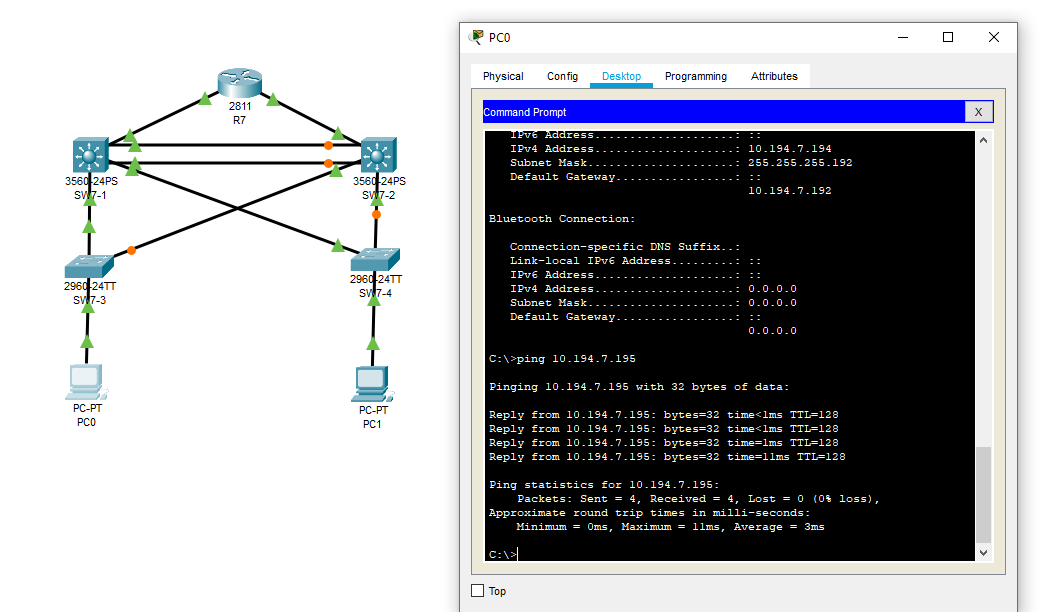
Дровосеков Д.А. КМБ-16

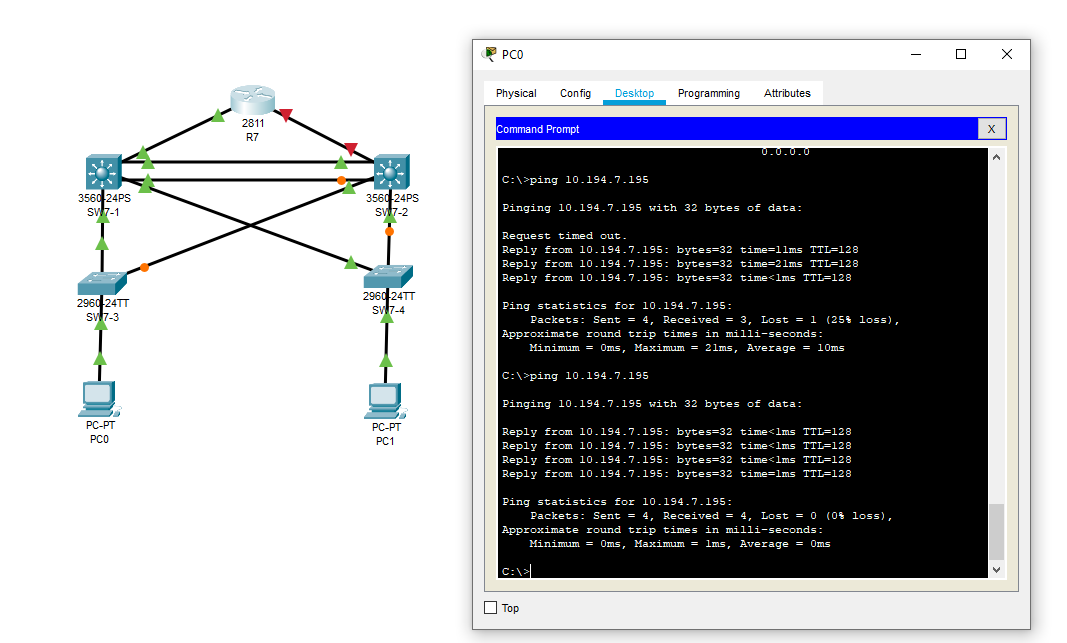
Чтобы убедиться в корректной работе построенной сети подключим две рабочие станции из одной VLAN.

Проверим связь между рабочими станциями при:

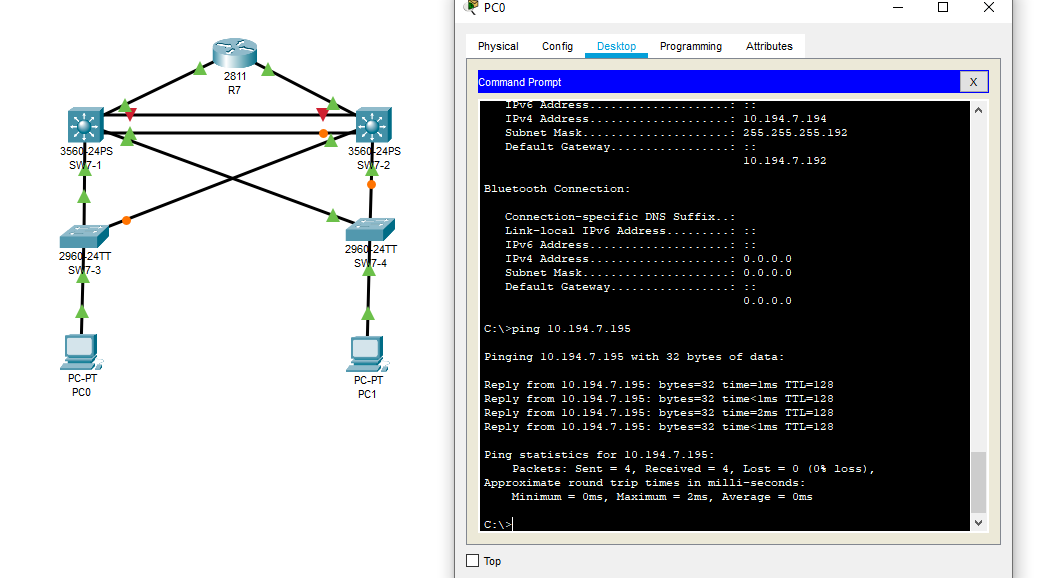
1. Полной работоспособности оборудования:



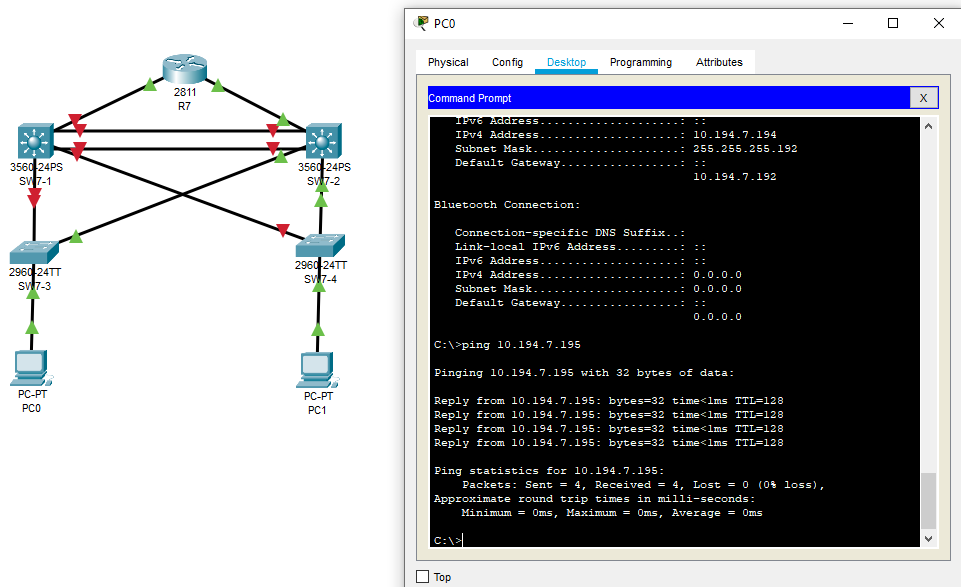
1. При отключении порта Fa0/3/1 маршрутизатора R7



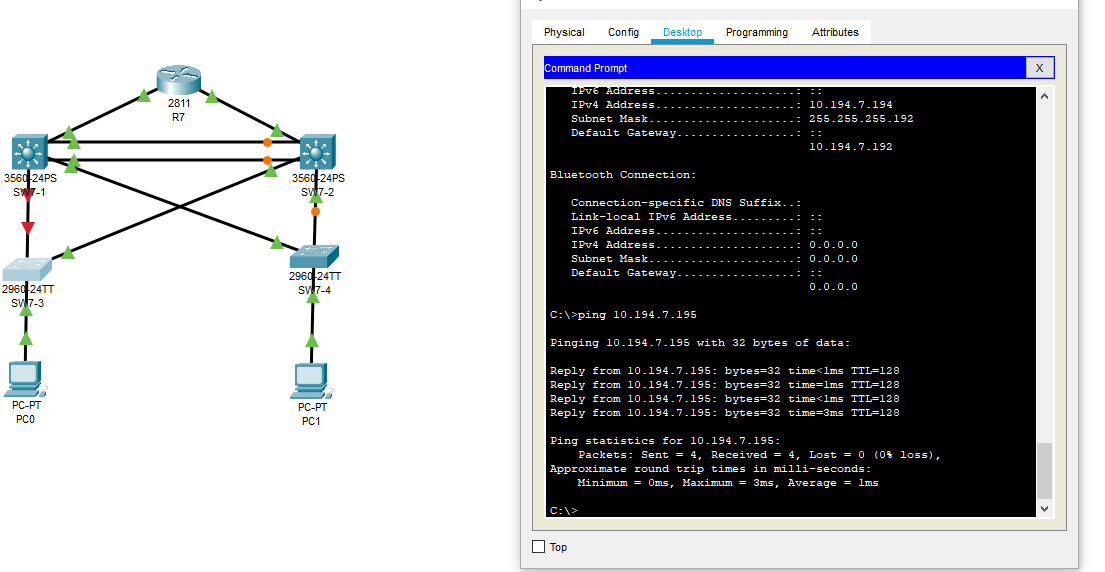
1. При отключении порта Gi0/1 коммутатора SW7-1



1. При отключении коммутатора SW7-1



1. При отключении порта Fa0/1 коммутатора SW7-3



1. Пояснить различия в работе между механизмами BPDU Guard, BPDU Filter и Root Guard. Описать области применения и назначение каждого из этих механизмов защиты.

BPDU Guard — функция, которая позволяет выключать порт при получении BPDU. Может быть включена глобально на коммутаторе или на интерфейсе. Таким образом BPDU guard защищает неизменность топологии сети, а главное препятствует злоумышленнику подключить устройство с низким приоритетом, чтобы заставить остальные коммутаторы думать, что в сети появился новый root и перестроить всю топологию относительно атакующего устройства.

Bdpufilter фильтрует в обе стороны, т.е. коммутатор отбрасывает все входящие BPDU и не отправляет BPDU в порт.

Root Guard - если функция включена на интерфейсе, то при получении на нём BPDU лучшего, чем текущий корневой коммутатор, порт переходит в состояние root-inconsistent (эквивалентно состоянию listening). После того как порт перестает получать BPDU, он переходит в нормальное состояние. Обычно эта функция включена на портах, подключенных к граничным коммутаторам, которые никогда не должны получать пакеты BPDU с более высоким BID.

2. Пояснить выбор портов активации механизма Root Guard на коммутаторах уровня ядра-распределения филиала.

Механизм Root Guard настраивается на портах коммутаторов SW7-1 и SW7-2, соединяющих с уровнем доступа. При изменении конфигурации, порт отключается, не дает устройствам на уровне доступа взять на себя роль корневого коммутатора.

3. Разработать проект внедрения механизма Loop Guard для защиты ЛВС от образования однонаправленных каналов связи.

Функция STP Loop Guard обеспечивает дополнительную защиту от закольцовывания при передаче на уровне 2 (петель STP). Петля STP появляется, когда порт в состоянии блокировки STP в топологии с резервированием ошибочно переходит в состояние пересылки. Обычно это происходит из-за того, что один из портов топологии с физическим резервированием (необязательно порт с блокировкой STP) больше не получает пакеты STP BPDU. Если все порты находятся в состоянии пересылки (forwarding), то это приводит к появлению петель (закольцовывания). Если порт, на котором включена функция Loop Guard, перестает получать пакеты BPDU из назначенного порта в сегменте, он переходит в состояние loop inconsistent вместо перехода в состояние forwarding. Как правило, состояние loop inconsistent является блокирующим, поэтому никакой трафик не пересылается. Если порт снова обнаруживает пакеты BPDU, он автоматически восстанавливается и переходит в состояние блокировки (blocking). Функцию Loop Guard следует применять к неназначенным портам.

Анализатор сетевого трафика (сниффер) поможет не только выявить наличие маршрутной петли, но и покажет сетевые устройства, которые ее создали:

1. Прежде всего, нужно локализовать проблемный участок. Определить какой из участков сети «падает».

2. Запустить сниффер с целью определения устройств, между которыми осуществляется столь «эмоциональное» общение.

3. Далее, понадобится определить пакеты, создающие широковещательный шторм и отфильтровать их. Как правило, эти IP-пакеты содержат одинаковый IP-идентификатор и их очень много.

4. Также, следует оценить время жизни таких пакетов. Проходя через роутер, пакет теряет единицу TTL, поэтому можно проследить каждую потерянную единицу вплоть до уничтожения самого пакета маршрутизатором.

5. Определив пакеты, имеющие явные признаки зацикливания в петле, можно отфильтровать (например, в Capsa) MAC-адреса физических устройств, которые принимают участие в общении по сетевой петле и посылают такие датаграммы.

6. Обладая сведениями о MAC-адресах, можно найти устройства, работа которых вызвала маршрутную петлю.

4. Смоделировать DoS-атаку на сетевую инфраструктуру при подключении к ЛВС коммутатора с наименьшим значением параметра BID.

BID состоит из числового значения приоритета и MAC-адреса. MAC-адрес устройства невозможно изменить, он имеет постоянное значение, поэтому можно изменить только величину приоритета. Атакующий коммутатор отправляет BPDU каждые 2 секунды с тем же приоритетом, что и у текущего корневого моста, но с немного меньшим численным MAC-адресом. Коммутатор-злоумышленник может запустить DoS-атаку, если он не распознает должным образом другие коммутаторы, вызывающие переполнение BPDU.

5. Смоделировать атаку типа BPDU spoofing на протокол STP путем подключения к ЛВС коммутатора нарушителя и получения им роли корневого моста.

Поскольку не существует механизма аутентификации, встроенного в протокол STP, существует возможность создания и отправки BPDU-фреймов вручную. Таким образом, злоумышленник может подключить собственный коммутатор на уровне ядра-распределения филиала и путём регулярной отправки ложных BPDU-фреймов с наименьшим значением BID обеспечивать для своего коммутатора роль корневого. Изменяя параметры Max Age, forward delay, hello time в C-BPDUs, с аналогичными параметрами, как у текущего designated bridge или designated root bridge, но с другими значениями параметров, определяющих паузы в рамках протокола. Мы могли бы управлять, по крайней мере, близлежащими STP-устройствами посредством постоянной и очень быстрой посылки таких C-BPDU.