Packet Tracer. Отработка комплексных практических навыков

Топология

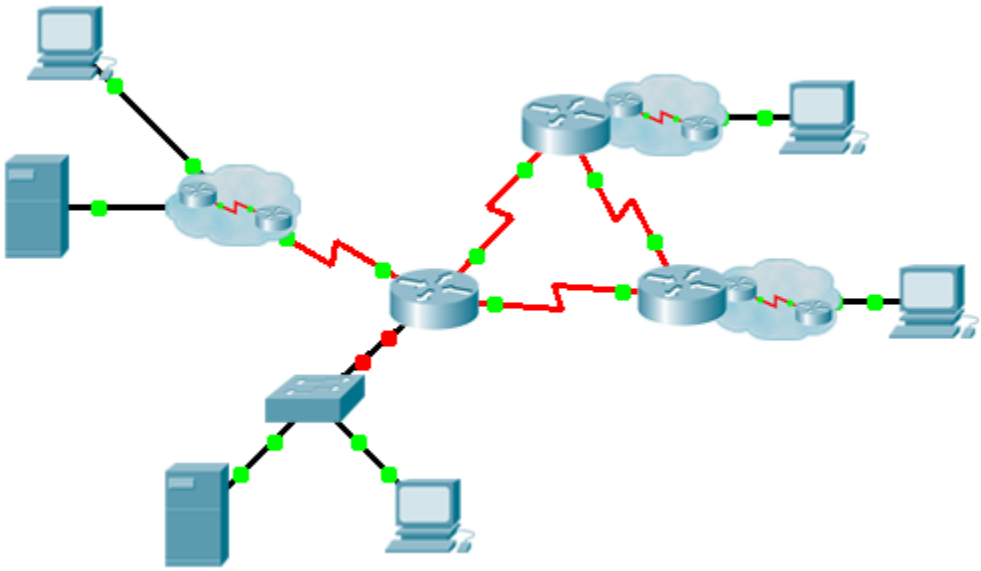

Таблица адресации

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

Сети VLAN и таблица назначения портов

VLAN – номер и имя	Назначение портов	Сеть
15 — Servers	F0/11 — F0/20	
30 — PCs	F0/1 — F0/10	
45 — Native	G1/1	
60 — Management	VLAN 60	

Сценарий

Это заключительное упражнение поможет отработать множество навыков, полученных в процессе освоения материала курса. Во-первых, нужно составить документацию сети. Убедитесь, что у вас есть 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 VLAN и преобразование NAT. Наконец, опираясь на документацию, необходимо провести проверку вашей реализации путём тестирования сквозного подключения.

Документация

Вы должны полностью задокументировать процесс настройки сети. Вам понадобится распечатка этих инструкций, включая схему топологии без каких-либо обозначений:

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

Реализация

Примечание. Все устройства в топологии, кроме , и , полностью настроены. Доступ к другим маршрутизаторам отсутствует. Вы можете получить доступ ко всем серверам и компьютерам для выполнения проверки.

Используя документацию, реализуйте приведённые ниже требования:

- Настройте доступ удалённого управления, 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 имя и назначьте сети VLAN. Порты следует настроить вручную как порты доступа.
- Настройте транковый канал.
- 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 службы syslog.
  - Отключите все неиспользуемые порты.
- Настройте маршрутизацию между VLAN.
- Настройте службы DHCP в сети VLAN 30. Используйте слово **LAN** в качестве имени пула (с учётом регистра).
- Выполните реализацию маршрутизации:
  - Используйте идентификатор 1 для процесса OSPF и идентификатор маршрутизатора 1.1.1.1
  - Настройте одно выражение network для всего адресного пространства
  - Выключите интерфейсы, которые не должны отправлять OSPF-сообщения.
  - Настройте маршрут по умолчанию в сеть Интернет.

- Выполните реализацию NAT:
  - Настройте стандартный ACL-список под номером 1, содержащий одно правило. 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 и два публичных адреса:

  Убедитесь, что получил всю информацию об адресации от

Проверка

Теперь все устройства должны успешно отправлять эхо-запросы всем другим устройствам. Если это не так, выполните поиск и устранение ошибок конфигурации. Процесс поиска неполадок может включать в себя ряд проверок:

- Проверьте удалённый доступ к , используя SSH на ПК.
- Убедитесь, что сетям VLAN назначены правильные порты и работает функция безопасности портов.
- Проверьте соседей OSPF и убедитесь в том, что таблица маршрутизации заполнена.
- Проверьте преобразования и статистику NAT.
  - **Внешний узел (Outside Host)** должен иметь доступ к **файловому серверу (File Server)** по публичному адресу.
  - Внутренние ПК должны иметь доступ к **веб-серверу**.
- В таблице **Результаты поиска и устранения неполадок** задокументируйте все неполадки, с которыми вы столкнулись, а также способы их устранения.

Результаты поиска и устранения неполадок

Проблема	Решение

Предлагаемый способ подсчёта баллов

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