Практика

# **В Wireshark захватить установку, завершение и сброс TCP-соединения, проанализировать трафик и объяснить происходящие процессы.**

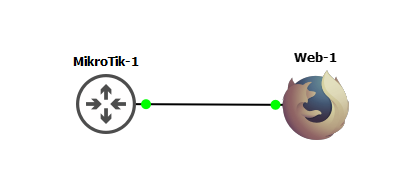
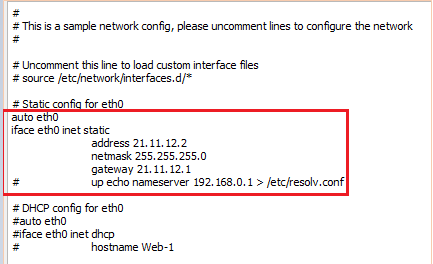


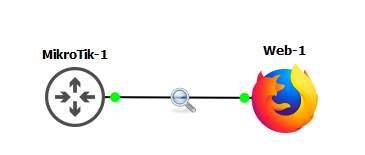
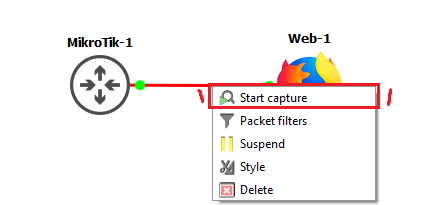
Схема сети



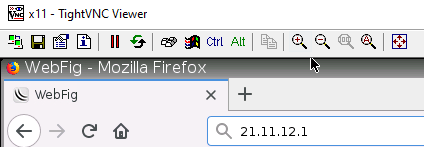
Настройка mikrotik



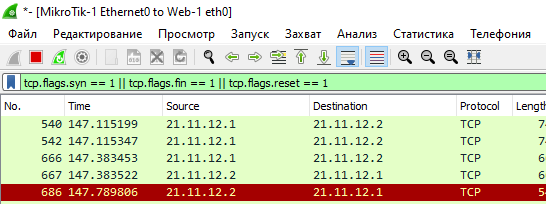
Настройка Web-1 через конфиг



Начинаем захват трафика

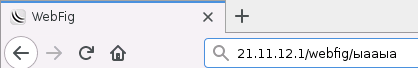


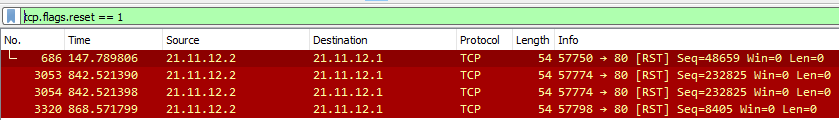
Заходим в Web1 нажимая дважды на него и вводим в поисковую строку ip микротика который задавали ранее



Пишем в фильтры tcp.flags.syn == 1 || tcp.flags.fin == 1 || tcp.flags.reset == 1 и теперь видим только tcp пакеты с флагами syn, fin, reset. Если например нужны tcp пакеты ***ТОЛЬКО с флагом*** syn пишите tcp.flags.syn == 1.

*!!!Чтобы появились пакеты reset нужно в поисковой строке ввести любые символы после «/webfig/»!!!*





*Немного теории чтобы объяснить, что к чему:*

**SYN (Synchronize)**

Цель: Флаг SYN используется в начале установки TCP-соединения между двумя устройствами.

Как это работает: Одно устройство отправляет пакет с установленным флагом SYN другому устройству. Это сообщает другому устройству о желании начать обмен данными и установить соединение.

Результат: Устройство, получившее пакет с флагом SYN, отправляет ответный пакет с установленными флагами SYN и ACK (если оно готово к установлению соединения). Это часть процесса "трехступенчатого рукопожатия", где устройства соглашаются на параметры соединения и синхронизируют начальные порядковые номера для передачи данных.

**FIN (Finish)**

Цель: Флаг FIN используется для закрытия TCP-соединения между устройствами.

Как это работает: Когда одно из устройств закончило отправку данных и хочет завершить соединение, оно отправляет пакет с установленным флагом FIN. Это сообщает другому устройству, что оно заканчивает передачу данных.

Результат: Получив пакет с установленным флагом FIN, второе устройство отправляет подтверждение ACK и может также отправить свой собственный пакет с установленным FIN, чтобы завершить соединение.

**RST (Reset)**

Цель: Флаг RST используется для принудительного прерывания соединения.

Как это работает: Если происходит что-то непредвиденное или ошибочное, устройство может отправить пакет с флагом RST, чтобы немедленно прервать соединение.

Результат: Это приводит к мгновенному завершению соединения без необходимости завершающего "рукопожатия". RST обычно используется для устранения ошибок или для принудительного завершения соединения.

Удачи! ♥

# **В Wireshark захватить ARP-запрос, ARP-ответ и самопроизвольный ARP, проанализировать трафик и объяснить происходящие процессы.**

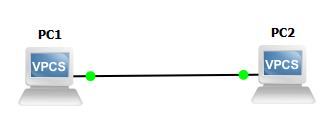


Схема сети

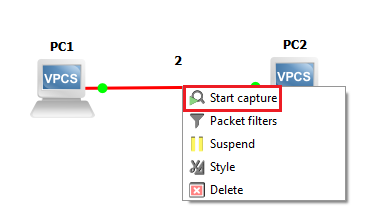




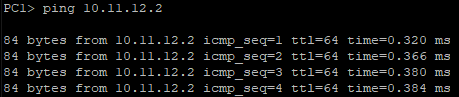
Задаем ip на обоих PC

*! Обязательно пропишите Save на обоих компах!*

**

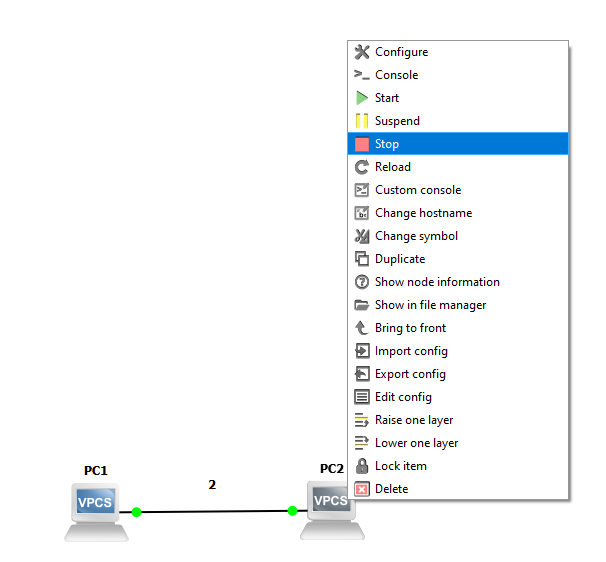


Нажимаем Start capture и начинаем захват трафика

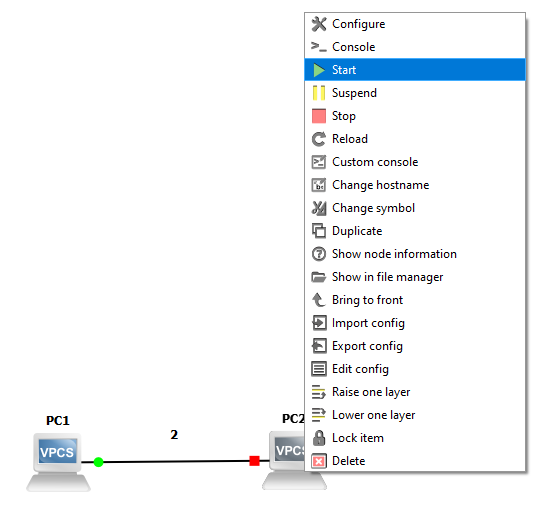


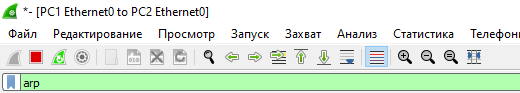
Для просмотра arp запроса и arp ответа нужно выполнить команду ping указав ip другого pc

Затем для того чтобы также в wireshark появились самопроизвольные arp перезапустите один из пк (при перезапуске первого у меня почему то вылетал wireshark так что я перезапустил второй)

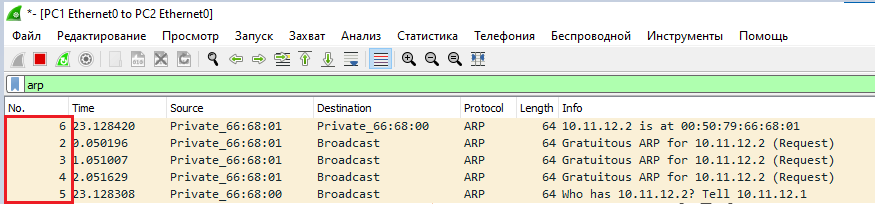


Затем включите его





Заходим в Wireshark и фильтруем по arp написав в строку фильтра «arp»



Сейчас будет объяснение по номерам пакетов они указаны слева выделены красным цветом. Arp-запрос: No 5; Arp-ответ: No 6, Arp-самопроизвольный: No 2,3,4.

*Немного теории чтобы объяснить, что к чему:*

**ARP-запросы**

ARP-запрос (ARP Request): Когда один из ваших ПК (назовем его ПК1) пытается связаться с другим ПК (ПК2) в той же локальной сети, но не знает его MAC-адрес, ПК1 отправляет ARP-запрос. Этот запрос содержит вопрос вроде "Кто имеет этот IP-адрес? Пожалуйста, отправьте свой MAC-адрес". Этот запрос отправляется широковещательно, то есть он достигает всех устройств в локальной сети.

**ARP-ответ (ARP Reply):** ПК2, который распознает свой IP-адрес в ARP-запросе, отвечает на него, отправляя ARP-ответ непосредственно ПК1. В этом ответе указывается MAC-адрес ПК2. После получения этого ответа, ПК1 может сохранить соответствие IP-адреса и MAC-адреса ПК2 в своей ARP-таблице для будущего использования.

**Самопроизвольные ARP-запросы (Gratuitous ARP)**

Самопроизвольный ARP-запрос: Это особый тип ARP-запроса, который отправляется устройством (например, ПК2) широковещательно по сети, но в нем указывается его собственный IP-адрес. Основная цель этого запроса – уведомить другие устройства в сети о своем IP-адресе и MAC-адресе. Это может быть полезно в нескольких случаях:

При запуске устройства для обновления ARP-таблиц других устройств в сети. (Как раз это и является причиной в нашем случае мы перезапускаем один из компов что и генерирует самопроизвольный arp)

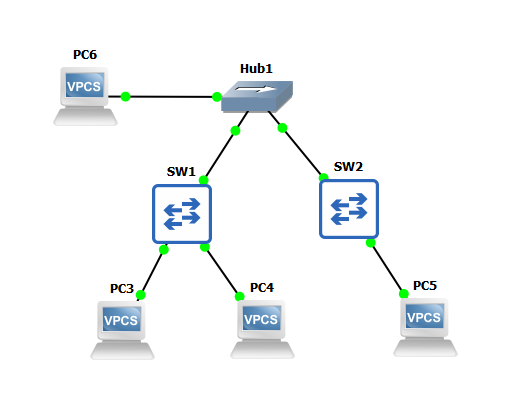
Для проверки, не используется ли IP-адрес другим устройством (для предотвращения конфликта адресов).

Для обновления информации в ARP-таблицах других устройств после изменения IP-адреса или сетевых настроек.

Удачи! ♥

1. Настроить сеть, состоящую из N компьютеров, M коммутаторов и концентратора. Сеть - A.B.C.D/E. На ПК назначить адреса (далее перечислены, какие). Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 4 компьютера (N=4), 2 коммутатора (M=2) и 1 концентратор.*



Cхема сети



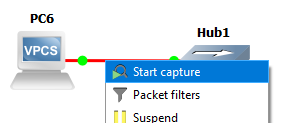


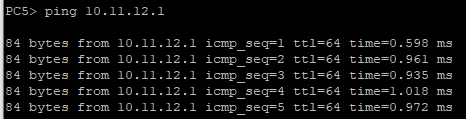




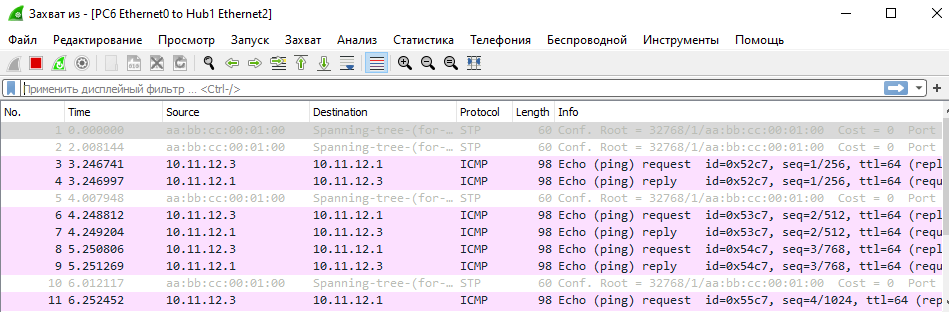
Задаем ip на все PC

Для того чтобы продемонстрировать работу hub тесть концертатратора нужно поставить захват трафика на любой связи которая напрямую подключена к hub





Проверка доступности с PC3 на PC5 (надо пингануть по такому ip чтобы пакет обязательно проходил через hub)



Далее показываем что hub рассылает пакеты всем независимо от того кому они адресованы

*Немного теории чтобы объяснить, что к чему:*

Концентратор (Hub):

Работа устройства:

* Концентратор работает на физическом уровне модели OSI (Уровень 1).
* Он передает входящий сигнал всем портам, кроме того, с которого сигнал пришел.

Характеристики:

* Концентратор не различает устройства в сети и отправляет данные всем подключенным устройствам.
* Пропускная способность сети делится между всеми подключенными устройствами.
* Повышенный риск коллизий, так как все устройства делят один и тот же коммуникационный канал.

*Примечание: до устройств, которые подключены только к коммутаторам трафик от концертатратора доходить не будет (если он конечно им не адресован) так как коммутатор фильтрует его и отправляет конкретным устройствам адресатам.*

Удачи! ♥

1. Настроить сеть, состоящую из N компьютеров и K коммутаторов с помощью IPv6-адресации для сети A:B: … :Y:Z/M. Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 3 компьютера, 2 коммутатора.*

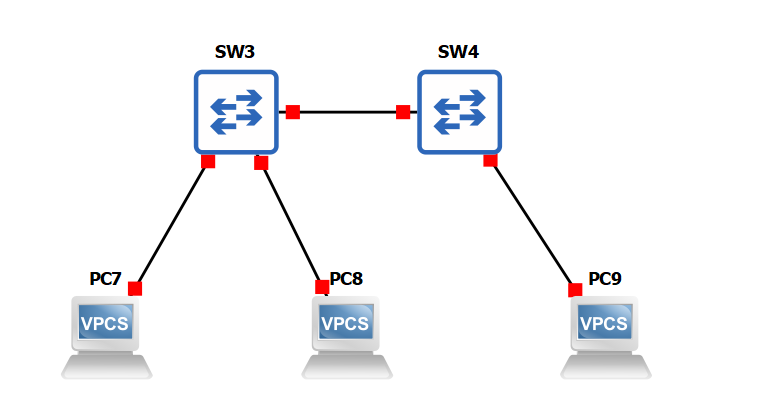
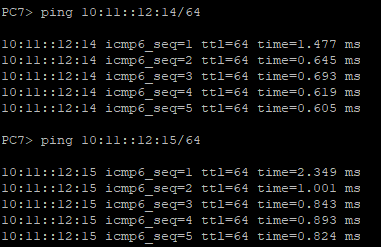
**

Схема сети





Задаем ipv6



Проверяем доступность PC

*Немного теории чтобы объяснить, что к чему:*

Хз что тут написать просто знайте что там где два двоеточия «::» в ipv6 адресе там нули. Так жеВ ipv6 128 бит тоесть 16 байт. Делиться он как мне сказали по «гектетам» (аналог октетов в ipv4 только содержит в себе не 8 бит а 16) но лучше это называть 16-ти ричным блоком это точно правильно. Тут стоит знать как делить ipv6 на подсети.

Удачи! ♥

1. Настроить IPv4-сеть, состоящую из N виртуальных сетей (VLAN), компьютеров (по 1-2 на каждый VLAN) и одного коммутатора. Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 2 виртуальные сети 4 компьютера и 1 коммутатор.*

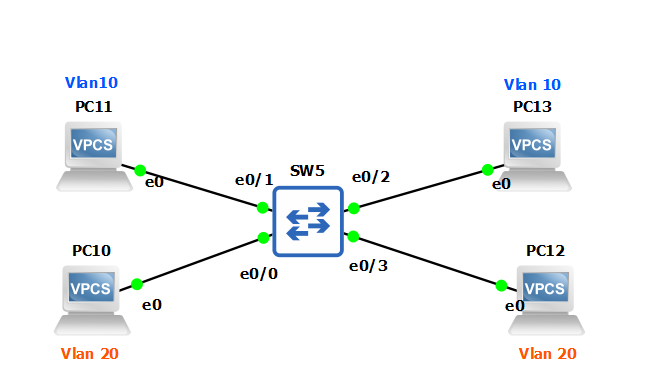
**

Схема сети



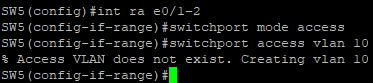




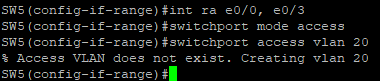


Задаем ip

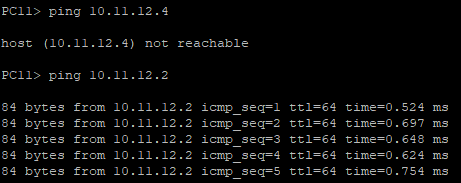
На коммутаторе заходим в интерфейсы подключенные к пк находящимися в одной сети Vlan и настраиваем access



Настройка для Vlan 10

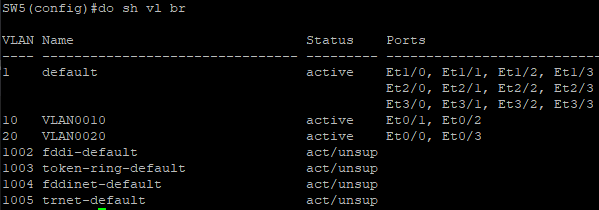


Настройка для Vlan 20



Показываем, что пинг проходит только на те устройства, которые находятся в той же сети Vlan

*(ip 10.11.12.4 принадлежит PC12 который находиться во Vlan 20 а пк с которого мы пингуем то есть PC11 находиться во Vlan 10 поэтому там трафик не проходит)*



Команда sh vlan brief для демонстрации настроенных vlan на коммутаторе

*Немного теории чтобы объяснить, что к чему:*

* Access порты в сетевом оборудовании, особенно в коммутаторах (switches), используются для подключения конечных устройств, таких как компьютеры, принтеры и тд.
* Изначально все порты коммутатора являются частью Vlan 1
* Транковые порты (trunk ports) — это сетевые порты на коммутаторе, которые способны передавать трафик для нескольких VLAN через один и тот же физический интерфейс. Они используются для передачи информации о разных VLAN между коммутаторами или другими сетевыми устройствами.

Удачи! ♥

1. Настроить IPv6-сеть, состоящую из N виртуальных сетей (VLAN), компьютеров (по 1-2 на каждый VLAN) и 1 коммутатора. Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 2 виртуальные сети 4 компьютера и 1 коммутатор.*

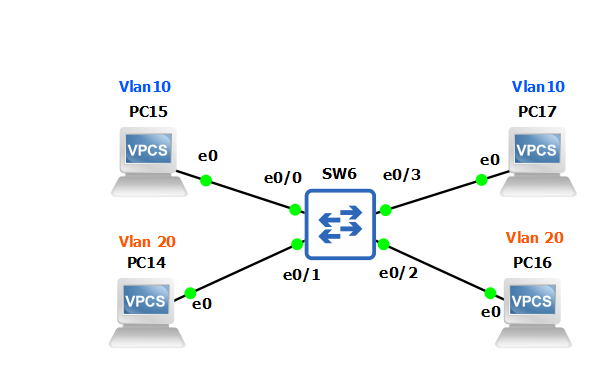
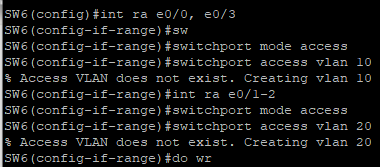


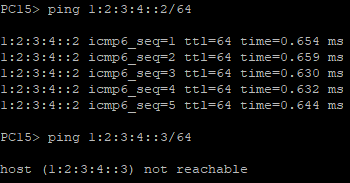
Схема сети



Настройка ipv6 (аналогично на других пк, меняеться только число 1 в конце тоесть у PC 17 например 1:2:3:4::2/64)

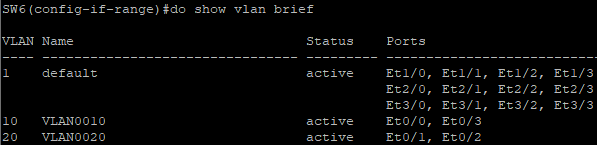


Настройка Vlan на коммутаторе



Показываем, что пинг проходит только на те устройства, которые находятся в той же сети Vlan

*(ip 1:2:3:4::3/64 принадлежит PC16 который находиться во Vlan 20 а пк с которого мы пингуем то есть PC15 находиться во Vlan 10 поэтому там трафик не проходит)*

**

Команда sh vlan brief для демонстрации настроенных vlan на коммутаторе

*Немного теории чтобы объяснить, что к чему:*

* Access порты в сетевом оборудовании, особенно в коммутаторах (switches), используются для подключения конечных устройств, таких как компьютеры, принтеры и тд.
* Изначально все порты коммутатора являются частью Vlan 1
* Транковые порты (trunk ports) — это сетевые порты на коммутаторе, которые способны передавать трафик для нескольких VLAN через один и тот же физический интерфейс. Они используются для передачи информации о разных VLAN между коммутаторами или другими сетевыми устройствами.

Удачи! ♥

1. Настроить IPv4-сеть, состоящую из N виртуальных сетей (VLAN), компьютеров (по 1-2 на каждый VLAN) и 2 коммутаторов, соединенные trunk’ом. Продемонстрировать работу trunk. Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 2 виртуальные сети 4 компьютера и 2 коммутаторa*

*Примечание: так как мы используем Trunk порты я подключил к каждому коммутатору компютеры находящиеся в разных Vlan. Это нужно чтобы продемонстрировать что коммутатор будет пропускать через транковый порт (тоесть в данном случае от SW5 к SW7) пакет относящийся к любой Vlan.*

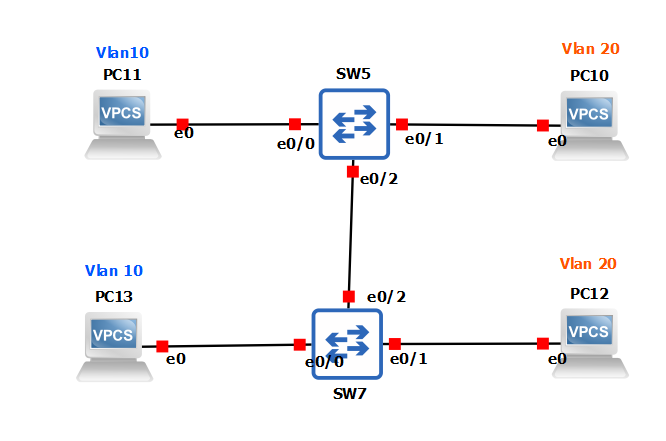
**

Схема сети

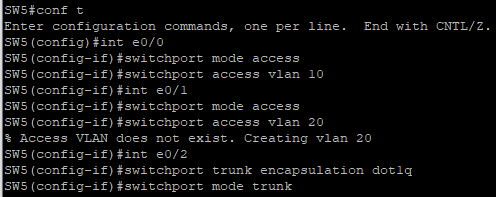




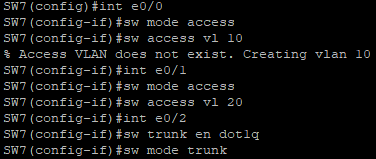




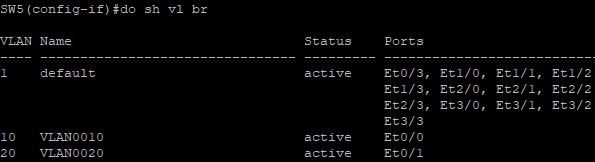
Задаем ip

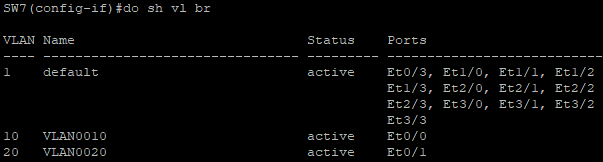


Настройка SW5 (порты, которые идут к пк настраиваем как access с нужными номерами vlan а те, что к коммутаторам как trunk)

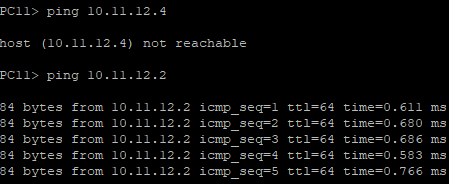


Настройка SW7 (порты, которые идут к пк настраиваем как access с нужными номерами vlan а те, что к коммутаторам как trunk) (используются сокращенные команды)





Командой show vlan brief демонстрируем настроенные vlan на обоих коммутаторах



Показываем, что пинг проходит только на те устройства, которые находятся в той же сети Vlan

*(ip 10.11.12.4 принадлежит PC12 который находиться во Vlan 20 а пк с которого мы пингуем то есть PC11 находиться во Vlan 10 поэтому там трафик не проходит)*

*Немного теории чтобы объяснить, что к чему:*

* Access порты в сетевом оборудовании, особенно в коммутаторах (switches), используются для подключения конечных устройств, таких как компьютеры, принтеры и тд.
* Изначально все порты коммутатора являются частью Vlan 1
* Транковые порты (trunk ports) — это сетевые порты на коммутаторе, которые способны передавать трафик для нескольких VLAN через один и тот же физический интерфейс. Они используются для передачи информации о разных VLAN между коммутаторами или другими сетевыми устройствами.

Удачи! ♥

1. Настроить IPv6-сеть, состоящую из N виртуальных сетей (VLAN), компьютеров (по 1-2 на каждый VLAN) и 2 коммутаторов, соединенные trunk’ом. Продемонстрировать работу trunk. Все неизвестные параметры задает преподаватель.

*Давайте предположим, что у нас есть 2 виртуальные сети 4 компьютера и 2 коммутаторa*

*Примечание: так как мы используем Trunk порты я подключил к каждому коммутатору компютеры находящиеся в разных Vlan. Это нужно чтобы продемонстрировать что коммутатор будет пропускать через транковый порт (тоесть в данном случае от SW5 к SW7) пакет относящийся к любой Vlan.*

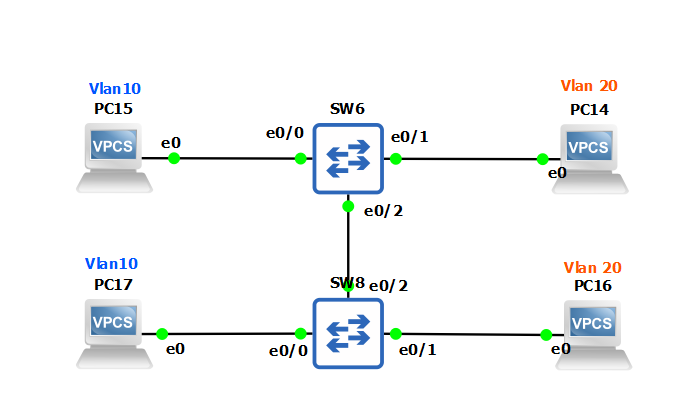
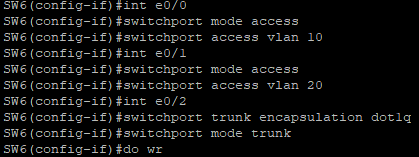


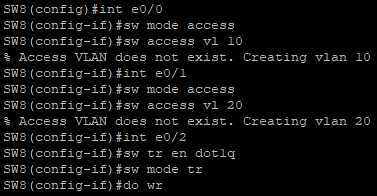
Схема сети



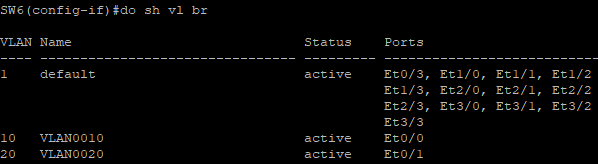
Настройка ipv6 (аналогично на других пк, меняеться только число 1 в конце тоесть у PC 17 например 1:2:3:4::2/64)

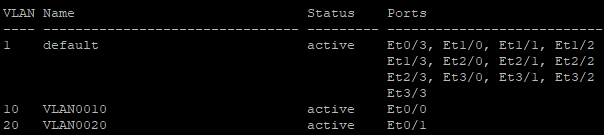


Настройка SW6 (порты, которые идут к пк настраиваем как access с нужными номерами vlan а те, что к коммутаторам как trunk)



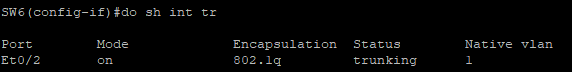
Настройка SW8 (порты, которые идут к пк настраиваем как access с нужными номерами vlan а те, что к коммутаторам как trunk) (используются сокращенные команды)



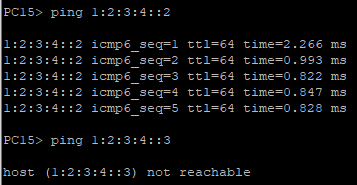


Командой show vlan brief демонстрируем настроенные vlan на обоих коммутаторах

*Примечание: для просмотра транковых портов коммутаора можете использовать команду «sh int trunk»*

**

Просмотр транковых протов



Показываем, что пинг проходит только на те устройства, которые находятся в той же сети Vlan

*(ip 1:2:3:4::3/64 принадлежит PC16 который находиться во Vlan 20 а пк с которого мы пингуем то есть PC15 находиться во Vlan 10 поэтому там трафик не проходит)*

*Немного теории чтобы объяснить, что к чему:*

* Access порты в сетевом оборудовании, особенно в коммутаторах (switches), используются для подключения конечных устройств, таких как компьютеры, принтеры и тд.
* Изначально все порты коммутатора являются частью Vlan 1
* Транковые порты (trunk ports) — это сетевые порты на коммутаторе, которые способны передавать трафик для нескольких VLAN через один и тот же физический интерфейс. Они используются для передачи информации о разных VLAN между коммутаторами или другими сетевыми устройствами.

Удачи! ♥