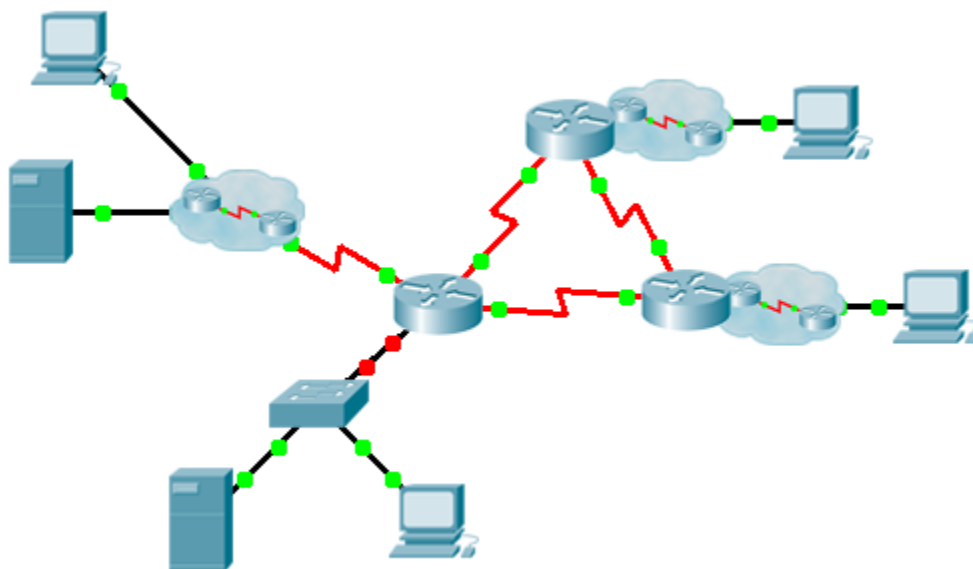


## Cisco Packet Tracer. Отработка комплексных практических навыков

### Топология



## Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
	G0/0.15			—
	G0/0.30			—
	G0/0.45			—
	G0/0.60			—
	S0/0/0		255.255.255.252	—
	S0/0/1		255.255.255.252	—
	S0/1/0		255.255.255.252	—
	G0/0			—
	S0/0/0		255.255.255.252	—
	S0/0/1		255.255.255.252	—
	G0/0			—
	S0/0/0		255.255.255.252	—
	S0/0/1		255.255.255.252	—
	VLAN 60			
	NIC	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 — PCs	F0/1 — F0/10	
45 — Native	G0/1	
60 — Management	VLAN 60	

## Сценарий

Данное заключительное упражнение поможет отработать многие навыки, полученные в процессе освоения учебного материала. Во-первых, нужно выполнить документирование сети. Вам понадобится распечатанный вариант этих инструкций. На этапе реализации вы будете настраивать на коммутаторе виртуальные сети VLAN, транки, функцию защиты портов и удаленный доступ по протоколу SSH. Затем вы организуете маршрутизацию между сетями VLAN и трансляцию NAT на маршрутизаторе. Наконец, опираясь на документацию, вы проведете проверку этой маршрутизации путем тестирования связи между конечными устройствами.

## Документация

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

- Подпишите все имена устройств, сетевые адреса и прочую важную информацию, выводимую 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 полностью настроены, за исключением \_\_\_\_\_, \_\_\_\_\_ и \_\_\_\_\_. Вы не имеете доступа к другим маршрутизаторам. Вы можете получить доступ ко всем серверам и компьютерам для выполнения проверки.

Используя документацию, реализуйте приведенные ниже требования:

- Настройте доступ к удаленному 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 проверки подлинности и временем ожидания 60 секунд.
  - Незашифрованные пароли необходимо зашифровать.
- Настройте сети VLAN, присвойте им имена и выполните назначение. Порты необходимо настроить вручную как порты доступа.
- Настройте транки.
- Настройте функцию защиты портов:
  - На порте Fa0/1 разрешите доступ для двух MAC-адресов, которые автоматически добавляются в конфигурационный файл после обнаружения. В случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала.
  - Отключите все неиспользуемые порты.
- Настройте маршрутизацию между VLAN.
- Настройте службу DHCP для VLAN 30. Используйте слово **LAN** в качестве имени пула (с учетом регистра)
- Реализуйте маршрутизацию:
  - В качестве протокола маршрутизации используйте RIPv2.
  - Настройте одно выражение network для всего адресного пространства
  - Отключите интерфейсы, которые не должны посылать сообщения RIPv2.
  - Настройте маршрут в Интернет по умолчанию.

- Настройте преобразование NAT:
  - Настройте стандартный ACL с номером 1, содержащий одну запись. Разрешите все IP-адреса, принадлежащие адресному пространству .
  - С помощью документации настройте статический NAT для файлового сервера (File Server).
  - Настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула, маску /30 и следующие два публичных 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 удаленный доступ к \_\_\_\_\_ , используя SSH на ПК.
- Убедитесь, что сетям VLAN назначены правильные порты, а защита портов работает.
- Проверьте соседей OSPF и полноту таблицы маршрутизации.
- Проверьте статистику и преобразования NAT.
  - **Внешний узел (Outside Host)** должен иметь доступ к **файловому серверу (File Server)** по публичному адресу.
  - Для внутренних компьютеров должен быть разрешен доступ к серверу **Web Server** (Веб-сервер).
- Используя приведенную ниже 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

Балл Packet Tracer: 70 баллов. За документирование дается 30 баллов.