3-м уровне.



1.1.7 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 (см. следующий слайд).

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.

1.1.7 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**

1.1.7 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 для 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**

1.1.7 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)
```

1.2. НАСТРОЙКА ПОРТОВ КОММУТАТОРА

1.2.1 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.

1.2.2 НАСТРОЙКА ПОРТОВ КОММУТАТОРА НА ФИЗИЧЕСКОМ УРОВНЕ

Порты коммутаторов можно настроить вручную с определёнными параметрами скорости и дуплексного режима. Используйте команду режима конфигурации интерфейса **duplex**, чтобы вручную установить дуплексный режим для порта коммутатора. Используйте команду режима конфигурации интерфейса **speed**, чтобы вручную задать скорость для порта коммутатора.

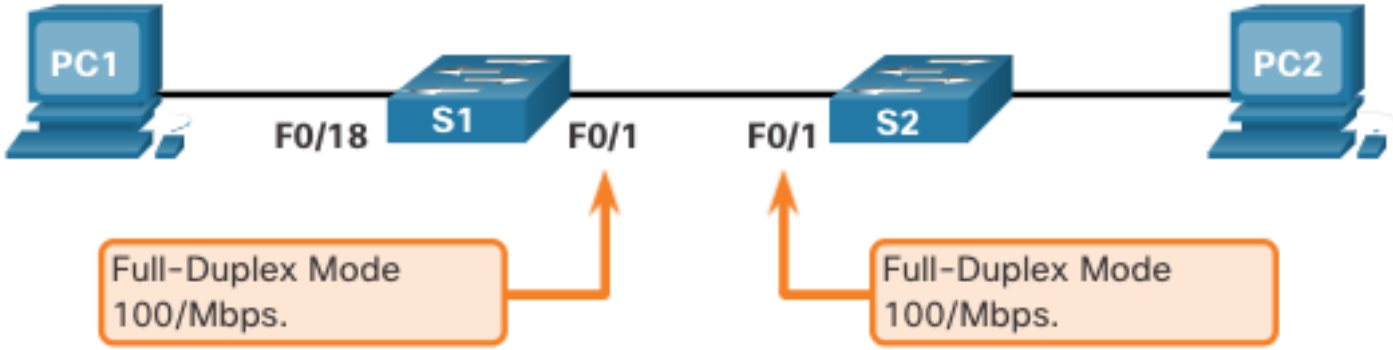
По умолчанию на коммутаторах Cisco Catalyst 2960 и 3560 настройки дуплексного режима и скорости выставлены в режим Auto. Порты 10/100/1000 функционируют в полудуплексном либо в полнодуплексном режиме, если установлена скорость 10 или 100 Мбит/с, и только в полнодуплексном, если задана скорость 1000 Мбит/с. Автосогласование полезно, когда настройки скорости и дуплекса для устройства, подключенного к порту, неизвестны или могут меняться. При подключении к известным устройствам, таким как серверы, выделенные рабочие станции или сетевые устройства, рекомендуется вручную задавать параметры скорости и дуплекса.

При поиске и устранении проблем с портом коммутатора необходимо проверить настройки дуплексной связи и скорости.

Примечание. Несовпадения в настройках дуплексного режима и скорости портов коммутаторов могут вызвать проблемы с подключением. Ошибка при автосогласовании приводит к несовпадениям в настройках.

Все порты оптоволоконных кабелей, например порты 100BASE-FX, работают только на предустановленной скорости и всегда в полнодуплексном режиме.

1.2.2 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**

1.2.3 ФУНКЦИЯ AUTO-MDIX

До недавнего времени при соединении устройств требовались определённые типы кабелей (прямые или кроссовые). Для соединения двух коммутаторов или коммутатора и маршрутизатора требовались разные кабели стандарта Ethernet. Использование функции автоматического определения кабеля (auto-MDIX) решило эту проблему. При включенной функции auto-MDIX интерфейс распознаёт требуемый тип кабельного соединения (прямое или кроссовое) и настраивает подключение соответствующим образом. В случае подключения к коммутаторам без функции auto-MDIX для соединения серверов, рабочих станций или маршрутизаторов следует использовать прямые кабели, тогда как для подключения к другим коммутаторам или повторителям используются кроссовые кабели.

Включённая функция auto-MDIX позволяет использовать любой тип кабеля для подключения к другим устройствам, а интерфейс автоматически настраивается для успешного взаимодействия. На новых маршрутизаторах и коммутаторах Cisco эту функцию включает команда режима конфигурации интерфейса **mdix auto**. При использовании функции auto-MDIX на интерфейсе скорость интерфейса и дуплексный режим должны быть настроены в режим auto, чтобы функция работала должным образом.

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

Чтобы просмотреть настройки функции auto-MDIX для конкретного интерфейса, следует использовать команду **show controllers ethernet-controller** с ключевым словом **phy**. Для отображения выходных данных, имеющих отношение к функции auto-MDIX, используйте фильтр **include Auto-MDIX**.

1.2.4 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**

1.2.5 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
```

1.2.5 ПРОВЕРКА КОНФИГУРАЦИИ ПОРТОВ КОММУТАТОРА

Команда **show interfaces** является ещё одной распространённой командой, которая выводит данные о состоянии и статистике сетевых интерфейсов коммутатора. Команда **show interfaces** часто используется при настройке и мониторинге сетевых устройств.

На рисунке показаны выходные данные команды **show interfaces fastEthernet 0/18**. Первая строка на рисунке ниже указывает, что интерфейс FastEthernet 0/18 находится в состоянии up/up, т.е. в рабочем состоянии. Выходные данные ниже показывают, что включён полнодуплексный режим, а скорость настроена на 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
```

1.2.6 ПРОБЛЕМЫ НА УРОВНЕ СЕТЕВОГО ДОСТУПА

Результат команды **show interfaces** можно использовать для обнаружения типичных проблем среды передачи данных. Важнейшие составляющие этих выходных данных отображают состояние протокола канального уровня и протокола канала передачи данных. На рисунке показана итоговая строка для проверки состояния интерфейса.

Первый параметр (FastEthernet0/1 is up) относится к аппаратному уровню и, по сути, указывает, получен ли интерфейсом сигнал обнаружения несущей от другого оконечного устройства. Второй параметр (line protocol is up) относится к канальному уровню. Он указывает, принимаются ли keepalive сообщения протокола канального уровня.

Используя результат команды **show interfaces**, можно устранить возможные проблемы следующим образом.

Если интерфейс включен, а канальный протокол не функционирует, существует проблема. Возможно несоответствие в типе инкапсуляции, интерфейс на другом конце мог быть выключен в результате сбоя или могли возникнуть проблемы с аппаратным обеспечением.

```
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,
```

1.2.6 ПРОБЛЕМЫ НА УРОВНЕ СЕТЕВОГО ДОСТУПА

В случае если протокол канального уровня (Line protocol) и интерфейс отключены, возможно, не подключён кабель или существуют другие проблемы с интерфейсом. Например, при соединении двух устройств напрямую мог быть отключен интерфейс на другом конце.

Если интерфейс отключён администратором, он был отключён вручную (с помощью команды **shutdown**) в активной конфигурации.

Выходные данные команды **show interfaces** отображают счетчики и статистику для интерфейса FastEthernet0/18, как показано на рисунке.

```
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
```

1.2.6 ПРОБЛЕМЫ НА УРОВНЕ СЕТЕВОГО ДОСТУПА

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.

1.1.7 ОШИБКИ ВВОДА ВЫВОДА

«Ошибки ввода» — это сумма всех ошибок в датаграммах, которые были получены при анализе интерфейса. Они включают в себя карликовые (runts) и гигантские (giants) кадры, ошибки CRC, отсутствие буфера, кадр, переполнение и проигнорированные пакеты. К ошибкам ввода, которые можно обнаружить с помощью команды show interfaces, относятся следующие:

Карликовые кадры (runt frames) — кадры Ethernet, размер которых не превышает минимально разрешённые 64 байта. Карликовые кадры чаще всего бывают вызваны неисправностью сетевой платы, но могут быть обусловлены и другими причинами, например чрезмерно высоким числом коллизий.

Гигантские кадры (giants) — кадры Ethernet, размер которых превышает максимальную длину кадра. Наличие гигантских кадров вызвано теми же причинами, что и наличие карликовых.

Ошибки CRC — в Ethernet и последовательных интерфейсах ошибки CRC обычно свидетельствуют о неполадках в среде передачи или кабеле. Частыми причинами ошибок являются электрические наводки, плохо закреплённые или повреждённые разъемы, а также неверно выбранный тип кабеля. Большое количество ошибок CRC приводит к шуму на канале, поэтому следует проверить кабель на повреждения и допустимую длину. Также по возможности следует найти и устранить источники шума.

1.1.7 ОШИБКИ ВВОДА ВЫВОДА

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

Коллизии — коллизии в полудуплексном режиме являются нормой, поэтому о них не стоит беспокоиться до тех пор, пока работа полудуплексного режима вас устраивает. Однако в правильно спроектированной и настроенной сети с использованием полнодуплексной связи коллизий быть не должно. Мы настоятельно рекомендуем использовать полнодуплексную связь, за исключением случаев, когда вы работаете с устаревшим оборудованием, требующим использования полудуплексного режима.

Поздние коллизии — это коллизии, которые происходят после передачи 512 бит кадра (преамбулы). Наиболее распространённая причина поздних коллизий — превышение допустимой длины кабеля. Неправильная настройка дуплексной связи также может вызывать поздние коллизии, например, в случае, когда один конец соединения настроен на полнодуплексный режим, а другой конец — на полудуплексный режим. Вы обнаружите поздние коллизии на интерфейсе, настроенном на полудуплексный режим. Для решения данной проблемы необходимо настроить один и тот же дуплексный режим на обоих концах соединения. В правильно спроектированной и настроенной сети поздние коллизии возникать не должны.

1.1.8 ПОИСК И УСТРАНЕНИЕ НЕПОЛАДОК НА УРОВНЕ СЕТЕВОГО ДОСТУПА

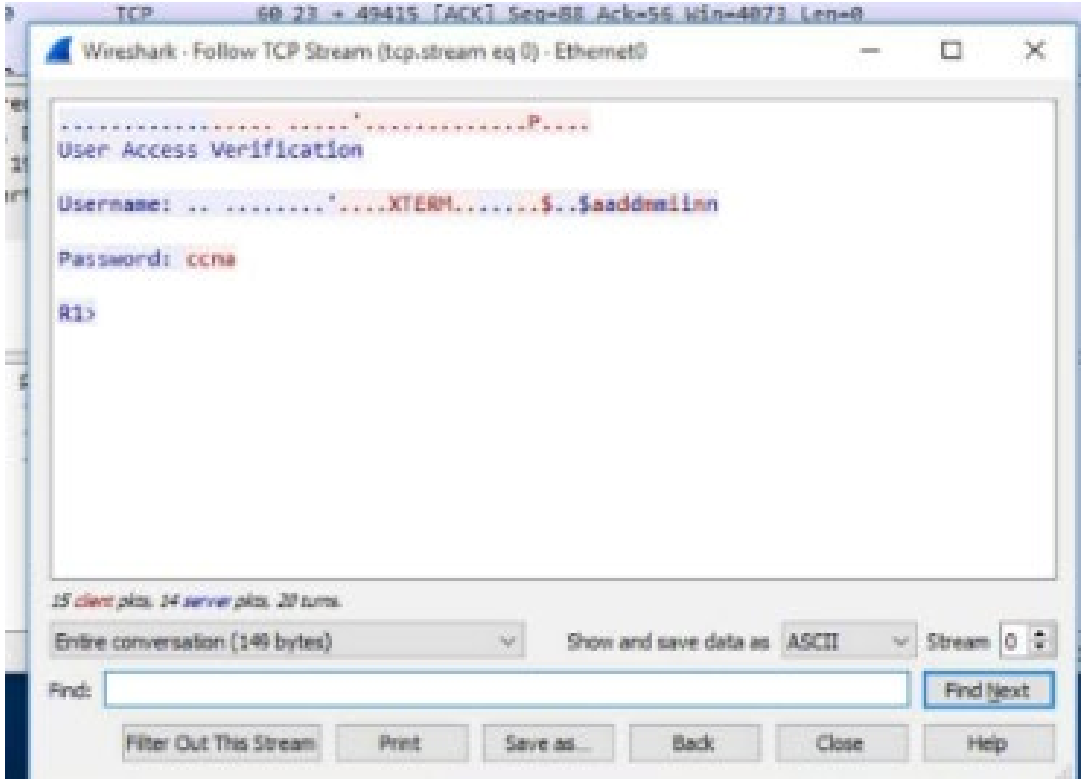
Для поиска и устранения неполадок при отсутствии или плохом качестве соединения коммутатора с другим устройством следуйте данному алгоритму действий:

1.3 УДАЛЕННЫЙ ЗАЩИЩЕННЫЙ ДОСТУП

1.3.1 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.

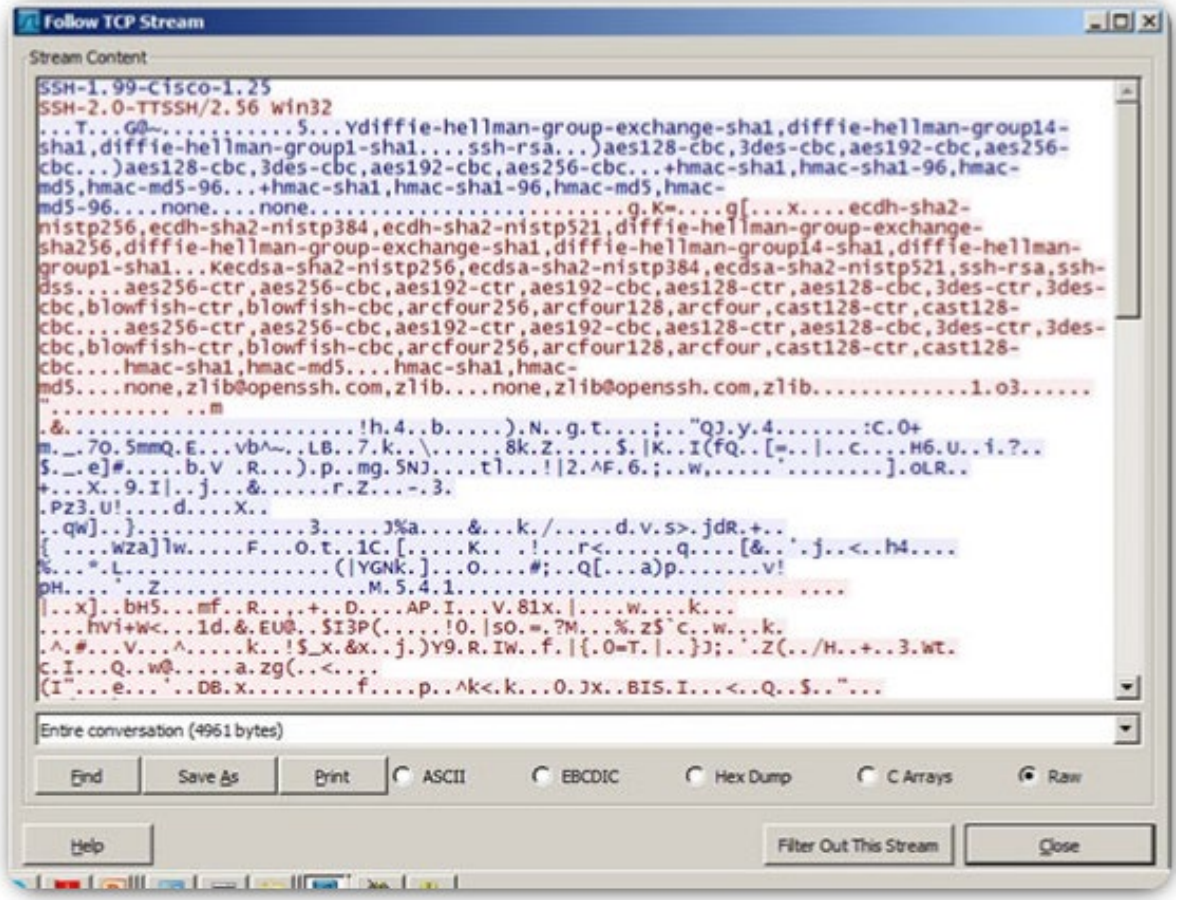
Злоумышленник может отслеживать пакеты с помощью Wireshark. Например, на рисунке актер угрозы захватил имя пользователя admin и пароль ccna из сеанса Telnet.



1.3.2 ПРИНЦИП РАБОТЫ ПРОТОКОЛА SSH

Протокол Secure shell (SSH) — это протокол, который обеспечивает безопасное (зашифрованное) соединение для управления удалённым устройством. Для безопасного управления удалёнными подключениями Cisco рекомендует заменить протокол Telnet протоколом SSH.

SSH обеспечивает защиту удалённых соединений, предоставляя надёжное шифрование данных аутентификации устройства (имя пользователя и пароль), а также данных, передаваемых между устройствами. SSH использует TCP-порт 22.



1.3.3 ПРОВЕРКА ПОДДЕРЖКИ SSH

Для функционирования протокола SSH на коммутаторе Catalyst 2960 коммутатор должен использовать версию ПО IOS с криптографическими функциями и возможностями (шифрованием). Используйте команду **show version** на коммутаторе, чтобы узнать, на какой версии IOS работает в данный момент коммутатор, как показано на рисунке.

В случае если имя операционной системы включает в себя сочетание k9, то данная версия IOS осуществляет поддержку криптографических функций и возможностей (шифрование).

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

1.3.4 НАСТРОЙКА ПРОТОКОЛА SSH

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

Шаг 1. Проверка поддержки протокола SSH. Чтобы проверить, поддерживается ли протокол SSH, используйте команду **show ip ssh**. Если на коммутаторе работает IOS, не поддерживающая криптографические функции, данная команда не будет распознана.

Шаг 2. Настройка домена IP. Присвойте имя IP-домену сети с помощью команды режима глобальной конфигурации **ip domain-name имя домена**.

Шаг 3. Создание пар ключей RSA. Не во всех версиях IOS по умолчанию используется версия 2 протокола SSH, а версия 1 SSH содержит ряд известных уязвимостей. Для настройки SSH версии 2 выполните команду режима глобальной конфигурации **ip ssh version 2**. Создание пары ключей RSA автоматически включает протокол SSH. Используйте команду режима глобальной конфигурации **crypto key generate rsa**, чтобы включить сервер SSH на коммутаторе и сгенерировать пару ключей RSA. При создании ключей RSA администратору требуется ввести длину модуля. Cisco рекомендует минимальный размер модуля 1024 бит. Более длинный модуль безопаснее, но его создание и использование требует больше времени.

Примечание. Для удаления пары ключей RSA используйте команду режима глобальной конфигурации **crypto key zeroize rsa**. После удаления пары ключей RSA SSH-сервер автоматически отключается.

1.3.4 НАСТРОЙКА ПРОТОКОЛА SSH

Шаг 4. Настройка аутентификации пользователя. SSH-сервер может аутентифицировать пользователей локально или с помощью сервера аутентификации. Для использования локального метода аутентификации создайте пару «имя пользователя — пароль» с помощью команды режима глобальной конфигурации **username имя_пользователя secret пароль**.

Шаг 5. Настройка каналов vty. Включите протокол SSH на каналах vty с помощью команды режима конфигурации канала **transport input ssh**. Диапазон каналов vty коммутатора Catalyst 2960 составляет от 0 до 15. Данная конфигурация предотвращает подключения по протоколам кроме SSH (например Telnet) и разрешает коммутатору принимать подключения только по протоколу SSH. Используйте команду режима глобальной конфигурации line vty, а затем команду режима конфигурации канала **login local**, чтобы при подключениях SSH требовалась локальная аутентификация из локальной базы данных имён.

Шаг 6. Включите SSH версии 2. По умолчанию SSH поддерживает обе версии (1 и 2). Если поддерживаются обе версии, результат команды **show ip ssh** сообщает о поддержке версии 1.99. У версии 1 есть ряд известных уязвимостей. По этой причине рекомендуется включать только версию 2. Включите эту версию SSH, используя команду режима глобальной конфигурации **ip ssh version 2**.

1.3.5 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. Здесь 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#
```

1.3.6 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#
```

1.4 БАЗОВАЯ КОНФИГУРАЦИЯ МАРШРУТИЗАТОРА

1.4.1 ПРИМЕРЫ БАЗОВОЙ НАСТРОЙКИ МАРШРУТИЗАТОРА

Маршрутизаторы и коммутаторы Cisco во многом похожи. Они поддерживают сходные 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. Дайте имя устройству, 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)#
```

1.4.2 НАСТРОЙКА ОСНОВНЫХ ПАРАМЕТРОВ МАРШРУТИЗАТОРА

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

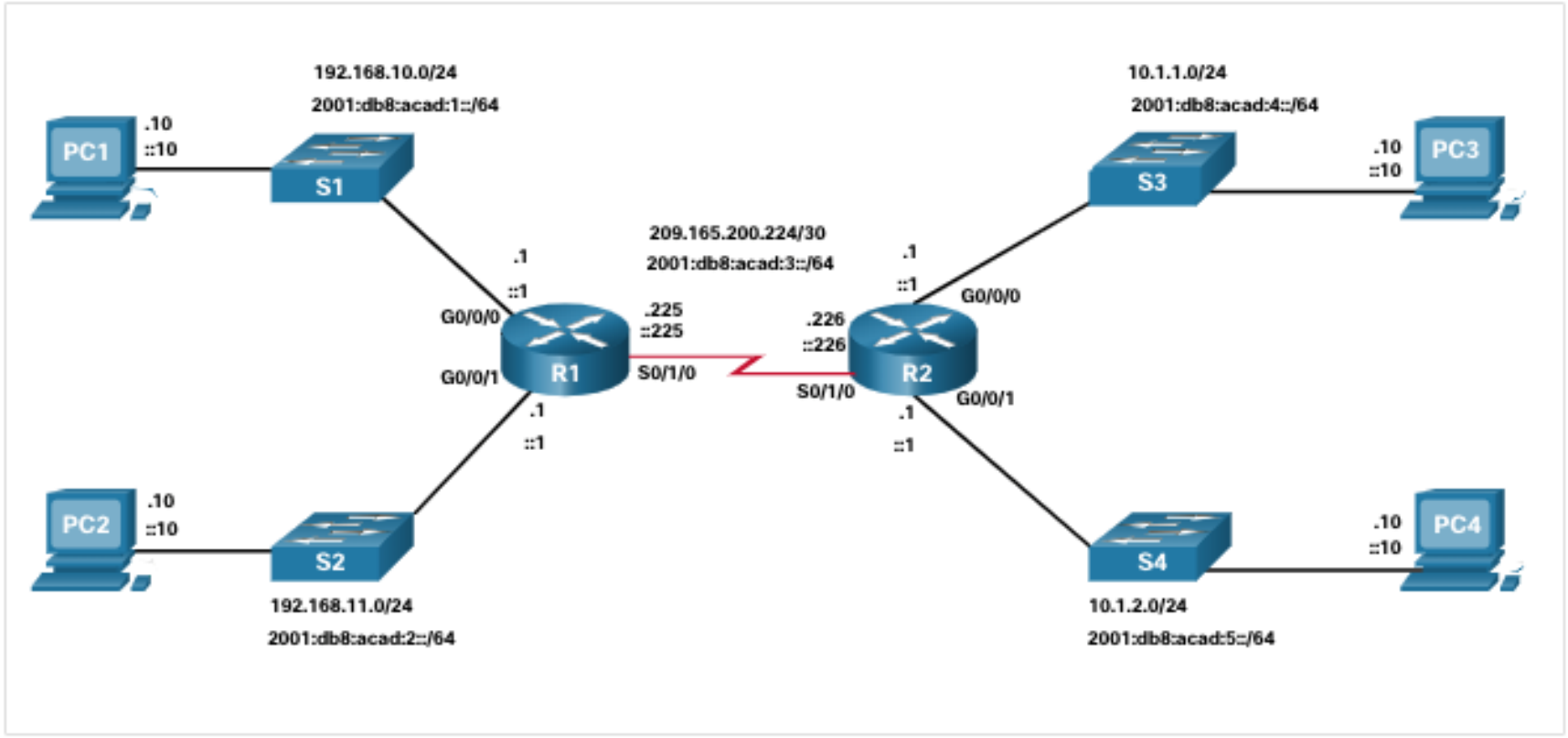
```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Сохраните изменения на маршрутизаторе, как показано в примере.

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

1.4.3 ТОПОЛОГИЯ 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.



1.4.4 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:

1. Настроить по крайней мере один интерфейс с IP-адресом. Используйте команды конфигурации интерфейса **interface IPv6 ipv6-address/prefixip-address** .

2. 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).

3. 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.

1.4.4 НАСТРОЙКА ИНТЕРФЕЙСОВ МАРШРУТИЗАТОРА

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)#
```

1.4.5 ИНТЕРФЕЙСЫ LOOPBACK IPV4

Другая распространенная конфигурация маршрутизаторов Cisco IOS — задействование интерфейса loopback.

Интерфейс loopback 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 loopback 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 loopback для имитации ссылки на Интернет.

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

1.5 ПРОВЕРКА СВЯЗИ МЕЖДУ ПОДКЛЮЧЕННЫМИ НАПРЯМУЮ СЕТЯМИ

1.5.1 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».

1.5.1 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 «up» и протоколе «up», как показано в примере. Получение других выходных данных указывает на проблему с конфигурацией или кабельным соединением.

```
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
```

1.5.2 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 рисунке, 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
```

1.5.3 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#
```

1.5.4 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#
```

1.5.4 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#
```

1.5.5 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.

1.5.6 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**.