Лабораторная работа №8. Обеспечение безопасности порта в cisco packet tracer.

Цель работы: получить практические навыки работы с оборудованием Cisco, используя эмулятор сетевой среды Cisco Packet Tracer. Для этого необходимо установить программу, изучить ее интерфейс и функциональные возможности. Собрать работоспособную модель сети на основе маршрутизаторов и коммутаторов, выполнить настройку маршрутизатора командами конфигурирования IOS с применением списков управления доступа ACL и службы трансляции адресов NAT.

Теоретический материал:

Команда access-list

Критерии фильтрации задаются в списке операторов разрешения и запрета, называемом списком доступа. Строки списка доступа сравниваются с IP-адресами и другой информацией пакета данных последовательно в том порядке, в котором были заданы, пока не будет найдено совпадение. При совпадении осуществляется выход из списка. При этом работа списка доступа напрямую зависит от порядка следования строк. Списки доступа имеют 2 правила: permit – разрешить, и deny – запретить. Именно они определяют, пропустить пакет дальше или запретить ему доступ.

Списки доступа бывают 2-ух типов: standard – стандартные (номера с 1 до 99) и extended – расширенные (номера с 100 до 199). Различия заключаются в возможности фильтровать пакеты не только по ip-адресу, но и по другим параметрам.

Формат команды (стандартные списки доступа):
access-list номер_списка/имя правило A.B.C.D a.b.c.d

где A.B.C.D a.b.c.d – ip-адрес и подстановочная маска соответственно.

Пример выполнения команды:

Router(config)#

Router(config)#access-list 10 deny 192.168.3.0 0.0.0.3

Данная команда означает, что данный список доступа блокирует любые пакеты с ip-адресами 192.168.3.1 - 192.168.3.3.

Команда enable secret

Обычно при входе в привилегированный режим требуется ввести пароль. Данная функция позволяет предотвратить несанкционированный доступ в данный режим, ведь именно из него можно изменять конфигурацию устройства. Данная команда позволяет установить такой пароль.

Формат команды:

enable secret пароль

Пример выполнения команды:

Switch(config)#enable secret 123

Switch(config)#

%SYS-5-CONFIG_I: Configured from console by console

Switch#exit

Switch con0 is now available

Press RETURN to get started.

Switch>enable

Password:

После того, как был установлен пароль, при попытке входа в привилегированный режим, коммутатор будет требовать от пользователя его ввести – в противном случае вход будет невозможен.

Команда interface

Команда для входа в режим конфигурирования интерфейсов конфигурируемого устройства. Данный режим представляет собой одно из подмножеств режима глобального конфигурирования и позволяет настраивать один из доступных сетевых интерфейсов (fa 0/0, s 2/0 и т.д.). Все изменения, вносимые в конфигурацию коммутатора в данном режиме относятся только к выбранному интерфейсу.

Формат команды (возможны 3 варианта):

interface тип порт

interface тип слот/порт

interface тип слот/подслот/порт

Примеры выполнения команды:

Switch(config)#interface vlan 1

Switch(config-if)#

Router(config)#interface s 3/0

Router(config-if)#

После введения данной команды с указанным интерфейсом пользователь имеет возможность приступить к его конфигурированию. Необходимо заметить, что, находясь в

режиме конфигурирования интерфейса, вид приглашения командной строки не отображает имя данного интерфейса.

Команда ip access-group

Данная команда используется для наложения списков доступа. Список накладывается на конкретный интерфейс, и указывается один из 2-ух параметров: in (на входящие пакеты) или out (на исходящие). Необходимо знать, что на каждом интерфейсе может быть включен только один список доступа.

Формат команды:

ip access-group номер_списка/имя_параметр

Пример выполнения команды:

Router(config-if)# ip access group 10 in

Router(config-if)#

В данном примере да выбранный интерфейс накладывается список доступа под номером 10: он будет проверять все входящие в интерфейс пакеты, так как выбран параметр in.

Команда no

Данная команда применяется в случае необходимости отменить действие какой-либо команды конфигурирования.

Формат команды:

no команда_которую_следует_отменить

Пример выполнения команды:

Switch(config-if)# no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#

В данном примере использовалась команда shutdown, которая отключает выбранный интерфейс. В итоге после выполнения no shutdown интерфейс включается.

Команда show

Show (англ. - показывать) – одна из наиболее важных команд, использующихся при настройке коммутаторов. Она применяется для просмотра информации любого рода и применяется практически во всех контекстах. Эта команда имеет больше всех параметров.

Здесь будут рассмотрены только те параметры, которые требуются в рамках данного курса. Другие параметры студент может изучить самостоятельно.

Таблица 1. Параметры команды show

Команда	**Описание**
show version	Выводит на экран данные о конфигурации аппаратной части системы, версии программного обеспечения, именах и источниках конфигурационных файлов и загруженных образах
show running-conf ig	Показывает содержание активной конфигурации
show interfaces	Показывает данные обо всех интерфейсах на устройстве
show protocols	Выводит данные о протоколах третьего сетевого уровня.

Команды ping и traceroute

Для диагностики возможности установления связи в сетях используются протоколы тип запрос-ответ или протокол эхо-пакетов. Результаты роботы такого протокола могут помочь в оценке надёжности пути к другому устройству, величин задержек в целом и между промежуточными устройствами. Для того чтобы такая команда работала, необходимо, чтобы не только локальное сетевое устройство знало, как попасть в пункт назначения, но и чтобы устройство в пункте назначения знало, как добраться до источника.

Команда **ping** посылает ICMP(Internet Control Message Protocol) эхо-пакеты для верификации соединения. В приведённом ниже примере время прохождения одного эхо-пакета превысило заданное, о чём свидетельствует точка (.) в выведенной информации, а четыре пакета прошли успешно, о чём говорит восклицательный знак (!).

Switch> **ping 172.16.101.1**
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:

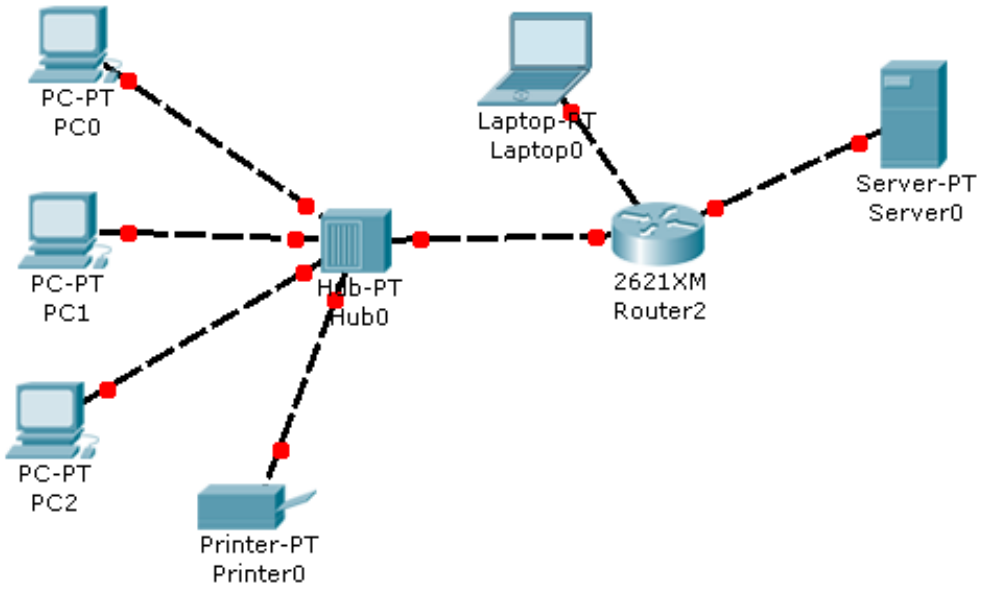
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms

Таблиця 2. Результаты команды ping

Символ	**Значение**
!	Успешный приём эхо-ответа
.	Превышено время ожидания
U	Пункт назначения недосягаем
C	Перегрузка сети
I	Выполнение команды прервано администратором
?	Неизвестный тип пакета
&	Пакет превысил значение параметра времени жизни TTL пакета

Практическая часть:

1. Собрать модель сети. Взять за основу предложенный ниже вариант, либо придумать свою, но отвечающую требованиям задания.



2. Настроить на маршутизаторе списки доступа ACL для выполнения следующих действий:
    1. Запретить ping из внешней сети.
    2. Запретить доступ из внешней сети к принтеру, размещенному во внутренней сети.

3. Разрешить одному из ПК внутренней сети доступ к внешнему фтп-серверу.
4. Разрешить одному из ПК внутренней сети доступ к внешнему mail-серверу.
5. Запретить icmp трафик из внутрисети.
6. Разрешить доступ из внутрисети ко внешнему WEB-серверу для всех ПК.

3. Выполнить настройку статической, динамической и динамической трансляции с использованием одного глобального адреса:

    1. Настройка статической трансляции

1. Настройте NAT.

   Пример настройки:

   ip nat inside source static 192.168.0.2 31.1.3.2

   ip nat inside source static 192.168.0.3 31.1.3.3

   interface FastEthernet 0/0

   ip nat inside

   interface FastEthernet 0/1

   ip nat outside

2. Просмотрите текущее состояние NAT при помощи команд **show ip nat translations** и **show ip nat statistics**.
3. Проверьте правильность статической маршрутизации, посылая пакеты **ping** из внутренней сети во внешнюю и обратно.
4. Выполните команды из п.2. во время взаимодействия между внутренней и внешней сетью и после него. Результаты добавьте в отчет.
5. Отмените статическую трансляцию адресов с помощью команды **no**:

   Пример:

   no ip nat inside source static 192.168.0.2 31.1.3.2

   no ip nat inside source static 192.168.0.3 31.1.3.3

6. Настройте списки ACL, необходимые для работы NAT. Добавьте в отчет сформированные правила.

Замечание. Список доступа должен разрешать только те адреса, которые действительно необходимо транслировать. Список доступа, разрешающий более широкий блок адресов может привести к непредсказуемым результатам.

    2. Настройка динамической трансляции

Добавьте во внутреннюю сеть еще две рабочие станции. Теперь внешних адресов меньше, чем реальных станций и вместо статической трансляции воспользуемся динамической.

1. Просмотрите таблицу NAT с помощью утилиты **show ip nat translations**. Убедитесь, что в таблице записи отсутствуют. Это означает, что узлы внутренней сети недоступны из внешней сети.
2. Настройте NAT в глобальном режиме аналогично следующему примеру:
   ip nat pool p1 31.1.3.2 1.1.3.3 netmask 255.255.255.0
   ip nat inside source list 1 pool p1
3. Пошлите пакеты **ping** из внутренней сети во внешнюю.
4. Просмотрите текущее состояние NAT при помощи команд **show ip nat translations** и **show ip nat statistics**. В таблице NAT должны появиться записи динамической трансляции адресов.
5. Пошлите пакеты **ping** из внешней сети во внутреннюю.
6. Изучите утилиты очистки записей динамической трансляции адресов таблицы NAT **clear**. Проверьте их работу.
7. Отмените динамическую трансляцию адресов:
   no ip nat inside source list 1 pool p1
8. Настройте списки ACL, необходимые для работы NAT. Добавьте в отчет сформированные правила.

1. Настройка динамической трансляции с использованием одного глобального адреса

1. Просмотрите таблицу NAT с помощью утилиты **show ip nat translations**. Убедитесь, что в таблице записи отсутствуют. Это означает, что узлы внутренней сети недоступны из внешней сети.
2. Настройте NAT в глобальном режиме аналогично:
   ip nat pool p2 31.1.3.2 31.1.3.2 netmask 255.255.255.0
   ip nat inside source list 1 pool p2 overload
3. Пошлите пакеты **ping** из внутренней сети во внешнюю.
4. Просмотрите текущее состояние NAT при помощи команд **show ip nat translations** и **show ip nat statistics**. Обратите внимание, что два внутренних локальных адреса используют один внутренний глобальный адрес, используя для этого разные порты TCP.
5. Изучите утилиту очистки расширенной записи динамической трансляции адресов таблицы NAT **clear**. Проверьте ее работу.
6. Отмените динамическую трансляцию адресов.

Контрольные вопросы:

1. Опишите отличия работы сетевого коммутатора и сетевого маршрутизатора.

2. Какие типы линий связи используются при организации локальной вычислительной сети? Дайте их характеристику.
3. Какие типы устройств входят в состав локальной вычислительной сети?
4. Перечислите действия, необходимые для организации локальной вычислительной сети.
5. Поясните в каких случаях и почему применяются прямой и перекрестный кабели UTP.