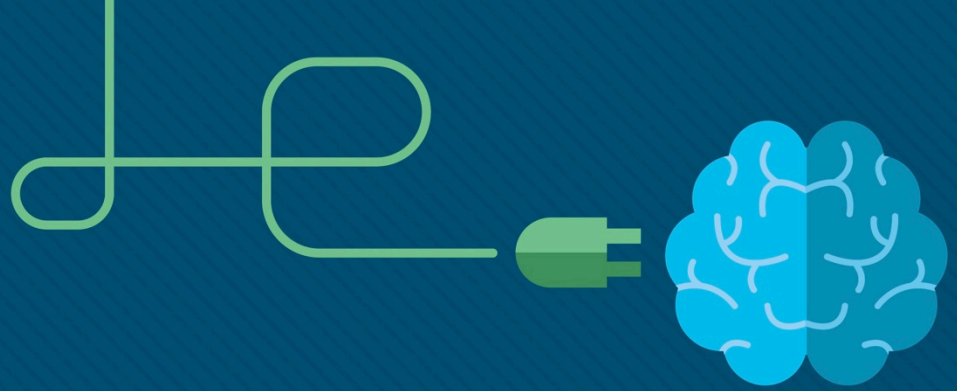


Глава 5. Конфигурация коммутатора

Материалы для инструктора

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Материалы для инструкторов. Глава 5. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 16

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

Глава 5. Конфигурация коммутатора

Routing and Switching Essentials 6.0.
Руководство по планированию

Глава 5. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
5.0.1.2	Упражнение в аудитории	Запишите число	Необязательно
5.1.1.6	Лабораторная работа	Базовая настройка коммутатора	Рекомендуется
5.1.2.2	Инструмент проверки синтаксиса	Настройка параметров дуплексного режима и скорости коммутационного порта	Рекомендуется
5.1.2.3	Инструмент проверки синтаксиса	Настройка функции Auto MDIX	Рекомендуется
5.2.1.2	Syntax Checker (Средство проверки синтаксиса)	Настройка SSH на линиях VTY	Рекомендуется
5.2.1.4	Packet Tracer	Настройка SSH	Рекомендуется
5.2.2.7	Packet Tracer	Настройка функции безопасности порта коммутатора	Рекомендуется
5.2.2.8	Packet Tracer	Поиск и устранение неполадок в системе безопасности портов коммутатора	Рекомендуется
5.2.2.9	Лабораторная работа	Настройка параметров безопасности коммутатора	Необязательно
5.3.1.1	Упражнение в аудитории	Коммутационное трио	Необязательно
5.3.1.2	Packet Tracer	Отработка комплексных практических навыков	Рекомендовано

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**.

Глава 5. Проверочная работа

- Закончив работу с главой 5, студенты должны выполнить проверочную работу по материалам этой главы.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

Глава 5. Практические рекомендации

Перед началом обучения по материалам главы 5 инструктор должен выполнить следующие действия.

- Выполнить проверочную работу по главе 5.
- Цели этой главы:
  - настройка начальных параметров на коммутаторе Cisco;
  - настройка портов коммутатора в соответствии с требованиями сети.
  - Настройте виртуальный интерфейс управления на коммутаторе.
  - Настройте функцию обеспечения безопасности портов для ограничения сетевого доступа.

Глава 5. Практические рекомендации (продолжение)

- Создайте топологию Packet Tracer с коммутатором и двумя или тремя подключенными к нему компьютерами, можно было использовать эту демонстрацию при прохождении всей главы.
- ? — это ключ к жизнеспособности IOS. Напомните студентам, что знак «?» — это их друг в любом устройстве Cisco. Скажите, что им следует постоянно им пользоваться при выполнении упражнений и лабораторных работ в аудитории и дома.
- Напомните студентам, насколько важную роль играют коммутаторы в любой компании. Даже если они являются инженерами начального уровня, велика вероятность того, что им попросят подключить и настроить коммутатор.
- Запишите на доске следующие термины и напомните студентам, где хранится различная информация.
  - ПЗУ — содержит ПО процедуры POST и начального загрузчика с кодом для проверки аппаратного обеспечения и обнаружения операционной системы, разрешенной для загрузки.
  - Флеш-память — содержит операционную систему.
  - ОЗУ — содержит текущую конфигурацию (команды, которые вводятся в коммутатор).
  - NVRAM — содержит конфигурацию, сохраненную при вводе команды **copy running-config startup-config** на маршрутизаторе Cisco или в командной строке коммутатора.

Глава 5. Практические рекомендации (продолжение)

- Установите коммутатор в передней части аудитории и напомните студентам, что консоль подключается к порту с меткой Console, расположенному на задней панели коммутатора, а подключение Ethernet идет от порта Ethernet компьютера или IP-телефона к передней панели коммутатора.
- Выполните команду **show boot** на коммутаторе в Packet Tracer и покажите студентам, какая IOS загружается.
- Запишите на доске три приглашения к вводу команды, которые выдает коммутатор, и спросите студентов, в чем состоит различие между ними.
  - Switch> (пользовательский режим EXEC; отображается при первой загрузке коммутатора)
  - Switch# (привилегированный режим EXEC; отображается после ввода команды **enable**)
  - switch: (режим начального загрузчика; отображается, когда на коммутаторе отсутствует операционная система или ее не удается обнаружить)
- Объясните, что для присутствия в сети коммутатору необходим IP-адрес точно так же, как любому устройству на основе TCP/IP (например, ПК).

Глава 5. Практические рекомендации (продолжение)

- Нарисуйте на доске три не соединенные друг с другом сети Ethernet (коммутатор с несколькими подключенными к нему ПК). Под сетями подпишите «Сеть 1», «Сеть 2» и «Сеть 3». Объясните, что при работе с коммутаторами вводится новый термин — виртуальная локальная сеть (VLAN). Сеть VLAN — это просто еще одно название сети с тем исключением, что ей дается номер. Под каждой сетью запишите следующее: VLAN 1 под словами «Сеть 1», VLAN 2 под «Сеть 2» и VLAN 3 под «Сеть 3». Затем укажите, что каждая сеть VLAN имеет свой номер.
- Объясните, что особая сеть VLAN используется только для сетевых устройств. К этой сети обычно не подключаются никакие пользователи. Это делается лишь в некоторых лабораторных работах и только для демонстрации студентам других принципов. Эта сеть VLAN называется сетью управления VLAN или просто сетью управления.
- Расскажите, что, в отличие от ПК, в коммутаторе IP-адрес назначается виртуальному интерфейсу, а не физическому порту Ethernet.

Глава 5. Практические рекомендации (продолжение)

- Напишите следующие команды на доске или введите их в коммутатор в Packet Tracer. Объясните, что рекомендуется назначать IP-адрес, шлюз по умолчанию, а также имя сети VLAN. Если коммутатор доступен в сети, его можно настраивать с удаленного устройства. Отметьте, что команды "vlan 99" и "name Management" рассматриваются в следующей главе, но обычно вводятся при настройке IP-адреса коммутатора.
  - **config t**
    interface vlan 99
    ip address 172.17.99.11 255.255.255.0
    no shutdown
    ip default-gateway 172.16.99.1 (адрес маршрутизатора, который находится в той же сети 172.17.99.0)
    vlan 99
    name Management
    exit
- Опишите, что очень важное соединение, например от коммутатора к сетевому принтеру, может быть автоматически согласовано с полудуплексом или со сниженной скоростью. Опишите, почему полезной бывает настройка дуплекса и скорости на устройстве вручную. Также расскажите, что это позволяет избежать проблем с подключением.

Глава 5. Практические рекомендации (продолжение)

- Откройте раздел 5.1.2.5 учебного плана и объясните следующие состояния.
  - Состояние интерфейса Up — состояние протокола линии связи Up (Up и Up в выходных данных команды **show interfaces** или **show ip interface brief**): состояние готовности
  - Состояние интерфейса Up — состояние протокола линии связи Down (Up и Down): обычно это проблема на уровне 2 с инкапсуляцией на другой стороне канала, или, возможно, возникла проблема с аппаратным обеспечением, хотя это менее вероятно.
  - Состояние интерфейса Down — состояние протокола линии связи Down (Down и Down): обычно это проблема на уровне 1 — проверьте кабель или порт.
  - Состояние интерфейса administratively down: используйте команду **no shutdown**, чтобы запустить интерфейс.
- Опишите, почему важно использовать протокол SSH вместо Telnet, но он должен поддерживаться версией IOS.
- Покажите рис. 1 из раздела 5.2.1.2 учебного плана и опишите действия для настройки протокола SSH.
  - Не забудьте объяснить, что команда **ip domain-name** используется для создания ключей RSA для SSH. Если доменное имя не задано, то при выполнении команды **crypto key generate** появится сообщение об ошибке, гласящее, что сначала необходимо определить доменное имя.

Глава 5. Практические рекомендации (продолжение)

- Рекомендации по обеспечению информационной безопасности:
  - Отключите порты, к которым не подключены устройства, с помощью команды **shutdown**.
  - Не используйте имя VLAN 1, так как оно чаще всего подвергается атакам.
  - Используйте безопасность портов, чтобы не допустить подключение к сети частных устройств вместо корпоративных проводных устройств.

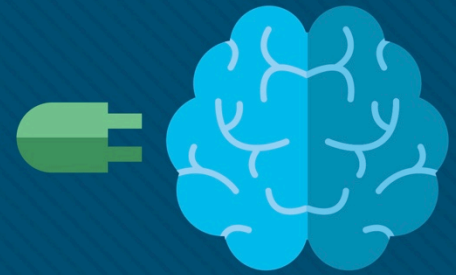
Глава 5. Практические рекомендации (продолжение)

- Полезные команды для использования на коммутаторе:
  - **show interfaces *ид_интерфейса*** или **show ip interface brief**
  - **show ip interface *ид_интерфейса***
  - **show running-config**
  - **show flash**
  - **show version**
  - **show mac-address-table**

Глава 5. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить ее на сайте сообщества сертифицированных компанией Cisco сетевых специалистов (CCNA).
- Студенты могут записаться на курс **Introduction to Packet Tracer** (для самостоятельного изучения).
- Студенты, которые готовятся к экзаменам по главам, финальному экзамену по курсу RSE или сертификации CCENT, могут просмотреть 15 занятий и видеороликов на веб-сайте Cisco Networking/CCENT Wikiversity: https://en.wikiversity.org/wiki/Cisco_Networking/CCENT


CISCO



Глава 5. Конфигурация коммутатора

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Глава 5. Разделы и цели

- 5.1. Настройка основных параметров коммутатора
  - Настройка базовых параметров коммутации в соответствии с сетевыми требованиями.
    - Настройка начальных параметров на коммутаторе Cisco.
    - Настройка портов коммутатора в соответствии с требованиями сети.
- 5.2. Базовая настройка устройства
  - Настройте коммутатор с применением практических рекомендаций по обеспечению информационной безопасности в сетях предприятий малого и среднего бизнеса.
    - Настройте виртуальный интерфейс управления на коммутаторе.
    - Настройте функцию обеспечения безопасности портов для ограничения сетевого доступа.

5.1. Первоначальная настройка коммутатора

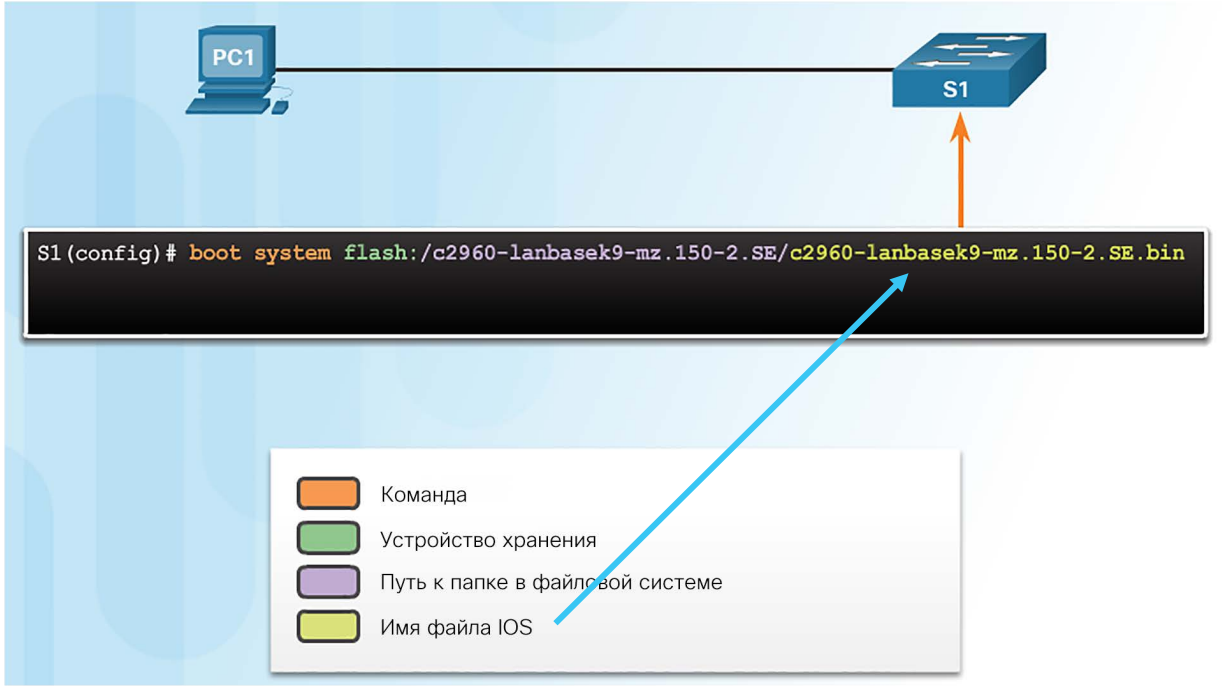
Последовательность загрузки коммутатора

- При включении коммутатора выполняется последовательность загрузки.
  - Выполняется программа самодиагностики при включении питания (POST), хранящаяся в ПЗУ, которая проверяет аппаратное обеспечение, например ЦП и ОЗУ.
  - Запускается начальный загрузчик, также хранящийся в ПЗУ, который инициализирует части ЦП, инициализирует файловую флеш-систему, а затем находит и загружает образ IOS.
    - Образ IOS можно указать в переменной среды BOOT.
    - Если эта переменная не задана, коммутатор просматривает файловую флеш-систему в поиске исполняемого файла образа, и если находит такой файл, то загружает его в ОЗУ и запускает.
    - Если исполняемый файл образа не найден, коммутатор отображает приглашение к вводу команды `switch:`, после чего можно ввести несколько команд для обеспечения доступа к файлам операционной системы, находящимся во флеш-памяти, а также к файлам, используемым для загрузки или перезагрузки операционной системы.
  - Если операционная система IOS загружается, инициализируются интерфейсы коммутатора и загружаются все команды, хранящиеся в файле загрузочной конфигурации.

Файл загрузочной конфигурации хранится в энергонезависимом ОЗУ (NVRAM).

Последовательность загрузки коммутатора (продолжение)

- Команда **boot system** служит для задания переменной среды BOOT.



Восстановление после сбоя системы

- Доступ к командной строке начального загрузчика можно получить через консольное подключение к коммутатору.

  1. Подключите ПК к консольному порту коммутатора с помощью кабеля.
  2. Настройте на ПК программу эмуляции терминалов.
  3. Отсоедините кабель питания коммутатора.
  4. Снова подключите кабель питания и одновременно с этим или в течение 15 секунд нажмите и удерживайте кнопку Mode (Режим) на передней панели коммутатора, пока индикатор System не мигнет желтым, а затем загорится зеленым цветом.

- Командная строка начального загрузчика — **switch:** (а не **Switch>**).
  - В командной строке начального загрузчика можно выполнять только некоторые команды.
  - Чтобы отобразить список доступных команд, используйте команду **help**.

```
switch: dir flash:
Directory of flash:/

    2  -rwx    11607161   Mar 1 2013 03:10:47 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    3  -rwx        1809   Mar 1 2013 00:02:48 +00:00  config.text
    5  -rwx        1919   Mar 1 2013 00:02:48 +00:00  private-config.text
    6  -rwx       59416   Mar 1 2013 00:02:49 +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
```

Светодиодные индикаторы коммутатора

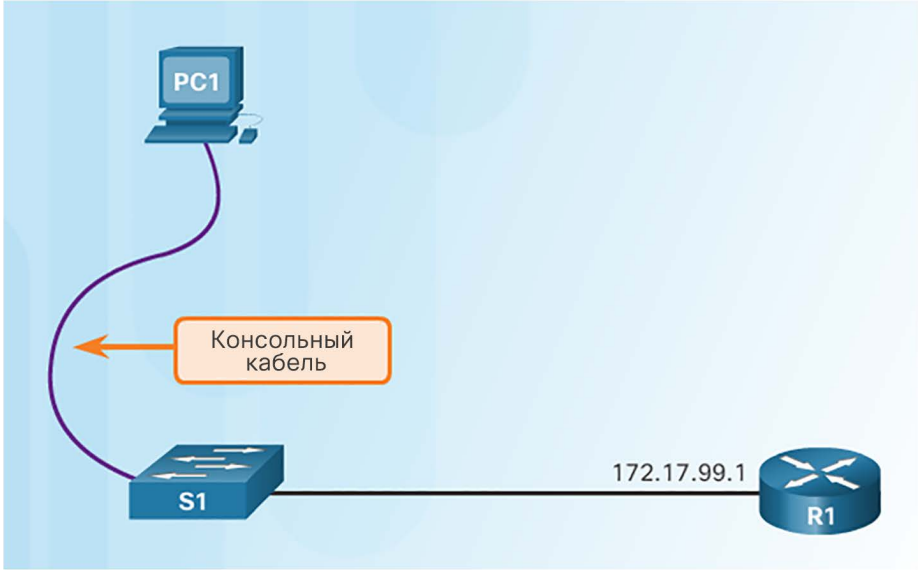
- Светодиодный индикатор System показывает, подается ли на коммутатор питание.
- Состояния индикатора порта:
  - Не горит — канал отсутствует или порт выключен
  - Горит зеленым — канал подключен ▲
  - Мигает зеленым — выполняется передача данных
  - Загорается попеременно зеленым и желтым — сбой канала ▲→▲→▲→▲
  - Горит желтым — порт не отправляет данные; обычно в течение первых 30 секунд после подключения или активации ▲
  - Мигает желтым — порт блокируется для предотвращения образования петли коммутации

Индикаторы коммутатора Catalyst 2960

1	Системный индикатор
2	Индикатор RPS (если на коммутаторе поддерживается RPS)
3	Индикатор состояния порта (это режим по умолчанию)
4	Индикатор дуплексных режимов портов
5	Индикатор скорости порта
6	Индикатор состояния питания через Ethernet (если на коммутаторе поддерживается питание через Ethernet)
7	Кнопка режима
8	Индикаторы портов

Подготовка к базовому управлению коммутатором

- Чтобы настроить на коммутаторе возможность удаленного доступа, необходимо задать IP-адрес, маску подсети и шлюз по умолчанию.
- Для управления коммутатором используется один конкретный виртуальный интерфейс коммутатора (SVI).
  - Виртуальному интерфейсу коммутатора назначается IP-адрес коммутатора.
  - По умолчанию управляющий виртуальный интерфейс коммутатора управляется и настраивается через сеть VLAN 1.
  - Управляющий виртуальный интерфейс коммутатора обычно называется сетью управления VLAN.
- В целях безопасности не рекомендуется использовать сеть VLAN 1 в качестве сети управления VLAN.



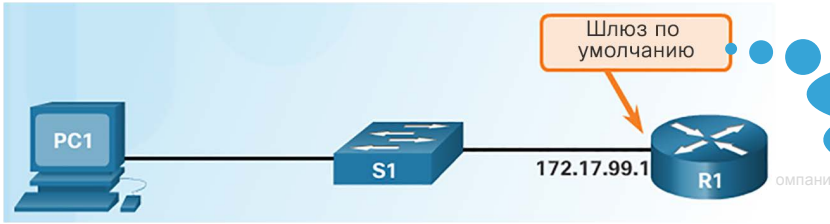
Помните, что консольный порт коммутатора находится на задней панели коммутатора.

Настройка основных параметров доступа для управления коммутатором с помощью IPv4

Команды коммутатора Cisco под управлением ОС IOS

Войдите в режим глобальной настройки.	`S1# configure terminal`
Войдите в режим интерфейсной конфигурации для SVI.	`S1(config)# interface vlan 99`
Настройте IP-адрес интерфейса управления.	`S1(config-if)# ip address 172.17.99.11 255.255.255.0`
Включите интерфейс управления.	`S1(config-if)# no shutdown`
Вернитесь в привилегированный исполнительский режим.	`S1(config-if)# exit`
Настройте шлюз по умолчанию для коммутатора.	`S1(config)# ip default-gateway 172.17.99.1`
Вернитесь в привилегированный исполнительский режим.	`S1(config)# end`
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	`S1# Скопируйте команду running-config startup-config`

Важная концепция



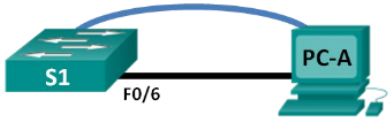
Шлюз по умолчанию — это адрес маршрутизатора. Он используется коммутатором для обмена данными с другими сетями.

Базовая настройка коммутатора

Cisco Networking Academy® Mind Wide Open™

Lab – Configuring Basic Switch Settings

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

Part 4: Manage the MAC Address Table

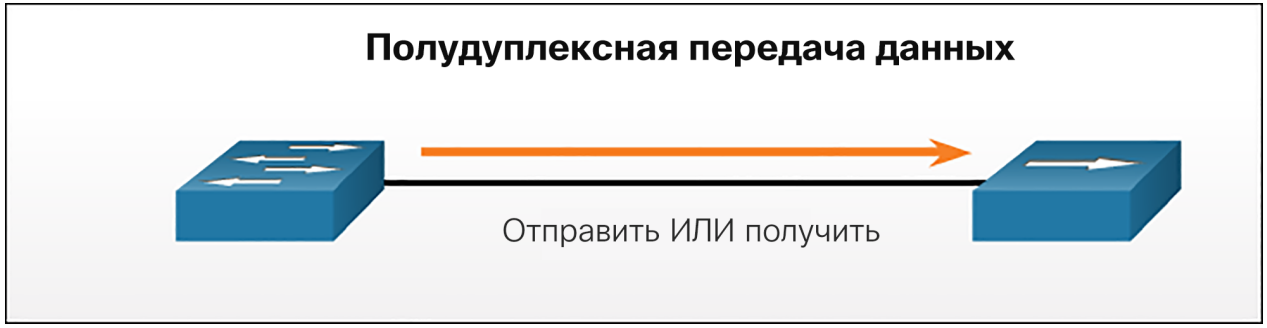
- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.

Дуплексная связь

- Для работы полнодуплексных соединений требуются сетевые интерфейсные платы, поддерживающие Gigabit Ethernet и 10Gb Ethernet.

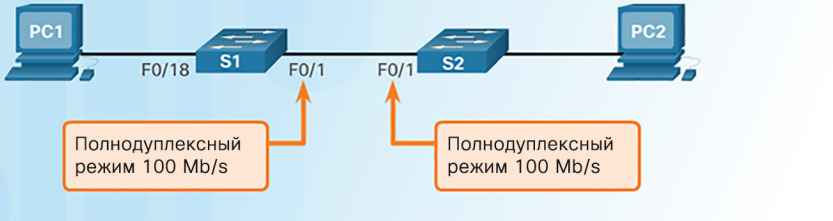
Двусторонняя связь

Однонаправленная связь



Настройка портов коммутатора на физическом уровне

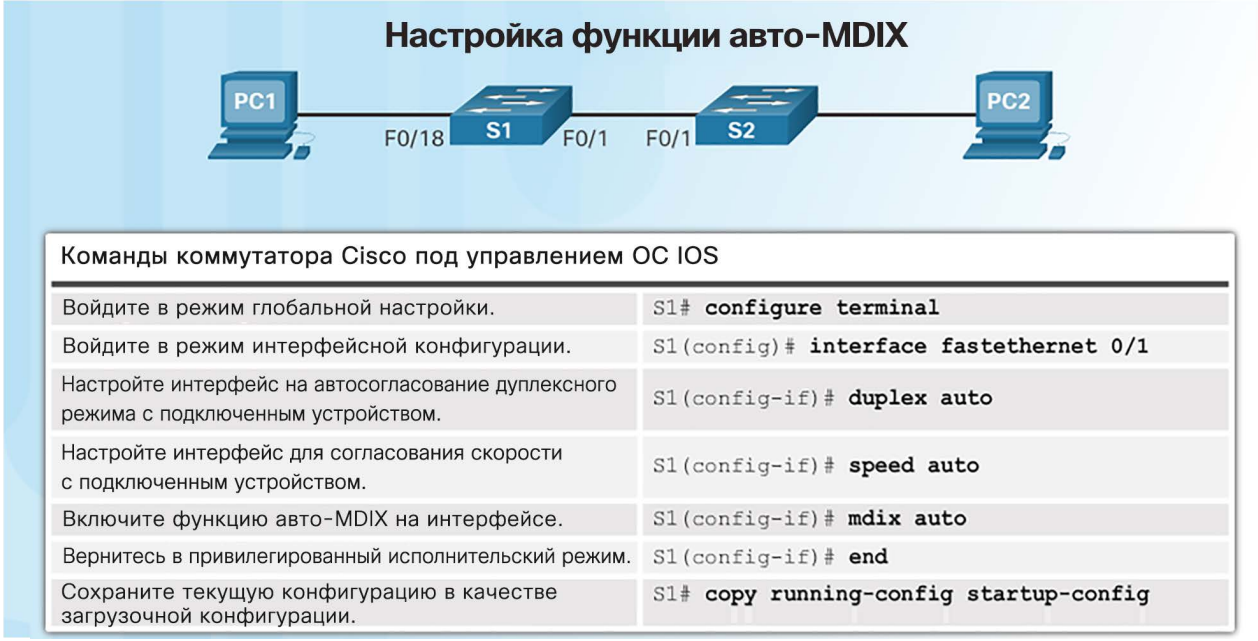
- В некоторых коммутаторах по умолчанию установлена автоматический выбор дуплексного режима и скорости.
- Несоответствие настроек дуплексного режима или скорости может привести к проблемам с подключением.
- Всегда проверяйте настройки скорости и дуплексного режима с помощью команды **show interface** *id_интерфейса*.
- Все волоконно-оптические порты работают на одной скорости и всегда в полнодуплексном режиме.



Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной настройки.	S1# **Настройте терминал**
Войдите в режим интерфейсной конфигурации.	S1(config)# **интерфейс FastEthernet 0/1**
Настройте дуплексный режим интерфейса.	S1(config-if)# **Дуплекс: полный**
Настройте скорость интерфейса.	S1(config-if)# **Скорость 100**
Вернитесь в привилегированный исполнительский режим.	S1(config-if)# **Конец**
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# **Скопируйте команду running-config startup-config**

Функция Auto-MDIX

- В некоторых коммутаторах имеется функция auto-MDIX (автоматический зависящий от среды передачи интерфейс с перекрестным соединением), позволяющая интерфейсу определять требуемый тип кабельного соединения (прямой или с перекрещиванием) и соответствующим образом настраивать подключение.



Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной настройки.	`S1# configure terminal`
Войдите в режим интерфейсной конфигурации.	`S1(config)# interface fastethernet 0/1`
Настройте интерфейс на автосогласование дуплексного режима с подключенным устройством.	`S1(config-if)# duplex auto`
Настройте интерфейс для согласования скорости с подключенным устройством.	`S1(config-if)# speed auto`
Включите функцию авто-MDIX на интерфейсе.	`S1(config-if)# mdix auto`
Вернитесь в привилегированный исполнительский режим.	`S1(config-if)# end`
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	`S1# copy running-config startup-config`

Функция Auto-MDIX (продолжение)

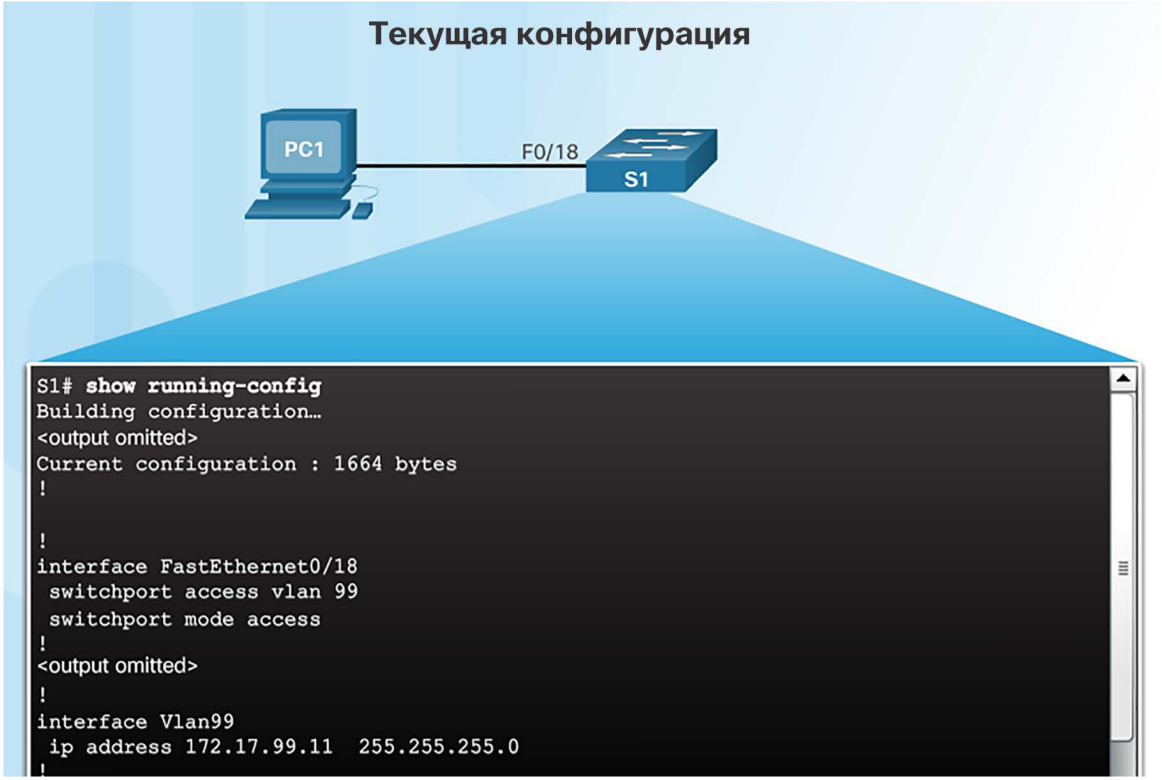
- Для проверки настроек функции auto-MDIX используется команда **show controllers Ethernet-controller**.

Проверка конфигурации портов коммутатора

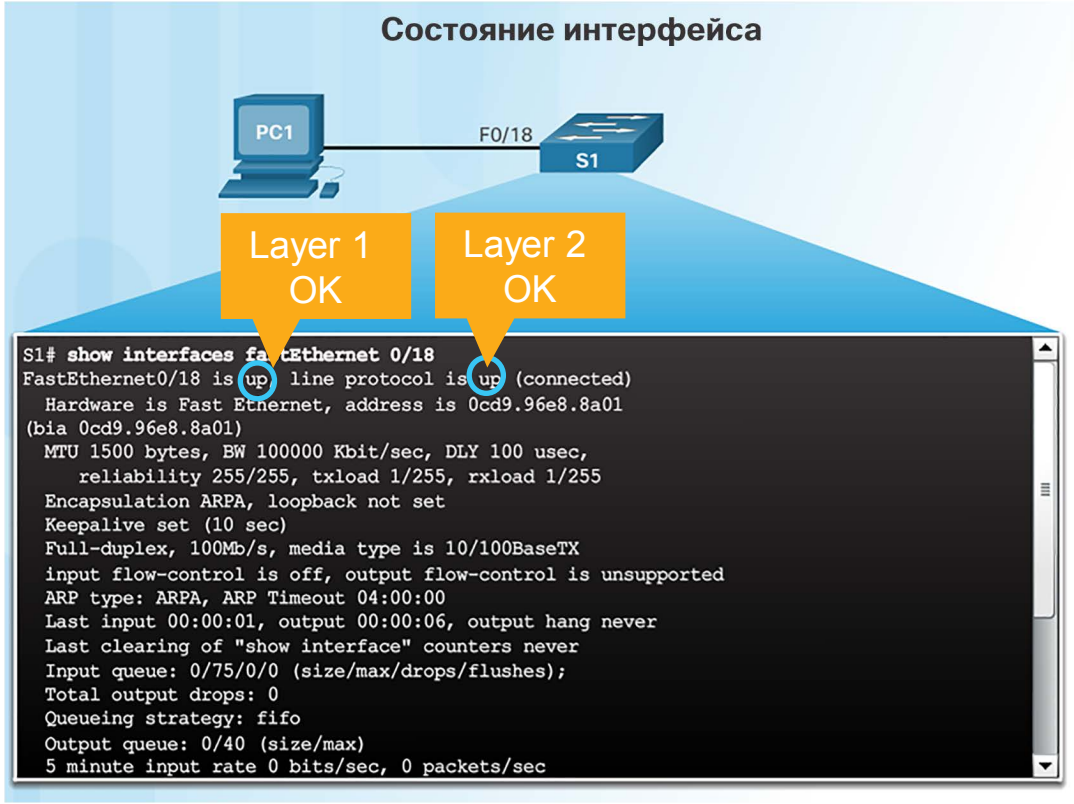
Команды коммутатора Cisco под управлением ОС IOS

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 флеш-системе.	S1# **show flash**
Отобразите состояние системного аппаратного и программного обеспечения.	S1# **show version**
Отобразите историю введенных команд.	S1# **show history**
Отобразите данные IP для интерфейса.	S1# **show ip** [*interface-id*]
Отобразите таблицу MAC-адресов.	S1# **show mac-address-table** ИЛИ S1# **show mac address-table**

Проверка конфигурации портов коммутатора (продолжение)



Проверка конфигурации портов коммутатора (продолжение)



Проблемы на уровне сетевого доступа

- Для обнаружения распространенных проблем среды передачи используется команда **show interfaces**.
- Первый параметр относится к физическому уровню (уровню 1). Он указывает, получает ли интерфейс сигнал обнаружения несущей.
- Второй параметр (состояние протокола) относится к уровню каналов передачи данных. Он указывает, правильно ли настроен протокол канального уровня передачи данных и принимаются ли сообщения keepalive.

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
```

Состояние интерфейса	Состояние протокола линии	Состояние канала
Вкл	Вкл	Рабочий
Выкл	Выкл	Проблемы с интерфейсом

Проблемы на уровне сетевого доступа (продолжение)

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast Ethernet, address is
0022.91c4.0e01 (bia 0022.91c4.0e01)MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 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
<output omitted>
```

Тип ошибки	Описание
Ошибки ввода	Общее количество ошибок. Включает «карликовые» и «гигантские» кадры, отсутствие буфера, CRC, ошибки в кадрах, переполнение и проигнорированные пакеты.
Ошибки типа «карликовый кадр» (Runts)	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.

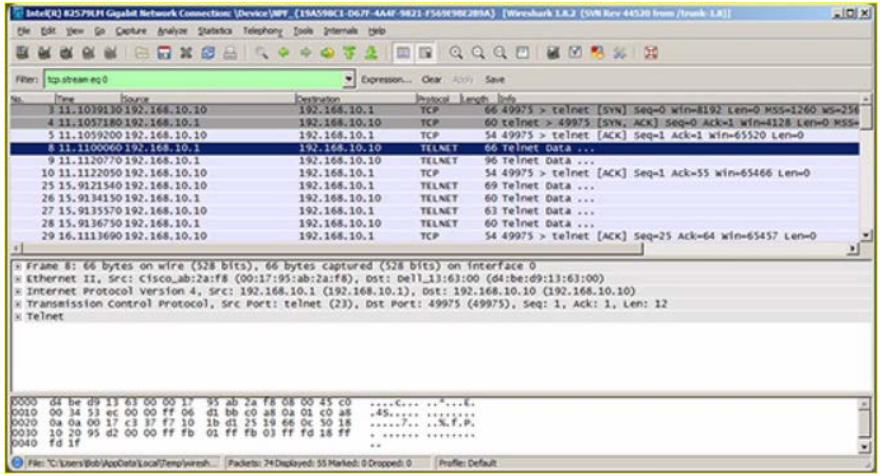
Поиск и устранение неполадок на уровне сетевого доступа

5.2. Безопасность коммутаторов

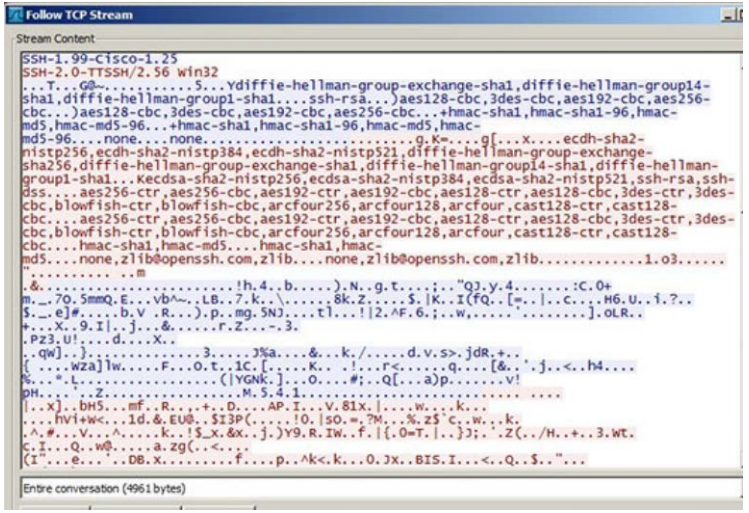
Принцип работы протокола SSH

- Протокол Secure Shell (SSH)
  - Протокол, который является альтернативой Telnet. При работе по протоколу Telnet имя пользователя и пароль, а также данные передаются в виде незащищенного обычного текста.
  - Протокол SSH является более безопасным, так как обеспечивает зашифрованное подключение для управления.

Снимок Telnet, выполненный ПО Wireshark

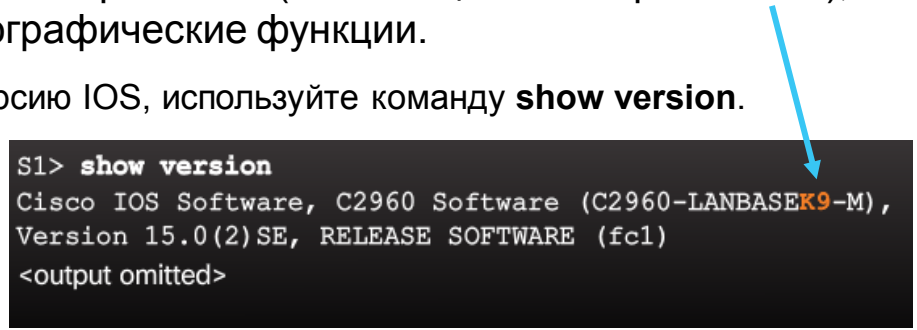


Снимок SSH, выполненный ПО Wireshark



Принцип работы протокола SSH (продолжение)

- Для настройки и использования протокола SSH на коммутаторе должна быть установлена версия IOS (k9 в конце имени файла IOS), в которой имеются криптографические функции.
  - Определить версию IOS, используйте команду **show version**.



Настройка протокола SSH

1. Проверьте поддержку протокола SSH.
2. Задайте имя домена IP.
3. Создайте пары ключей RSA.
4. Настройте аутентификацию пользователя.
5. Настройте каналы vty.
6. Включите SSH версии 2.

Команда, используемая при создании ключей, которую обычно забывают

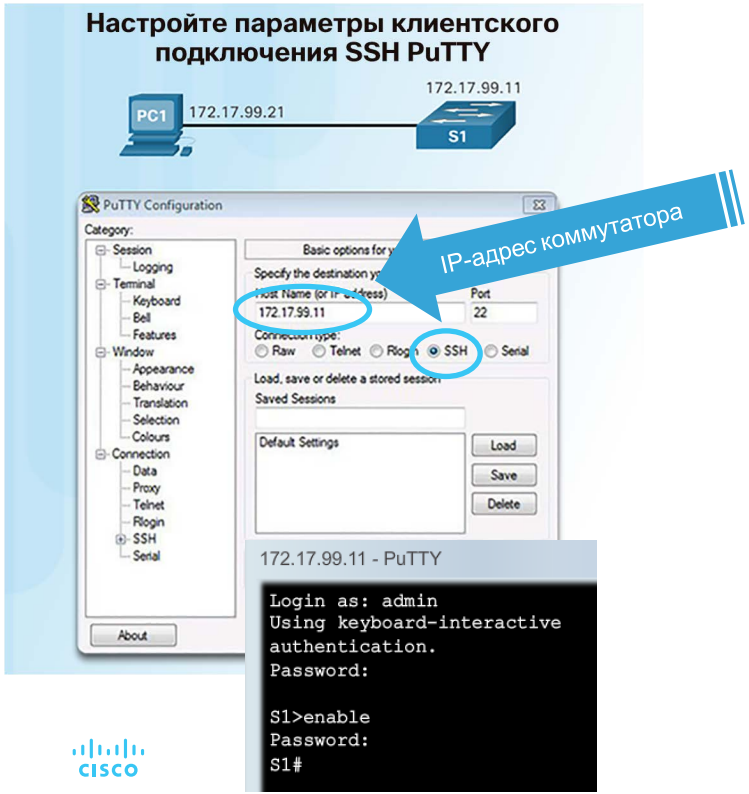
```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

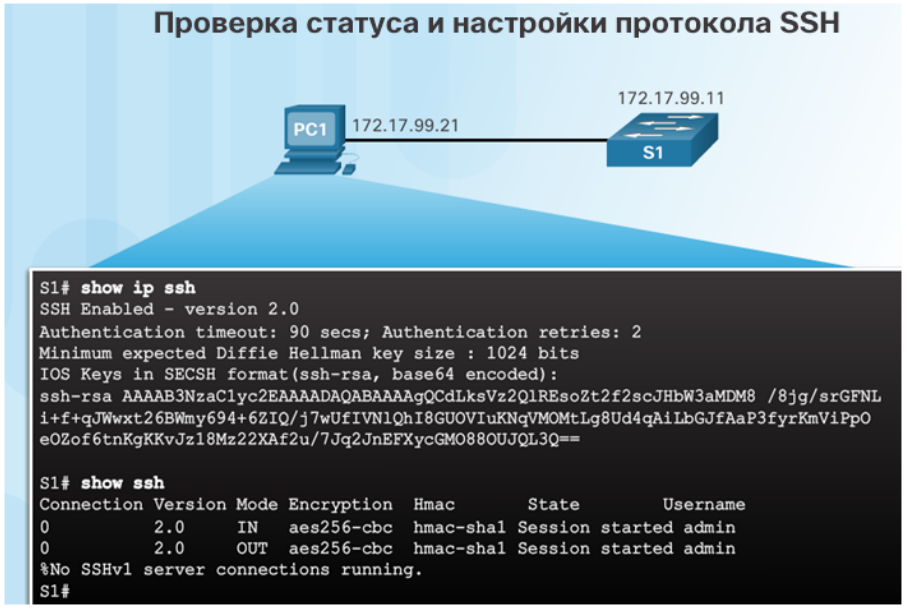
По умолчанию принимается и Telnet, и SSH (transport input all)

Команда `Login local` обеспечивает принудительное использование локальной базы данных для имени пользователя / пароля.

Проверка протокола SSH

- На ПК подключитесь к коммутатору по протоколу SSH.





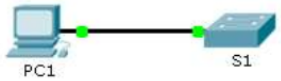
На этом ПК для обмена данными и выполнения команд на коммутаторе используется протокол SSH.

Packet Tracer. Настройка протокола SSH

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Configuring SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objectives

Part 1: Secure Passwords

Part 2: Encrypt Communications

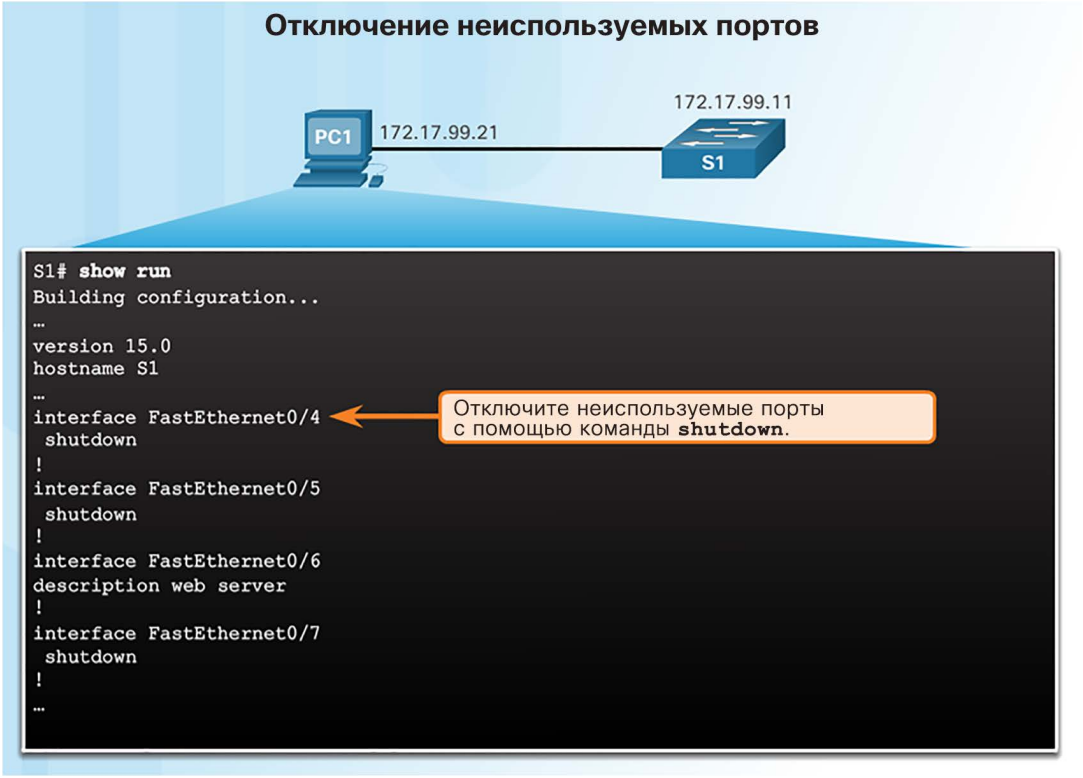
Part 3: Verify SSH Implementation

Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

Защита неиспользуемых портов

С помощью команды **Interface range** можно применить конфигурацию к нескольким портам коммутатора одновременно.



Функция безопасности портов. Принцип работы

- Функция безопасности портов ограничивает количество допустимых MAC-адресов, которым разрешено передавать данные через порт коммутатора.
  - Если для порта включена функция безопасности и неизвестный MAC-адрес отправляет на него данные, коммутатор сообщает об инцидентах, связанных с безопасностью.
  - По умолчанию разрешен 1 безопасный MAC-адрес.
- Для настройки MAC-адресов в рамках функции безопасности портов используются следующие способы.
  - Статические безопасные MAC-адреса — задаются вручную

    switchport port-security mac-address *mac-адрес*
  - Динамические безопасные MAC-адреса — получаются динамически и удаляются при перезапуске коммутатора
  - Закрепленные безопасные MAC-адреса — получаются динамически и добавляются в текущую конфигурацию (которую затем можно сохранить в файле загрузочной конфигурации для постоянного сохранения этих MAC-адресов)

    switchport port-security mac-address sticky *mac-адрес*

Примечание. При отключении получения закрепленных MAC-адресов эти адреса преобразуются в динамические защищенные адреса и удаляются из текущей конфигурации.

Безопасность портов: режимы реагирования на нарушения

- Protect (Защита) — данные, поступающие от неизвестных MAC-адресов, удаляются; коммутатор **НЕ ВЫДАЕТ** уведомление об инциденте безопасности.
- Restrict (Ограничение) — данные, поступающие от неизвестных MAC-адресов, удаляются; коммутатор **ВЫДАЕТ** уведомление об инциденте безопасности, и счетчик нарушений растет.
- Shutdown (Выключение) — (режим по умолчанию) интерфейс отключается из-за возникновения ошибки, а индикатор порта гаснет. Счетчик нарушений увеличивается. Для выхода из состояния отключения после ошибки следует выдать на интерфейсе команду shutdown, а затем команду no shutdown.

Режимы реагирования на нарушения	Пересылает трафик	Передает сообщение SYSLOG	Выводит сообщение об ошибке	Увеличивает счетчик нарушений	Выключает порт
Защита	Нет	Нет	Нет	Нет	Нет
Ограничение	Нет	Да	Нет	Да	Нет
Выключение	Нет	Нет	Нет	Да	Да

Возникновение следующих ситуаций может свидетельствовать об инцидентах, связанных с безопасностью

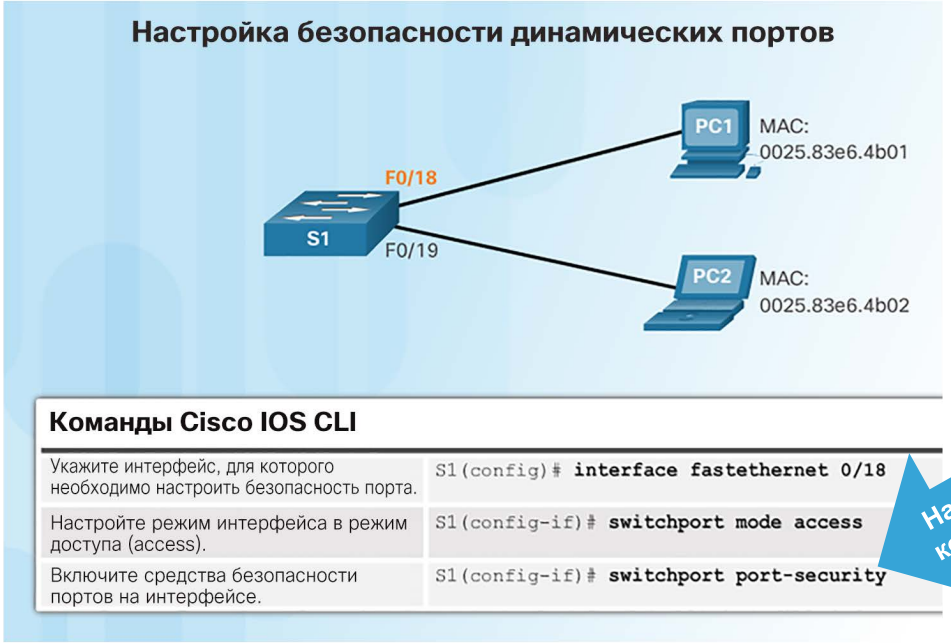
- Рабочая станция с MAC-адресом, которого нет в таблице адресов, пытается получить доступ к интерфейсу, когда таблица заполнена.
- Адрес используется в двух защищенных интерфейсах в рамках одной VLAN.

Безопасность портов: настройка

Функция	Настройка по умолчанию
Функция безопасности портов	Отключена на порте
Максимальное количество защищенных MAC-адресов	1
Режим проверки на нарушение безопасности	Завершение работы. Порт отключается, когда максимальное количество защищенных MAC-адресов отключено.
Получение прикрепленного адреса	Выключено

Безопасность портов: настройка (продолжение)

- Перед настройкой функции безопасности портов переведите порт в режим доступа и с помощью команды настройки интерфейса **switchport port-security** включите функцию безопасности портов на интерфейсе.



Безопасность портов: настройка (продолжение)

Настройка безопасности портов с привязкой к MAC-адресам

Команды Cisco IOS CLI

Укажите интерфейс, для которого необходимо настроить безопасность порта.	`S1(config)# interface fastethernet 0/19`
Задайте максимальное количество безопасных адресов, допустимых для доступа к порту	`S1(config-if)# switchport mode access`
Включите средства безопасности портов на интерфейсе.	`S1(config-if)# switchport port-security`
Задайте максимальное количество безопасных адресов, допустимых для доступа к порту	`S1(config-if)# switchport port-security maximum 10`
Включите получение прикрепленных адресов	`S1(config-if)# switchport port-security mac-address sticky`

Наиболее распространенная ошибка конфигурации — забыть эту команду!

Безопасность портов: проверка

- Команда **show port-security interface** позволяет узнать максимальное количество MAC-адресов, разрешенных на конкретном порту, а также сколько из этих адресов было получено динамически с использованием ключевого слова sticky.

Динамически

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

С использованием sticky

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```

Безопасность портов: проверка (продолжение)

- Чтобы просмотреть полученные динамически MAC-адреса, которые были добавлены в конфигурацию, используйте команду **show running-config**.

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

- Команда **show port-security address** показывает, как были получены MAC-адреса на конкретном порту.

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type             Ports    Remaining Age
                                                     (mins)
----    -----------       ----             -----    -------------
1       0025.83e6.4b01    SecureDynamic    Fa0/18       -
1       0025.83e6.4b02    SecureSticky     Fa0/19       -
------------------------------------------------------------
```

Порты в состоянии отключения после ошибки

- При инцидентах, связанных с безопасностью порта, отображаются сообщения консоли коммутатора. Обратите внимание, что состояние канала порта изменяется на "down" (отключение).

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Порты в состоянии отключения после ошибки (продолжение)

- Проверьте состояние порта и настройки безопасности порта.

```
S1# show interface fa0/18 status
Port Name  Status        Vlan  Duplex  Speed   Type
Fa0/18     err-disabled  1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

- Не включайте порт, пока угроза безопасности не будет исследована и устранена.
- Обратите внимание, что необходимо сначала выключить порт, а затем выполнить команду **no shutdown**, чтобы этот порт можно было снова использовать после произошедшего инцидента, связанного с безопасностью.

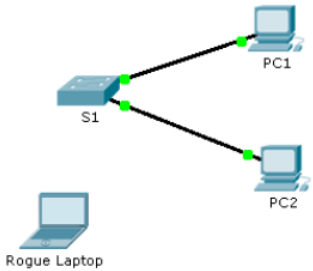
```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
 administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 FastEthernet0/18, changed state to up
```

Packet Tracer. Настройка функции безопасности портов коммутатора

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

Background

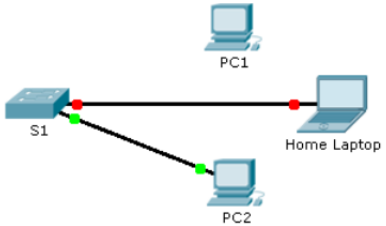
In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Packet Tracer. Поиск и устранение неполадок функции информационной безопасности портов коммутатора

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Troubleshooting Switch Port Security

Topology



Scenario

The employee who normally uses PC1 brought his laptop from home, disconnected PC1 and connected the laptop to the telecommunication outlet. After reminding him of the security policy that does not allow personal devices on the network, you now must reconnect PC1 and re-enable the port.

Requirements

- Disconnect **Home Laptop** and reconnect **PC1** to the appropriate port.
  - When **PC1** was reconnected to the switch port, did the port status change?
  - Enter the command to view the port status. What is the state of the port?
  - Which port security command enabled this feature?
- Enable the port using the necessary command.
- Verify connectivity. **PC1** should now be able to ping **PC2**.

Packet Tracer. Настройка функций безопасности коммутатора

Cisco Networking Academy® Mind Wide Open™

Lab – Configuring Switch Security Features

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

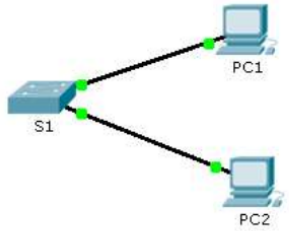
5.3. Обзор главы

Packet Tracer. Отработка комплексных практических навыков

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0

Scenario

The network administrator asked you to configure a new switch. In this activity, you will use a list of requirements to configure the new switch with initial settings, SSH, and port security.

Глава 5. Настройка коммутатора

- Настройка базовых параметров коммутации в соответствии с сетевыми требованиями.
- Настройте коммутатор с применением практических рекомендаций по обеспечению информационной безопасности в сетях предприятий малого и среднего бизнеса.

Новые термины и команды

- POST
- Начальный загрузчик
- **boot system** (команда)
- **show boot** (команда)
- switch: (приглашение к вводу команды)
- Кнопка переключения режима
- Индикатор системы
- Индикатор порта
- SVI
- VLAN
- Сеть VLAN управления (Management VLAN)
- **interface vlan** (команда)
- **vlan** (команда)
- **name** (команда)
- Полнодуплексный режим
- Полудуплексный режим
- Скорость порта
- **duplex** (команда)
- **speed** (команда)
- **mdix** (команда)
- **show interfaces** (команда)
- Конфигурация SSH
- **ip domain-name** (команда)
- **crypto key generate rsa** (команда)
- **transport input local** (команда)
- **username secret** (команда)
- **ip ssh version 2** (команда)
- **login local** (команда)
- **show ip ssh** (команда)
- Неиспользуемые порты
- Функция безопасности портов
- **switchport mode access** (команда)
- **switchport port-security** (команда)
- **switchport port-security maximum** (команда)
- **switchport port-security mac-address sticky** (команда)
- **show port-security interface** (команда)
- **show port-security address** (команда)


CISCO