Packet Tracer. Отработка комплексных практических навыков

Топология

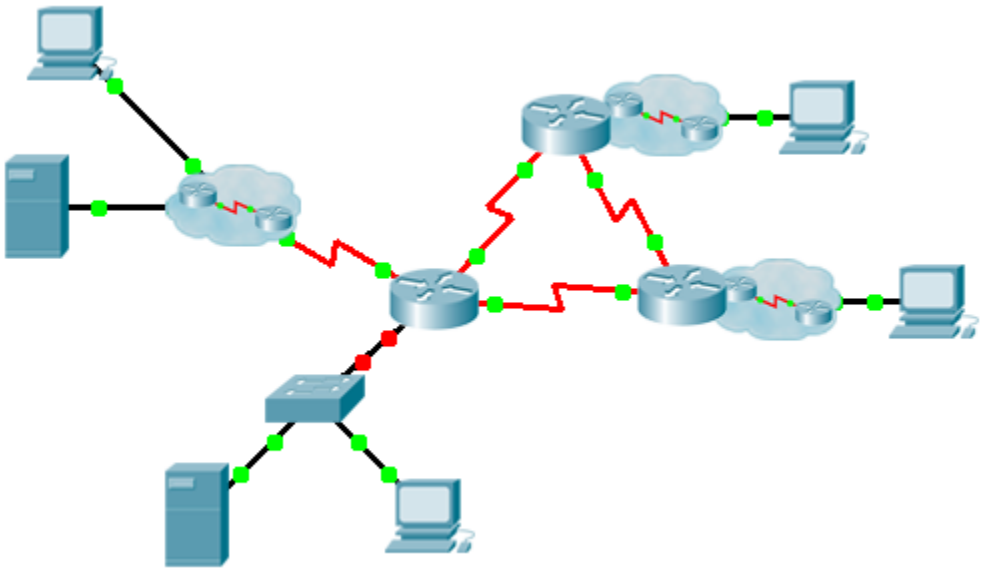

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
	G0/0.15			N/A
	G0/0.30			N/A
	G0/0.45			N/A
	G0/0.60			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	S0/1/0		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	VLAN 60			
	Сетевой адаптер	Назначенный DHCP	Назначенный DHCP	Назначенный DHCP

Таблица сетей VLAN и назначений портов

Номер сети VLAN — имя	Назначения портов	Сеть
15 — Servers	F0/11 - F0/20	
30 — PC	F0/1 - F0/10	
45 — Native	G1/1	
60 — Management	VLAN 60	

Сценарий

При прохождении данного интерактивного задания вам будет необходимо задействовать множество навыков, полученных в процессе изучения курса CCNA. Во-первых, вам предстоит составить документацию сети. Поэтому вам понадобится распечатанный вариант инструкций. На этапе реализации вы будете настраивать на коммутаторе виртуальные сети VLAN, транковые каналы, функцию защиты портов и удалённый доступ по протоколу SSH. Затем вы реализуете на маршрутизаторе маршрутизацию между сетями VLAN и преобразование NAT. Наконец, опираясь на документацию, необходимо будет проверить выполненную реализацию с помощью тестирования сквозного подключения.

Документация

Вы должны полностью задокументировать процесс настройки сети. Вам понадобится распечатка этих инструкций, включая диаграмму топологии без подписей:

- Присвойте метки всем именам устройств, сетевым адресам и прочей основной информации, созданной с помощью Packet Tracer.
- Заполните **Таблицу адресации** и **Таблицу сетей VLAN и назначений портов**.
- Заполните все пропуски в разделах **Реализация** и **Проверка**. Данная информация предоставляется при запуске задания Packet Tracer.

Реализация

Примечание. Все устройства в топологии за исключением _____, _____ и _____ полностью настроены. Вы не имеете доступ к другим маршрутизаторам. Для выполнения проверки вы можете получить доступ ко всем серверам и компьютерам.

Используя документацию, выполните приведённые ниже требования:

_____

- Настройте доступ к удалённому управлению устройством, в том числе IP-адресацию и SSH:
  - Домен — cisco.com
  - Пользователь — _____**,** пароль — _____
  - Длина ключа шифрования составляет 1024 бит
  - Протокол SSH версии 2 с ограничением на две попытки аутентификации и временем ожидания 60 секунд
  - Незашифрованные пароли необходимо зашифровать.
- Настройте, присвойте имена и назначьте сети VLAN. Порты необходимо настроить вручную в качестве портов доступа.
- Настройте транковую связь.
- Настройте функцию защиты портов:
  - На порте Fa0/1 разрешите доступ для двух MAC-адресов, которые автоматически добавляются в конфигурационный файл после обнаружения. Порт не должен быть выключен; в случае нарушения безопасности должно быть зафиксировано сообщение системного журнала.
  - Отключите все неиспользуемые порты.

_____

- Настройте маршрутизацию между сетями VLAN.
- Настройте DHCP-службы для VLAN 30. Используйте слово **LAN** в качестве имени пула (с учетом регистра).
- Реализуйте маршрутизацию:
  - Используйте идентификатор процесса OSPF со значением 1 и идентификатор маршрутизатора 1.1.1.1
  - Настройте одно выражением network для всего адресного пространства _____
  - Выключите интерфейсы, которые не должны отправлять OSPF-сообщения.
  - Настройте маршрут по умолчанию в сеть Интернет.

- Настройте преобразование сетевых адресов NAT:
  - Настройте стандартный ACL-список под номером 1, содержащий одну запись. Разрешите все IP-адреса, принадлежащие адресному пространству _____**.**
  - С помощью документации настройте статический NAT для файлового сервера (File Server).
  - Настройте динамический NAT с PAT, используя имя пула на свой выбор, маску /30 и следующие публичные адреса:

    _____

_____

Убедитесь, что _____ получил всю информацию об адресации от _____.

Проверка

Теперь все устройства должны успешно отправлять эхо-запросы другим устройствам. В противном случае выполните отладку. В рамках задания также необходимо выполнить следующее:

- проверить удалённый доступ к _____**,** используя SSH на ПК;
- убедиться, что сетям VLAN назначены правильные порты и обеспечивается защита портов;
- проверить соседей OSPF и всю таблицу маршрутизации;
- проверить преобразования NAT и статические IP-адреса.
  - **Внешний узел (Outside Host)** должен иметь доступ к **файловому серверу (File Server)** по публичному адресу.
  - Для внутренних ПК должен быть разрешен доступ к **веб-серверу (Web Server)**.
- Используя таблицу **Документация поиска и устранения неполадок,** задокументируйте все неполадки, с которыми вы столкнулись, а также способы их устранения.

Документация поиска и устранения неполадок

Проблема	Решение

Предлагаемый способ подсчета баллов

Выполнение задания в Packet Tracer дает 70 баллов. Документация дает 30 баллов.