ЗАДАНИЕ

1. Взять за основу лабораторную работу №1. Использовать Cisco Packet Tracer.

2. Изучить команды: `vlan`, `switchport mode`, `switchport access`, `switchport trunk`, `vtp`, `show vlan`, `show vtp`. Изучить как хранится информация о виланах.

3. Среди коммутаторов выбрать один -- Root. Дополнительно подключить к Root маршрутизатор либо заменить Root -- коммутатор заменить L3-коммутатором. В качестве маршрутизатора использовать 2811, 2901 либо 4331; в качестве L3-коммутатора использовать 3560 либо 3650. Учесть топологию и следующие пункты задания. Маршрутизатор можно подключить посредством более чем одного канала.

4. Реализовать концепцию виланов 802.1Q. Можно с помощью VTP. Одну из станций включить в административный вилан для управления всеми устройствами-посредниками. Оставшиеся станции распределить между двумя пользовательскими виланами, так чтобы к каждому из крайних коммутаторов были подключены станции из обоих виланов. Предусмотреть вилан для оригинально трафика (native) с идентификатором, отличным от идентификатора по умолчанию. Запретить передачу по транкам пакетов из неизвестных виланов. Использовать CLI.

5. Изучить команды: `speed`, `duplex`, `mdix`, `channel-group`, `interface port-channel`, `show etherchannel`.

6. Соединить Root с каждым из соседних коммутаторов минимум двумя физическими каналами. Настроить статическую либо динамическую агрегацию каналов. Параметры задействованных физических соединений (скорость и режим) задать вручную. Использовать CLI.

7. Изучить команды: `spanning-tree vlan`, `spanning-tree portfast`, `spanning-tree bpduguard`, `show spanning-tree`.

8. Убедиться в работоспособности PVST+. В каждом из виланов Root принудительно назначить корневым мостом. Использовать PortFast и BPDU Guard. Использовать CLI.

9. Изучить команды для создания SVI и подинтерфейсов (на маршрутизаторе), команду `encapsulation dot1q` (на маршрутизаторе).

10. Настроить маршрутизацию между виланами и тем самым обеспечить достижимость всех сетевых интерфейсов. Для адресации в виланах использовать соответствующее количество подсетей из указанных в варианте задания. Использовать CLI (коммутаторы, маршрутизатор) и графический интерфейс (ПК, ноутбуки).

11. Изучить команду `switchport port-security`.

12. С помощью Port Security защитить физический порт, к которому подключена станция для администрирования, от несанкционированного доступа (по своему усмотрению). Административно выключить все

незадействованные порты коммутаторов. Использовать CLI. Подумать о том как можно защитить административный вилан.

Требования к отчету:

1. Отчет оформлять по аналогии с отчетом по первой лабораторной работе.
2. Теоретическая часть. Пояснить (в произвольной форме, практический смысл) почему был выбран именно маршрутизатор либо L3-коммутатор, почему был использован либо не использован VTP, почему был выбран именно такой вариант агрегации каналов. Описать (детально) в чем заключается защита с помощью Port Security.
3. Практическая часть. Применительно к каждому коммутатору (маршрутизатору), переписать (вручную) части рабочей конфигурации, относящиеся к реализованным возможностям. Применительно к каждому ПК (ноутбуку), перерисовать панель `Desktop` -> `IP Configuration` -> `IP Configuration`.

Рабочие материалы:

1. На отдельном листе еще раз напечатать (скриншот) или изобразить (вручную) реализованную в Packet Tracer топологию. Названия сетевых интерфейсов должны быть видны. Кроме того, возле топологии указать использованные подсети. Возле каждого ПК (ноутбука) указать вилан, к которому он относится.