

# ???? ?? ?????? ? ???????????? Cisco

## ?????? ?????????????? ? ?????????????

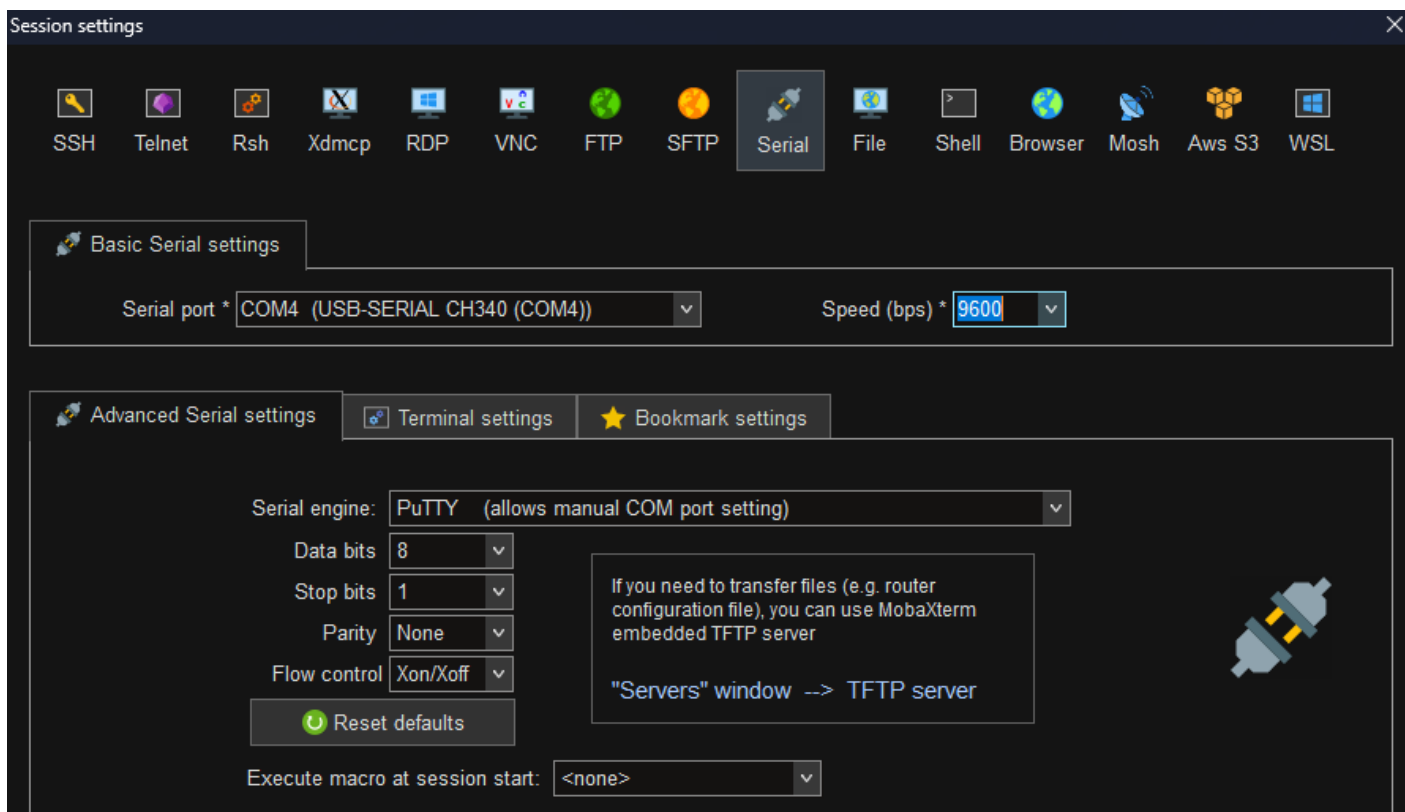
Для базовой настройки коммутатора Cisco 2960 вам понадобится:

- сам коммутатор;
- кабель RJ-45-RS-232 или USB к RJ45 и RS232;
- компьютер с COM-портом или переходник USB 2.0-RS232 при его отсутствии;
- кабель питания CEE 7/7.

После того, как вы подключили коммутатор к питанию и он включился, необходимо подключить консольный порт к самому коммутатору и к компьютеру.

Для входа в терминал коммутатора необходимо использовать утилиты вроде Putty или MobaXTerm.

Подключение к коммутатору необходимо выполнять по COM порту со следующими параметрами:



???????????????? ???? ?????

1. Когда вы подключаетесь к коммутатору в первый раз и установочный мастер предлагает пошаговую настройку (Continue with configuration dialog? [yes/no]), необходимо отказаться от нее.

2. После этого загрузится пользовательский режим ввода «Switch>» — перейдите в привилегированный режим:

```
Switch>enable
```

```
Password: (нажмите «Enter», пароль по умолчанию отсутствует)
```

```
Switch# (режим привилегированного доступа обозначается символом #)
```

3. Измените имя коммутатора. Для этого нужно активировать режим глобальной конфигурации, что позволит настраивать конфигурацию всего коммутатора:

Если в сети есть много коммутаторов, то уникальное имя должен иметь каждый из них. В дальнейшем это поможет определить, что конфигурация реализуется именно на том устройстве, что нужно. Длинные имена использовать не рекомендуется, лучше выбирать короткие.

```
Switch# configure terminal
Switch(config)# hostname
Switch00 (новое имя – Switch00)
Switch00(config)#
```

#### 4. Задайте пароль для привилегированного режима:

```
Switch00(config)# enable secret <ваш пароль>
Switch00(config)# service password-encryption (добавляем сохранение паролей в зашифрованном виде)
```

#### 5. **Рекомендация:** запретите несанкционированный поиск в DNS:

При вводе неправильной команды коммутатор не будет искать доменное имя

```
Switch00(config)# no ip domain-lookup
Switch00(config)#
```

#### 6. Установите IP-адрес для порта управления коммутатором:

```
Switch00(config)# interface fa0/0
Switch00(config-if)# no shutdown
Switch00(config-if)# ip address 192.168.0.1 255.255.255.0 (На порт fa0/0 установили адрес 192.168.0.1 255.255.255.0)
Switch00(config-if)# exit
Switch00(config)#
```

#### 7. Установите пароль для консольного подключения:

```
Switch00(config)# line console 0
Switch00(config-line)# password <ваш пароль>
Switch00(config-line)# login
Switch00(config-line)# exit
```

**Базовая настройка коммутатора Cisco 2960 на этом завершается.**

?????????? VLAN

?????????? VLAN

Настройка Virtual LANs (VLANs) позволяет создавать виртуальные сегменты сети и логически разделять трафик между ними. Рассмотрим, что нужно сделать для установки VLAN.

1. Перейдите в режим глобальной конфигурации:

```
Switch00# configure terminal
Switch00(config)#
```

2. Создайте VLAN, например VLAN 10 с именем:

```
Switch00(config)# vlan 10
Switch00(config-vlan)# name Platform01
Switch00(config-vlan)# exit
```

3. Назначьте порты VLAN:

```
Switch00(config)# interface <т_и> <н_и> (например, fa0/1)
Switch00(config-if)# switchport mode access
Switch00(config-if)# switchport access vlan 10
Switch00(config-if)# exit
```

*Назначаем порт на VLAN 10. <ти> — тип интерфейса, например FastEthernet или GigabitEthernet, <н\_и> — номер интерфейса, который вы хотите настроить, например 0/1.*

4. После завершения настройки не забудьте сохранить изменения:

```
Switch00# copy running-config startup-config
```

?????????? Access ? Trunk ?????? ?? ??????????????

Некоторые обозначения:

access port – это порт, который принадлежит к одному VLAN, и может передавать нетегированный информационный трафик;

trunk port – это коммутационный порт, посредством которого может передаваться тегированный трафик от одного либо нескольких VLAN.

Коммутаторы Cisco ранних версий работали с двумя протоколами: 802.1Q, ISL. Второй из них относится к проприетарному протоколу, который применяется в коммутационных платформах Cisco. Этот протокол позволяет инкапсулировать фрейм

с целью передачи данных о причастности к тому или иному VLAN. Современные модели этот протокол не поддерживают, а работают только с 802.1Q.

Для назначения коммутационного порта доступа в VLAN 10 нужно написать следующие команды:

```
Switch00(config)# interface fa0/1
Switch00(config-if)# switchport mode access
Switch00(config-if)# switchport access vlan 10
```

Настройка диапазона коммутационных портов с fa0/4 до fa0/5 выполняется следующим образом: `sw1(config)# interface range fa0/4 - 5`

Чтобы иметь возможность передачи трафика от нескольких VLAN посредством одного порта, его следует перевести в режим trunk. Конкретные режимы интерфейса (режим умолчания отличаются для разных моделей):

- auto – это автоматический режим порта, из которого переход в режим trunk возможен только в том случае, если порт на другом конце связи будет в режиме desirable или on;
- desirable – это режим, из которого порт может перейти к режиму trunk; в этом состоянии он периодически посылает DTP-кадры к другому порту, запрашивая его перейти в режим trunk; этот режим будет установлен, если другой порт находится в одном из трех режимов: auto, desirable или on;
- trunk – в этом случае порт постоянно пребывает в состоянии trunk, даже если другой порт не может поддерживать такой же режим;
- nonegotiate – это режим, с которого порт готов выполнить переход к режиму trunk; он не выполняет передачу DTP-кадров к другому порту. Этот режим предусмотрен для исключения конфликтных ситуаций с другим оборудованием (не бренда Cisco). В этом случае коммутационное устройство на другом конце связи должно быть настроено в ручном режиме для использования режима trunk.

По умолчанию для режима trunk разрешаются все VLAN. Чтобы через любой из поддерживаемых VLAN выполнялась передача данных, он должен быть активным. В активную фазу он переходит тогда, когда его создали на коммутаторе и один из его портов находится в режиме up/up.

VLAN создается на коммутаторе посредством команды `vlan`. Также он может формироваться автоматически на коммутаторе, когда к нему добавляются интерфейсы в режиме access.

Для создания статического trunk нужно порта нужно написать следующие команды:

```
Switch00(config)# interface fa0/22
Switch00(config-if)# switchport trunk encapsulation dot1q
```

```
Switch00(config-if)# switchport mode trunk
```

Изначально, по умолчанию, в trunk разрешаются все VLAN. Также можно создать ограничение перечня VLAN, которые можно передавать через тот или иной trunk. Чтобы указать список разрешенных VLAN для порта fa0/22 нужно выполнить:

```
Switch00(config)# interface fa0/22  
Switch00(config-if)# switchport trunk allowed vlan 10
```

## ???????? SPAN

### ?????????? ?? ????????? SPAN

- Для источников SPAN вы можете отслеживать трафик для одного порта или VLAN, а также для серии или диапазона портов или VLAN для каждого сеанса. Совмещать порты-источники и VLAN-источники в одном сеансе SPAN невозможно.
- Порт назначения не может быть портом источника; порт источника не может быть портом назначения.
- Невозможно иметь два сеанса SPAN, использующих один и тот же порт назначения.
- При настройке порта коммутатора в качестве порта назначения SPAN он больше не является обычным портом коммутатора; через порт назначения SPAN проходит только отслеживаемый трафик.
- Ввод команд конфигурации SPAN не удаляет ранее настроенные параметры SPAN. Для удаления настроенных параметров SPAN необходимо ввести глобальную команду конфигурации **no monitor session** { session\_number | all | local | remote }.
- Для локального SPAN исходящие пакеты через порт назначения SPAN содержат исходные заголовки инкапсуляции — без тегов или IEEE 802.1Q — если указаны ключевые слова репликации инкапсуляции . Если ключевые слова не указаны, пакеты отправляются в исходном формате. Для портов назначения RSPAN исходящие пакеты не тегируются.
- Вы можете настроить отключенный порт как порт источника или назначения, но функция SPAN не запустится, пока не будут включены порт назначения и хотя бы один порт источника или исходная VLAN.
- Вы можете ограничить SPAN-трафик определенными VLAN с помощью ключевого слова **filter vlan** . Если отслеживается транк-порт, отслеживается только трафик в VLAN, указанных этим ключевым словом. По умолчанию на транк-порту отслеживаются все VLAN.
- В одном сеансе SPAN нельзя смешивать исходные VLAN и фильтрующие VLAN.

### ????????? ?????????? ?????? SPAN

Войдите в привилегированный режим EXEC и выполните следующие действия, чтобы создать сеанс SPAN и указать исходные (контролируемые) порты или VLAN, а также порты назначения (контролируемые):

|       | Команда                                                                                                                                                       | Цель                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Шаг 1 | <b>configure terminal</b>                                                                                                                                     | Войдите в режим глобальной конфигурации.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Шаг 2 | <b>no monitor session</b> { session_number   <b>all</b>   <b>local</b>   <b>remote</b> }                                                                      | <p>Удалите любую существующую конфигурацию SPAN для сеанса.</p> <p>Для <i>session_number</i> диапазон составляет от 1 до 66. Укажите <b>all</b> , чтобы удалить все сеансы SPAN, <b>local</b> , чтобы удалить все локальные сеансы, или <b>remote</b>, чтобы удалить все удаленные сеансы SPAN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Шаг 3 | <b>monitor session</b> session_number <b>source</b> { <b>interface</b> interface-id   <b>vlan</b> vlan-id } [ ,   - ] [ <b>both</b>   <b>rx</b>   <b>tx</b> ] | <p>Укажите сеанс SPAN и порт источника (контролируемый порт).</p> <p>Для <i>session_number</i> диапазон составляет от 1 до 66. Для <i>interface-id</i> укажите исходный порт или исходную VLAN для мониторинга.</p> <ul style="list-style-type: none"> <li>Для параметра <i>source interface-id</i> укажите порт источника для мониторинга. Допустимые интерфейсы включают физические интерфейсы и логические интерфейсы порт-канал ( <b>port-channel</b> <i>port-channel-number</i> ) . Допустимые номера порт-каналов — от 1 до 6.</li> <li>Для <i>vlan-id</i> укажите исходную VLAN для мониторинга. Диапазон значений — от 1 до 4094 (исключая RSPAN VLAN).</li> </ul> <p><b>Примечание.</b> Один сеанс может включать несколько источников (портов или VLAN), определенных в серии команд, но вы не можете объединить исходные порты и исходные VLAN в одном сеансе. (Необязательно) [ ,   - ] Укажите серию или диапазон интерфейсов. Введите пробел до и после запятой; введите пробел до и после дефиса. (Необязательно) Укажите направление трафика для отслеживания. Если направление трафика не указано, SPAN отслеживает как исходящий, так и входящий трафик.</p> <ul style="list-style-type: none"> <li><b>both</b> — отслеживать как входящий, так и исходящий трафик. Этот вариант используется по умолчанию.</li> <li><b>rx</b> — Мониторинг полученного трафика.</li> <li><b>tx</b> —Мониторинг отправленного трафика.</li> </ul> <p><b>Примечание.</b> Вы можете использовать команду <b>monitor session_number source</b> несколько раз для настройки нескольких исходных портов.</p> |

|          |                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Шаг<br>4 | <b>monitor session</b> session_number <b>destination</b> {<br><b>interface</b> interface-id [ ,   - ] [ <b>encapsulation</b> {<br><b>dot1q</b>   <b>replicate</b> }]} | <p>Укажите сеанс SPAN и порт назначения (порт мониторинга).</p> <p>Для <i>session_number</i> укажите номер сеанса, введенный на шаге 3.</p> <p><b>Примечание.</b> Для локального SPAN необходимо использовать один и тот же номер сеанса для исходного и целевого интерфейсов.</p> <p>Для <i>interface-id</i> укажите порт назначения. Интерфейс назначения должен быть физическим портом; он не может быть EtherChannel или VLAN.</p> <p>(Необязательно) [ ,   - ] Укажите серию или диапазон интерфейсов. Введите пробел до и после запятой; введите пробел до и после дефиса.</p> <p>(Необязательно) Введите <b>encapsulation dot1q</b>, чтобы указать, что интерфейс назначения использует метод инкапсуляции IEEE 802.1Q.</p> <p>(Необязательно) Введите <b>encapsulation replicate</b>, чтобы указать, что целевой интерфейс копирует метод инкапсуляции исходного интерфейса. Если этот параметр не выбран, по умолчанию пакеты отправляются в исходном формате (без тегов).</p> <p><b>Примечание.</b> Вы можете использовать команду <b>monitor session session_number destination</b> несколько раз для настройки нескольких портов назначения.</p> |
| Шаг<br>5 | <b>end</b>                                                                                                                                                            | Вернитесь в привилегированный режим EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Шаг<br>6 | <b>show monitor</b> [session session_number]<br><br><b>show running-config</b>                                                                                        | Проверьте конфигурацию.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Шаг<br>7 | <b>копировать running-config startup-config</b>                                                                                                                       | (Необязательно) Сохраните конфигурацию в файле конфигурации.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Пример настройки SPAN на коммутаторе для VLAN 10:

```
Switch00>enable
Switch00#conf t
Switch00(config)#no monitor session all
Switch00(config)#monitor session 1 source vlan 10 both
Switch00(config)#monitor session 1 destination interface f0/24 encapsulation replicate
Switch00(config)#end
Switch00#wr
```

# ?????????? SNMP

Настройка **SNMP** на коммутаторах и маршрутизаторах Cisco позволит вам мониторить состояние девайсов и сохранить свои нервы/время, в случаях, когда они начинают сбоить (игра на опережение). В целом, выглядит это так: сетевое устройство будет отправлять информацию о CPU, памяти, температуре, I/O и прочих на **NMS (Network Management System)** сервер.

Чтобы настроить SNMP на коммутаторе необходимо выполнить следующие команды:

```
Switch00>enable
Switch00#conf t
Switch00(config)#snmp-server
Switch00(config)#snmp-server community public R0 (только read-only права для публичной строки
сообщества)
Switch00(config)#snmp-server community private RW (read-write права для приватной строки
сообщества)
Switch00(config)#snmp-server enable traps (Включение SNMP trap)
Switch00(config)#snmp-server host 192.168.0.100 public (здесь может быть любой адрес NMS
сервера)
Switch00(config)#exit
Switch00#write memory
```

## ????????? ?????????? ???????? SSH/Telnet

### ????????? Telnet

```
Switch00# clock set 18:32:00 08 January 2024 (установка текущего времени и даты)
Switch00# conf t
Switch00(config)# line vty 0 2 (переход к режиму конф-и терминальных линий)
Switch00(config-line)# transport input telnet (подключение только по telnet)
Switch00(config-line)# password <ваш пароль> (активируем пароль для telnet сессий)
Switch00(config-line)# login local (Вход по имени пользователя и паролю из локальной базы
данных)
Switch00(config-line)# logging synchronous (запрещает вывод каких-либо консольных сообщений,
которые в свою очередь могут прервать ввод команд в консольном режиме)
Switch00(config-line)# end
Switch00# copy running-config startup-config (сохраняем настройки)
```

Учитывая, что информация при telnet-соединениях передается в открытом виде, рекомендуется использовать SSH-соединения, которые обеспечат шифрование трафика.

## ???????? SSH

```
Switch00# clock set 18:32:00 08 January 2024 (установка текущего времени и даты)
Switch00# conf t
Switch00(config)# ip domain name google.com (задаем домен, если его нет пишется любой)
Switch00(config)# crypto key generate rsa (генерируем RSA-ключа под ssh)
Switch00(config)# ip ssh version 2 (указываем версию SSH-протокола)
Switch00(config)# ip ssh authentication-retries 3 (устанавливаем допустимое число попыток
подключения по SSH)
Switch00(config)# service password-encryption (добавляем сохранение паролей в зашифрованном
виде )
Switch00(config)# line vty 0 2 (переход к режиму конф-и терминальных линий)
Switch00(config-line)# transport input ssh (подключение только по SSH)
Switch00(config-line)# exec timeout 20 0 (активируем автоматическую смерть SSH-сессии через 20
минут)
Switch00(config-line)# end
Switch00# copy running-config startup-config (сохраняем настройки)
```

Для того, чтобы не ограничиваться одним протоколом и использовать как SSH так и Telnet, можно заменить команду `transport input ssh` на `transport input all`

Revision #4

Created 22 July 2025 17:15:24

Updated 17 November 2025 09:11:31 by Sergey Malyugin