**ПОЯСНЕНИЕ, ПОЧЕМУ МАЛО БАЛЛОВ В pkt ФАЙЛЕ:**

**Не засчитывает добавление интерфейсов в vlan BlackHole (скорее всего ошибка в названии)**

**Packet Tracer - Конфигурация безопасности коммутатора**

**Таблица VLAN**

| **Коммутатор** | **Номер VLAN** | **Имя VLAN** | **Членство в порту** | **Сеть** |
| --- | --- | --- | --- | --- |
| SW-1 | 10 | Администратор | F0/1, F0/2 | 192.168.10.0/24 |
| *SW-1* | 20 | Продажи | F0/10 | 192.168.20.0/24 |
| *SW-1* | 99 | Управление | F0/24 | 192.168.99.0/24 |
| *SW-1* | 100 | Собственный | G0/1, G0/2 | Нет |
| *SW-1* | 999 | BlackHole | Все неиспользуемые | Нет |
| SW-2 | 10 | Администратор | F0/1, F0/22 | 192.168.10.0/24 |
| *SW-2* | 20 | Продажи | F0/10 | 192.168.20.0/24 |
| *SW-2* | 99 | Управление | F0/24 | 192.168.99.0/24 |
| *SW-2* | 100 | Собственный | Нет | Нет |
| *SW-2* | 999 | BlackHole | Все неиспользуемые | None |

**Задачи**

**Часть 1. Создание защищенного магистрального соединения**

**Часть 2: Безопасность неиспользуемых портов коммутатора**

**Часть 3: Обеспечение безопасности портов**

**Часть 4: Включение отслеживание DHCP**

**Часть 5: Настройка Rapid PVST, PortFast и BPDU Guard**

**Общая информация**

Вы повышаете безопасность на двух коммутаторах доступа в частично настроенной сети. Вы реализуете ряд мер безопасности, описанных в этом модуле, в соответствии с приведенными ниже требованиями. Обратите внимание, что в этой сети настроена маршрутизация, поэтому соединение между узлами в разных VLAN должно функционировать после завершения.

**Инструкция**

**Шаг 1:Создание защищенного магистрального соединения**

a.     Соедините порты G0/2 двух коммутаторов уровня доступа.

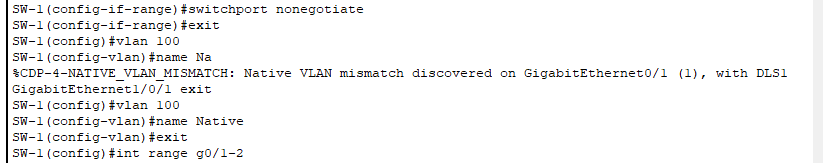
б.     Настройте порты G0/1 и G0/2 как статическое магистральное соединение на обоих коммутаторах.

в.     Отключите согласование DTP на обеих сторонах канала.

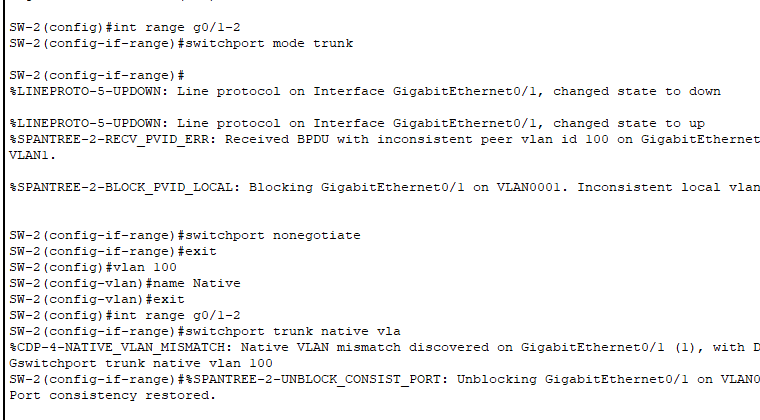
г.     Создайте VLAN 100 и присвойте ей имя Native на обоих коммутаторах.

д.     Настройте все магистральные порты на обоих коммутаторах для использования VLAN 100 в качестве native VLAN.









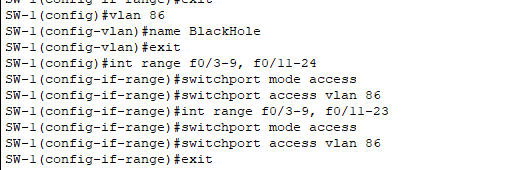
**Шаг 2: Безопасность неиспользуемых портов коммутатора**

1. Отключите все неиспользуемые порты на коммутаторе SW-1.



б.     На коммутаторе S1 создайте сеть VLAN 86 и присвойте ей имя BlackHole. Настроенное имя должно точно соответствовать требованию.

в.     Переместите все неиспользуемые порты коммутатора во VLAN BlackHole.



**Шаг 3: Настройте параметры безопасности портов.**

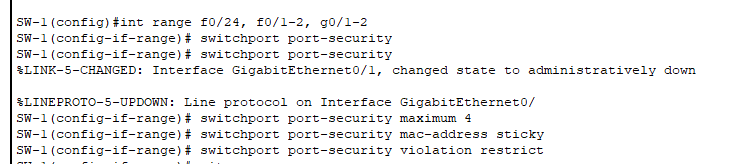
a.     Активируйте защиту портов на всех активных портах доступа на коммутаторе SW-1.

б.     Сконфигурируйте активные порты, чтобы разрешить изучение максимум 4 MAC-адресов на портах.

в.     Для портов F0/1 на SW-1 статически сконфигурируйте MAC-адрес компьютера с использованием защиты порта.

г.     Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса МАС, изученные на этом порту, в текущую конфигурацию.

д.     Настройте режим нарушения безопасности порта, чтобы отбрасывать пакеты с MAC-адресов, которые превышают максимум, генерировать запись системного журнала, но не отключать порты.

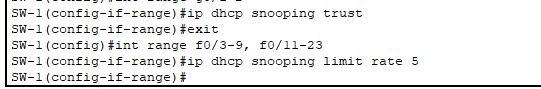


**Шаг 4: Настройте анализ DHCP-трафика.**

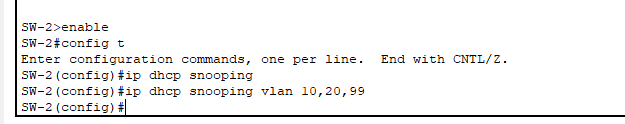
1. Настройте магистральные порты на SW-1 как доверенные порты.



б.     Ограничьте ненадежные порты на SW-1 пятью DHCP-пакетами в секунду.



в.     На SW-2 включите DHCP snooping глобально и для VLAN 10, 20 и 99.

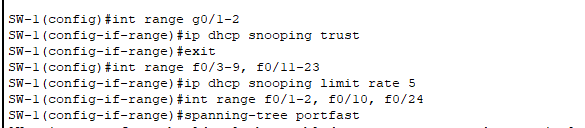


**Примечание.**Конфигурация отслеживания DHCP может не работать должным образом в Packet Tracer.

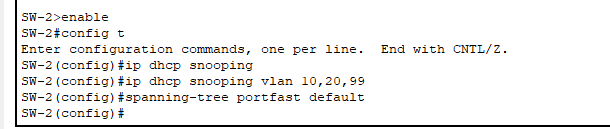
**Часть 5. Настройка PortFast и BPDU Guard**

a.     Включите PortFast на всех портах доступа, которые используются на SW-1.

б.     Включите BPDU Guard на всех портах доступа, которые используются на SW-1.



в.     Настройте SW-2, чтобы все порты доступа использовали PortFast по умолчанию.



*Конец документа*