CISCO Academy

Базовая конфигурация сетевых устройств

Топология



Цели

Часть 1. Создание сети и настройка основных параметров устройств Часть 2. Проверка соединения

Необходимые ресурсы

- 1 маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
- 1 коммутатор (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (под управлением Windows с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией

Инструкции

Часть 1. Создание сети и настройка основных параметров устройств

Шаг 1. Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2. Разбиение сети на подсети

Вам предоставлена сеть с входящим в нее ір-адресом 192.168.100.110/26. Разбейте предоставленную вам сеть на 6 равных подсети максимально возможного размера.

РС0 - находится в 3 по порядку подсети (подсеть А).

РС1 - находится в 5 по порядку подсети (подсеть В).

Первую, вторую, четвертую и шестую подсети сейчас задействовать не понадобится.

Шаг 3. Назначение ір-адресации устройствам

Назначьте ір-адреса, используя правила:

1) Компьютеры имеют первые узловые ір адреса в сети.

2) Маршрутизаторы имеют последние узловые ір адреса в сети.

3) Коммутаторы имеют предпоследние узловые ір адреса в сети.

Шаг 4. Настройка маршрутизатора

Укажите описание для интерфейсов маршрутизатора:

- для G0/2 - "To_A" (без кавычек);

- для G0/0 - "To_B" (без кавычек);

Настройте имя маршрутизатора – Rout_ФАМИЛИЯ.

Настройте сообщение, выводимое при подключении с текстом – «Protect» (без кавычек, пробелов и пустых строк).

Запретите обращение к DNS серверу для интерпретации неправильно введенных команд.

Настройте пароли. Для привилегированного режима используйте "connect123"(без кавычек, зашифрованный пароль), в качестве пароля консоли - "connect789" (без кавычек). Пароли должны запрашиваться при попытке получения доступа к соответствующему режиму.

Настройте подключение по SSH на маршрутизаторе по всем виртуальным линиям:

- длина rsa ключа – 1024;

- пользователь для подключения - user (с максимальным уровнем привилегий), пароль (зашифрованный) – userpass123.

Установите время разлогивания при бездействии равное 50 секундам.

Также необходимо разрешить подключаться к маршрутизатору только по протоколу SSH.

Зашифруйте все пароли.

Настройте защиту таким образом, чтобы если в течение 70 секунд был 7 раз введен неверный пароль, то доступ к устройству блокировался на 50 секунд.

Установите минимальную длину пароля равную 10.

Шаг 5. Настройка коммутатора

Задайте на коммутаторе IP-адрес для удаленного подключения (используйте предпоследний доступный в подсети "А" узловой IP-адрес для vlan 1).

Обеспечьте удаленное подключение по сети к коммутатору с компьютера РС1 для управления им.

Часть 2. Проверка соединения

Убедитесь в следующем:

- ПК "видят" друг друга;
- к сетевым устройства можно подключиться по сети с любого устройства и конфигурировать их.

Если что-то не работает - постарайтесь исправить.