Лабораторная работа

Обеспечение безопасности в сетях на базе оборудования Cisco. Списки управления доступом ACL и служба трансляции адресов NAT

УДК 004.9

Составители: доц. канд. техн. наук В.Н. Круглов, С.А. Широков

Лабораторная работа. Обеспечение безопасности в сетях на базе оборудования Cisco. Списки управления доступом ACL и служба трансляции адресов NAT/ сост. С.А.Широков, В.Н. Круглов. Екатеринбург: УГТУ-УПИ, 2010. 35 с.

Для выполнения лабораторной работы отводится два занятия. Лабораторная работа имеет цель оказать помощь в обретении практических навыков студентами всех форм обучения (очной, заочной, очно-заочной, экстерната) специальности 230102 – «Автоматизированные системы обработки информации и управления» при построении сетей на базе оборудования CISCO и вопросам безопасности на основе технологий ACL и NAT.

Методические указания могут быть полезны также преподавателям, осуществляющим руководство студентами – практикантами, и руководителям преддипломной практики студентов.

Библиогр.: назв. табл. 3. рис. 1.

Подготовлено кафедрой «Автоматизированные системы управления».

СОДЕРЖАНИЕ

1. 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.

2. Введение

Packet Tracer — бесплатный эмулятор сетевой среды, выпускаемый фирмой Cisco. Позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы работающие на операционной системе Cisco IOS, взаимодействовать между несколькими пользователями. Включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650. Кроме того среди компонентов есть серверы DHCP, HTTP, TFTP, FTP, TIME, рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства Wi-Fi и различные типы линий связи.

Данный пакет имитационного проектирования и моделирования позволяет создавать виртуальные сети практически любой топологии и производить в них поиск неисправностей. Кроме этого он используется при обучении по курсу CCNA профессиональной сертификации в области информационных технологий для работы с продукцией Cisco Systems.

3. Краткое описание интерфейса программы

После установки программы в меню пуск появляется следующая ссылка для запуска: *Пуск > Все программы > Cisco Packet Tracer > Cisco*

Packet Tracer. Открыв *Packet Tracer*, вы увидите главное окно программы, изображенное на рисунке 1, которое состоит из 10 областей:

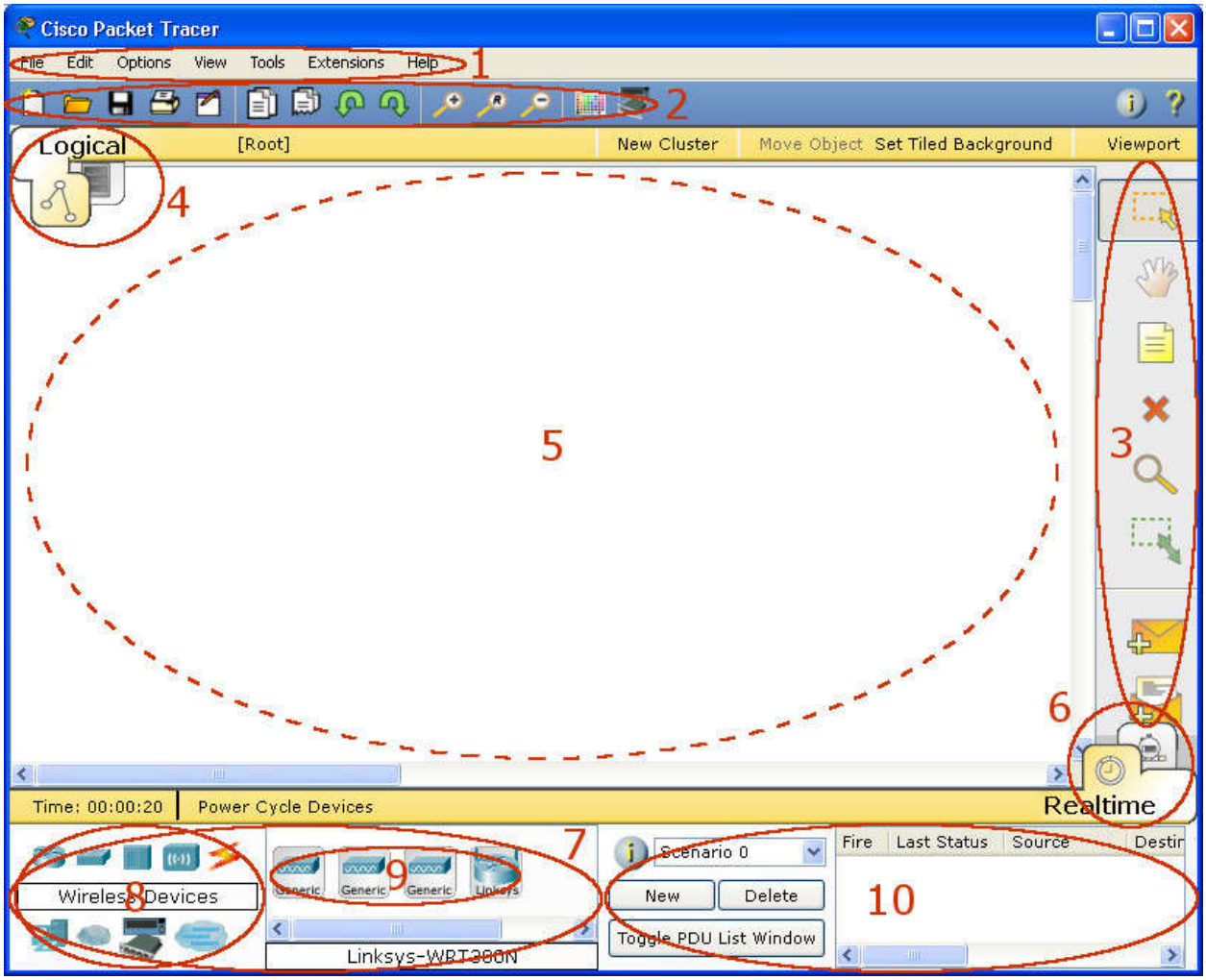


Рисунок 1 – Главное окно программы *Cisco Packet Tracer*

1. ***Главное меню***. Предоставляет интерфейс управления для оконных приложений со стандартными разделами: *File, Edit, Options, View, Tools, Extensions* и *Help* и командами *Open, Save, Save as Pkz, Print* и *Preferences.*
2. ***Панель инструментов***. Содержит кнопки быстрого вызова команд из меню *File* и *Edit* а так же команд *Zoom, Drawing Palette и Custom Devices Dialog.*
3. **Панель инструментов рабочей области.** Содержит наиболее часто используемые операции, применяемые при построении модели сети:

Select, Move Layout, Place Note, Delete, Inspect, Resize Shape, Add Simple PDU и *Add Complex PDU.*

4. ***Навигационная панель.*** Эта особая панель, которая располагается под панелью инструментов. Она позволяет переключать рабочую область между логической и физической топологией сети. Физическая топология подразумевает расположение устройств в городе, районе, офисе. Здесь можно посмотреть как топологию сети всего города, так и расположение устройств в офисе, и даже на отдельной Rack-стойке.
5. ***Рабочая область***. Данная область занимает большую чать окна программы, здесь происходит конструирование виртуальной сети, где размещаются устройства и строятся связи между ними. Двойной клик по любому устройству открывает окно его конфигурации.

   Окно конфигурации устройств состоит из 3-х вкладок:

   1) *Phusical* – Показывает внешний вид устройства и позволяет добавлять либо убирать модули. Модули нельзя добавлять/извлекать при включенном устройстве!
   2) *Config* — эта вкладка не открывается, пока устройство не загрузилось. Здесь осуществляется графическое конфигурирование оборудования Cisco без применения командной строки, но для информативности внизу отображаются команды, которые выполняются при конфигурации.
   3) *CLI/Desktop* – в зависимости от устройства позволяет получить доступ к командной строке IOS либо к рабочему столу Linux.
6. ***Панель симуляции/реального времени***. После запуска программа находится в логическом режиме реального времени, можно строить сеть и смотреть, как она работает. Данная панель позволяет переключаться в режим симуляции и обратно. В этом режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет наглядно видеть, по какому интерфейсу в данный момент перемещается

пакет, какой протокол используется и т.д. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован.

7. ***Блок выбора сетевых компонентов***. Область выбора устройств либо методов связи для перетаскивания в рабочую область. Состоит из двух составных частей: области выбора типа устройства и области выбора конкретной модели устройства.
8. ***Область типа устройств***. Позволяет выбрать и моделировать большое количество устройств различного назначения: маршрутизаторы, комутаторы (в том числе и мосты), хабы и повторители, конечные устройства – ПК, серверы, принтеры, IP-телефоны; безпроводные устройства: точки доступа и безпроводные маршрутизаторы; остальные устройства – Internet-облако, DSL-модем и кабельный модем, а так же разнообразные линий связи от консольного кабеля до оптической линии.
9. ***Область моделей устройств***. Область выбора конкретной модели устройства указанного типа. Перечислим некоторые модели устройств, которые может моделировать *Packet Tracer :* маршрутизаторы: 1841, 2620XM, 2621XM, 2811; коммутаторы: 2959-24, 2950T, 2960, 3560; беспроводные устройства: Linksys-WRT300N и многое другое.
10. ***Окно пользовательских пакетов.*** Окно управляет пакетами, которые были созданы в сети во время сценария симуляции.

В дополнение к теоретической части лабораторной работы предлагается просмотреть обучающий видеоурок *“Демонстрация работы в Packet Tracer.avi”*, более детально знакомящий пользователя с интерфесом программы *Packet Tracer* и основам работы в ней.

4. Введение в межсетевую операционную систему IOS компании Cisco.

При первом входе в сетевое устройство пользователь видит командную строку пользовательского режима вида:

Switch>

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

Press ENTER to start.
Switch>
Switch> ***enable***
Switch#
Switch# ***disable***
Switch>

Здесь и далее вывод сетевого устройства будет даваться обычным шрифтом, а ввод пользователя **жирным** шрифтом.

О переходе в этот режим будет свидетельствовать появление в командной строке приглашения в виде знака #. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подинтерфейса, линии, сетевого устройства, карты маршрутов и т.п. Для выхода из системы IOS необходимо набрать на клавиатуре команду ***exit*** (выход).

Switch> ***exit***

Независимо от того, как обращаются к сетевому устройству: через консоль терминальной программы, подсоединённой через ноль-модем к

COM-порту сетевого устройства, либо в рамках сеанса протокола Telnet, устройство можно перевести в один из режимов. Нас интересуют следующие режимы.

Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид типа *Switch>*.

Привилегированный режим — поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид типа *Switch#.*

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид типа *Switch(config)#* .

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (***?***) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - *More* -. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходов в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима

configure. При вводе этой команды следует указать источник команд конфигурирования: *terminal* (терминал), *memory* (энергонезависимая память или файл), *network* (сервер tftp (Trivial ftp -упрощённый ftp) в сети). По умолчанию команды вводятся с терминала консоли. Например:

Switch# ***configure terminal***
Switch(config)#(commands)
Switch(config)# exit
Switch#

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение *Switch(config-if)#*, сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

Switch# ***conf t***
Switch(config)# ***interface type port***
Switch(config-if)# ***(commands)***
Switch(config-if)# ***exit***
Switch(config)# ***exit***

5. Список команд

В данном списке собраны только те команды конфигурирования, которые необходимы для выполнения лабораторной работы.

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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*.

5.5. 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.

5.6. 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.

5.7. 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

Таблица 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

Команды ***traceroute*** показывает адреса промежуточных интерфейсов (хопов) на пути пакетов в пункт назначения.

Switch> ***traceroute 172.16.101.1***

Расширенная версия команды ping поддерживается только в

привилегированном режиме. Команда в режиме диалога опрашивает значения параметров. Важно отметить, что эта команда позволяет, находясь на одном устройстве, проверять связь между сетевыми интерфейсами на других устройствах.

Router# ***ping***
Protocol [ip]:
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: ***y***
Source address:1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data [no]:
Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:

6. Введение в технологию ACL

Списки управления доступом (Access Control List, ACL) – одно из важнейших средств организации базовой безопасности составных и распределенных IP-сетей. Требование безопасности особенно актуально в локальных корпоративных сетях, когда они через пограничные маршрутизаторы связаны с открытой глобальной сетью Internet.

Списки доступа являются управляемыми фильтрами для проходящего трафика и при соответствующей настройке один трафик они могут беспрепятственно пропускать дальше, другой – блокировать (подавлять, отбрасывать). ACL устанавливаются на интерфейсах маршрутизаторов. Очевидным и естественным местом ACL являются интерфейсы пограничных маршрутизаторов. В результате эти маршрутизаторы становятся межсетевыми экранами или брандмаурами (firewall), подавляя

непредусмотренный сетевой трафик из Internet в корпоративную сеть и наоборот и обеспечивая защиту периметра корпоративной сети.

Операционная система маршрутизаторов от компании Cisco Systems имеет мощные встроенные средства для создания разнообразных по сложности и функциональности списков доступа. При этом критерием для фильтрации могут быть значения IP-адреса отправителя и получателя проходящих пакетов сетевого уровня, имена протоколов более высокого уровня, номера TCP- и UDP-портов и др. параметры.

В целом, список доступа ACL представляет собой упорядоченный набор из одного или нескольких правил (шаблонов), используемых для сравнения с параметрами проходящих пакетов через данный интерфейс. Синтаксически отдельное правило – это одна строка. Для каждого пакета список ACL просматривается заново, последовательно, начиная с первого правила:

- если параметры пакета не совпадают с параметрами данного правила, то правило игнорируется и рассматривается следующее по порядку правило;
- если параметры пакета правилу удовлетворяют, то выполняется одно из запрограммированных в правиле действий – разрешить (ключевое слово **permit**) прохождение пакета дальше или блокировать (**deny**) прохождение. При этом последующие правила в ACL для этого пакета уже не рассматриваются.

С целью большей безопасности в конце каждого списка ACL присутствует неотображаемое (скрытое) правило – “запретить все кроме того, что в ACL явно разрешено”. Об этом правиле следует всегда помнить.

Для идентификации конкретного ACL всем его правилам присваивается некоторый одинаковый числовой номер (так называемые “нумерованные” ACL) или символьное имя (“именованные” ACL). Номер

или имя используются для ссылки на правила ACL как на единый объект. Далее рассматриваются только более распространенные нумерованные ACL.

Существует два вида списков доступа: стандартные (standard) ACL и расширенные (extended) ACL. Стандартные ACL более простые и содержат в правилах только адрес отправителя пакета, а расширенные – как адрес отправителя, так и адрес получателя, а также множество других контролируемых параметров.

Настройка списков доступа всегда состоит из двух этапов:

Этап 1. определения ACL, т.е. написания правил-шаблонов для сравнения;

Этап 2. активизации определенного ACL на заданном интерфейсе маршрутизатора. Пока второй шаг не выполнен, списки доступа никакого влияния на фильтрацию пакетов не оказывают.

7. Виды списков доступа

7.1. Стандартные списки доступа

Список доступа – это список строк-правил. Каждое правило стандартного списка ACL фильтрации IP-пакетов для маршрутизаторов Cisco вводится по команде (в глобальном режиме!):

access-list *номер ACL* **deny** | **permit** *адрес отправителя спец. маска адреса*

Здесь:

номер ACL – любой номер из диапазона **1…99** или **1300…1999**;

адрес отправителя – 32-битовый IP-адрес хоста или адрес подсети;

спец. маска адреса – 32-битовая маска специального для ACL вида. В этой маске цепочка нулей слева указывают на те биты *адреса отправителя*, которые должны обязательно проверяться на совпадение с этими же битами в адресе отправителя, а оставшиеся единицы маски указывают на те биты, для которых совпадение проверять не требуется.

Пара *адрес отправителя* и *спец.маска адреса* образуют адресный шаблон-правило для фильтрации проходящих пакетов через интерфейс. Если

адрес отправителя пакета совпадает с адресным шаблоном, то выполняется указанное в команде действие – запретить или разрешить. Если не совпадает, то команда игнорируется и анализируется следующая по порядку команда из данного ACL. Введение специальной маски адреса позволяет гибко формировать адресный шаблон для фильтрации, как отдельных IP-адресов, так и сразу группы адресов хостов. Примеры адресных шаблонов:

- ***192.168.15.22 0.0.0.0*** - должны проверяться все биты адреса на совпадение с указанным адресом.
- ***host 192.168.15.22*** - другая разрешенная и более наглядная форма записи шаблона, по действию подобная предыдущей.
- ***255.255.255.255*** - не требуется проверять никакие биты на совпадение, т.е. правилу соответствует любой адрес отправителя.
- ***any*** - “всякий”. Другая разрешенная и более наглядная форма записи шаблона, по действию подобная предыдущей.
- ***192.168.18.128 0.0.0.31*** - с данным шаблоном сравниваются все адреса из диапазона 192.168.18.128 – 192.168.18.159. В справедливости утверждения можно убедиться, представив адрес и маску в двоичном коде.

Команды определения списка доступа вводятся одна за другой, пока не будет сформирован весь ACL. Он может состоять и из одной команды. В конец ACL автоматически помещается неотображаемая команда:

access-list *номер ACL* **deny any**

Ранее введенные команды исправить невозможно; необходимо удалить весь ACL и ввести его заново.

Для активизации ACL его необходимо “присоединить” к желаемому интерфейсу маршрутизатора. Сначала надо войти в режим конфигурации этого интерфейса, затем выдать команду присоединения:

ip access-group *номер ACL* **in** | **out**

где: номер ACL - ссылка на номер активизируемого списка доступа;

in - требование фильтрации входящего (inbound) трафика;

out - фильтрация исходящего (outbound) от маршрутизатора трафика.

Для отмены фильтрации достаточно отменить команду присоединения, поставив перед ней ключевое слово **no**.

7.2. Расширенные списки доступа

Расширенные списки в принципе подобны стандартным, только содержат больше контролируемых параметров. Правило фильтрации IP-пакета для расширенного списка определяется следующим общим выражением:

access-list *номер ACL* **deny** | **permit** *протокол адр.шаблон отправ. адр.шаблон получат.* [*дополнит.спецификации протокола верхн.уровня*]

Здесь: *номер ACL* – любой номер из диапазона **100…199** или **2000…2699**;

протокол – один из протоколов **tcp** (**6**), **udp** (**17**), **icmp** (**1**), **ospf** (**89**), **ip** (**0**) и некоторые другие Internet-протоколы. Можно указывать или имя протокола или его числовой код (приведен в скобках). Если правило относится к любому протоколу, то указывается протокол **ip**.

адр.шаблон отправ. и *адр.шаблон получат.* – это пары *<адрес отправителя спец. маска адреса>* и *<адрес получателя спец.маска адреса>*. Работа с адресными шаблонами рассмотрена в предыдущем разделе;

дополнительные спецификации – зависят от конкретного протокола, указанного в поле *протокол*. Для **tcp**, **udp**, **icmp** эти спецификации приведены ниже.

Проходящий пакет проверяется на совпадение со всеми параметрами, указанными в текущем правиле. При полном совпадении выполняется, как обычно, предписанное в правиле действие. Если совпадения нет хотя бы с одним параметром, то данное правило игнорируется и рассматривается следующее.

В конец ACL автоматически так же помещается неотображаемая команда:

access-list *номер ACL* **deny ip any any**

Активизация расширенного списка производится такой же командой, какой активизируется стандартный ACL.

Остановимся на специфике определения правил ACL для фильтрации IP-пакетов с контролем параметров протоколов верхнего уровня **tcp**, **udp**, **icmp**, как наиболее важных и применяемых чаще других.

7.3. Применение в правилах ключевого слова tcp

access-list номер ACL **deny** | **permit tcp** *адр.шаблон отправ. [оператор порт отправ.] адр.шаблон получат. [оператор порт получат.]* [**established**]

Здесь:

порт отправ., *порт получат.* – TCP-порты отправителя и получателя. Порт можно указывать или символьным именем, или его числовым кодом (0-65535). Некоторые общеизвестные имена портов и их коды (в скобках): **ftp-data** (**20**) FTP-данные; **ftp** (**21**) FTP-управление; **telnet** (**23**) Telnet-сервер; **smtp** (**25**) Почтовый сервер; **domain** (**53**) Сервер DNS; **www** (**80**) Web-сервер;

оператор – один из операторов сравнения: **lt** (меньше, чем), **eq** (равно), **gt** (больше, чем), **neq** (не равно), **range** (для указания диапазона номеров портов, например, **range 20 21**);

established – ключевое слово, требующее проверки того, установлен ли бит **ack** (подтверждение) или **rst** (рестарт) в заголовке сегмента, проходящего в составе IP-пакета. Если TCP-соединение уже существует, то как известно, бит **ack** всегда установлен. Если соединение только запрашивается, то бит **ack** сброшен (установлен только бит **syn** - синхронизация счетчиков байтов).

7.4. Применение в правилах ключевого слова udp

Синтаксис команды ввода данного правила почти такой же, как и с параметром **tcp**:

access-list *номер ACL* **deny** | **permit udp** *адр.шаблон отправ.* [*оператор порт отправ.*] *адр.шаблон получат.* [*оператор порт получат.*]

В операторах сравнения порты здесь также можно указывать или символьным именем, или его числовым кодом (0-65535). Вот некоторые важные приложения, использующие протокол UDP, их общеизвестные имена портов и коды портов (в скобках): **tftp** (**69**) простой протокол передачи файлов; **snmp** (**161**) простой протокол управления в сети; **rip** (**520**) протокол динамической маршрутизации RIP.

7.5. Присвоение уникального номера каждому списку управления доступом

В процессе конфигурирования маршрутизатора каждому списку управления доступом необходимо присвоить индивидуальный номер; при назначении номера необходимо принимать во внимание диапазон номеров, который зарезервирован для данного протокола или стека. В примере 1 показаны стандартные списки управления доступом с номерами 1 и 2, которые привязываются к интерфейсу Ethernet 0.

Пример 1. Применение списков управления доступом к интерфейсу

```
access list 1 permit 5.6.0.0  0.0.255.255
access list 1 deny 7.9.0.0  0.0.255.255
!
access list 2 permit 1.2.3.4
access list 2 deny 1.2.0.0  0.0.255.255
!
interface ethernet 0
ip address 1.1.1.1  255.0.0.0
!
```

ip access-group 1 in
ip access-group 2 out

В таблице 3 перечислены наиболее часто используемые протокольные номера списков контроля доступа.

Таблица 3. Протокольные номера списков ACL

Протокол и тип списка	**Диапазон номеров**
Стандартные списки IP	1-99
Расширенные списки IP	100-199
Протокол AppleTalk	600-699
Стандартные списки IPX	800-899
Расширенные списки IPX	900-999
Протокол IPX SAP (Service Advertising Protocol — протокол извещения о службах)	1000-1099

7.6. Проверка списков управления доступом

Команда ***show ip interface*** отображает информацию об интерфейсах и показывает, установлены ли на них списки управления доступом. Результат выполнения этой команды приведен в примере 2. Обратите внимание на строки 9 и 10: для исходящего трафика интерфейса Ethernet 0 установлен список управления доступом с номером 10, для исходящих потоков данных списков нет.

Пример 2. Результат выполнения команды **show ip interface**

Router> show ip interface
Ethernet0 is up, line protocol is up
Internet address is 192.54.22.2, subnet mask is 255.255.255.0
Broadcast address is 255.255.255.255
Address determined by nonvolatile memory
MTU is 1500 bytes
Helper address is 192.52.71.4

Secondary address 131.152.115.2, subnet mask 255.255.255.0
Outgoing ACL is set
Inbound ACL is not set
Proxy ARP is enabled
Security 1eve1 is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
Gateway Discovery is disabled
IP accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Router>

Команда ***show access-lists*** отображает содержимое всех списков управления доступом. Если после двух указанных ключевых слов ввести имя или номер списка управления доступом в качестве параметра, то будет отображено содержимое конкретного списка ACL.

8. Преобразование сетевых адресов NAT

Network address translation (NAT - перенос сетевых адресов) создан для упрощения и сокрытия IP адресации. NAT позволяет представить внешнему миру внутреннюю структуру IP адресации предприятия иначе, чем она на самом деле выглядит. Это разрешает организации соединяться с Интернетом, не имея внутри себя глобальной уникальной IP адресации. Это даёт возможность выхода в Интернет для корпоративных внутренних IP сетей с внутренними IP адресами (intranet), которые глобально неуникальны и поэтому не могут маршрутизироваться в Интернете. NAT применяется также для связи территориально распределённых подразделений организации через Интернет.

Мировым сообществом для Интранет адресации выделены следующие диапазоны адресов:

- Class A: 10.0.0.0-10.255.255.255
- Class B: 172.16.0.0-172.16.255.255
- Class C: 192.168.1-192.168.255.255

NAT переводит внутренний IP адрес из внутреннего адресного пространства в IP адрес во внешнем адресном пространстве. Когда NAT получает пакет из intranet, он изменяет в нём адрес источника, пересчитывает контрольную сумму и отправляет его в Интернет.

NAT преобразует и отображает адреса из одной области в другую. Это обеспечивает прозрачную маршрутизацию от узла к узлу. В NAT существует несколько способов трансляции адресов, используемых в различных частных случаях.

При отправке пакетов от интерфейса внутреннего хоста NAT заменяет в нём адрес источника на некоторый глобальный адрес. При приёме ответного пакета NAT заменяет в нём глобальный адрес приёмника (адрес внешнего интерфейса локального маршрутизатора) на адрес интерфейса внутреннего хоста. Для такой замены маршрутизатор поддерживает специальные таблицы преобразований адресов, которые постоянно обновляются. Различают три способа преобразования адресов: *статический, динамический* и *перегрузка* (overload). При статическом NAT в явном виде с помощью команд IOS задаются пары внутренний_адрес - глобальный _адрес. При динамическом преобразовании глобальные адреса берутся из определённого пула внешних адресов. При перегрузке все внутренние адреса, подлежащие преобразованию, заменяются на единственный глобальный адрес внешнего интерфейса маршрутизатора.

Для конфигурирования NAT следует определить на маршрутизаторе внутренние и внешние сети с помощью команд **ip nat inside | outside**. Эти командs определяются на уровне интерфейсов, то есть в контексте команды

interface. Дополнительные команды зависят от используемого типа NAT. Это либо задание статического NAT, либо определение пула внешних адресов либо задание команды для перегрузки. Как правило, следует также задать список управления доступом ACL для определения внутреннего трафика, который будет преобразовываться. Сам по себе ACL не осуществляет никакого NAT преобразования.

Процесс NAT прозрачен для внутренних адресов. Так хост с внутренним адресом, отправивший пакет во внешний мир и получивший ответ «не догадывается», что пакет прошел NAT преобразование на маршрутизаторе, как при отправке, так и при приёме. Внутреннему хосту представляется, что он имеет непосредственный выход во внешний мир.

8.1. Конфигурация статической трансляции

Для конфигурации статической трансляции необходимо выполнить следующие действия:

1) Установить режим статической трансляции между внутренним локальным адресом и внутренним глобальным адресом:
   ip nat inside source static <локальный адрес> <глобальный адрес>
2) Указать внутренний интерфейс: ***interface*** <тип> <номер>
3) Пометить данный интерфейс, как принадлежащий внутренней сети
   ip nat inside
4) Указать внешний интерфейс: ***interface*** <тип> <номер>
5) Пометить данный интерфейс, как принадлежащий внешней сети:
   ip nat outside

8.2. Конфигурация динамической трансляции

Для конфигурации динамической трансляции необходимо выполнить следующие действия:

1) Определить пул глобальных адресов:

ip nat pool <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]

2) Определить стандартный список доступа, регламентирующий адреса, подлежащие трансляции:
   access-list <номер> permit <адрес или блок адресов>
3) Установить динамическую трансляцию на основе списка доступа, определенного на предыдущем шаге:
   ip nat inside source list <номер списка доступа> pool <имя>
4) Указать внутренний интерфейс: ***interface*** <тип> <номер>
5) Пометить данный интерфейс, как принадлежащий внутренней сети:
   ip nat inside
6) Указать внешний интерфейс: ***interface*** <тип> <номер>
7) Пометить данный интерфейс, как принадлежащий внешней сети:
   ip nat outside

Представленный ниже пример транслирует все адреса узлов-источников, определенных списком доступа 1 (разрешены адреса от 192.168.1.0/24), в пул адресов, названный nrt-208. Этот пул содержит адреса с 171.69.233.208 по 171.69.233.233.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

8.3. Использование одного внутреннего глобального адреса

Существует возможность экономии пула внутренних глобальных адресов путем разрешения маршрутизатору использовать один глобальный адрес для трансляции нескольких локальных адресов. Если используется такой вариант конфигурации, то маршрутизатор использует информацию протоколов более высокого уровня (например, TCP и UDP) для обратной трансляции глобального адреса в корректные локальные адреса. При использовании соответствия нескольких локальных адресов одному глобальному адресу номера портов TCP или UDP каждого внутреннего узла указывают на локальные адреса этих узлов.

Для конфигурирования режима использования одного внутреннего глобального адреса необходимо выполнить следующие шаги:

1) Определить пул глобальных адресов:
   ip nat pool <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]
2) Определить стандартный список доступа:
   access-list <номер> permit <внутренний адрес или блок адресов>
3) Установить режим динамической трансляции адресов, разрешенных в списке доступа, определенном на предыдущем шаге:
   ip nat inside source list <номер списка доступа> pool <имя> overload
4) Указать внутренний интерфейс: ***interface*** <тип> <номер>
5) Пометить данный интерфейс, как принадлежащий внутренней сети:
   ip nat inside
6) Указать внешний интерфейс: ***interface*** <тип> <номер>
7) Пометить данный интерфейс, как принадлежащий внешней сети:
   ip nat outside

Представленный ниже пример создает пул адресов, называемый net-208. Данный пул содержит адреса с 171.69.233.208 по 171.69.233.233. Список

доступа 1 разрежает пакеты, имеющие адреса отправителя с 192.168.1.0 по 192.168.1.255. Если в данный момент не производится процедура трансляции, то адреса в пакетах, соответствующих условиям списка доступа 1, транслируются в адрес из указанного пула. Маршрутизатор позволяет нескольким внутренним адресам использовать один глобальный адрес. Для определения того или иного соединения маршрутизатор использует номера портов.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask
255.255.255.240
ip nat inside source list 1 pool net-208 overload
!
interface serial0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

8.4. Мониторинг и сопровождение NAT

По умолчанию таблица динамической трансляции адресов со временем очищается автоматически. Однако, имеется возможность проведения работ по мониторингу и сопровождению NAT с консоли управления маршрутизатором:

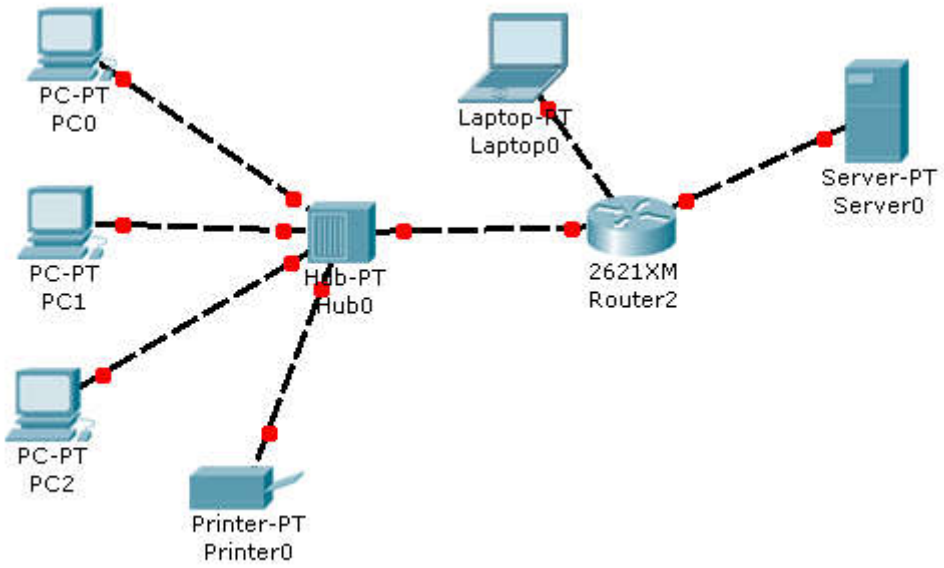
- Очистить все записи динамической трансляции адресов из таблицы NAT: ***clear*** *ip nat translation* *
- Очистить простую запись динамической трансляции, содержащей информацию либо о внутренней трансляции, либо о внутренней и внешней трансляции:

clear *ip nat translation inside <глобальный адрес> <локальный адрес> [outside <локальный адрес> <глобальный адрес>]*

- Очистить простую запись динамической трансляции, содержащую информацию о внешней трансляции:
  clear *ip nat translation outside <локальный адрес> <глобальный адрес>*
- Очистить расширенную запись динамической трансляции:
  clear *ip nat translation <протокол> inside <глобальный адрес> <глобальный порт> <локальный адрес> <локальный порт> [outside <локальный адрес> <локальный порт> <глобальный адрес> <глобальный порт>]*

9. 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:
   2.1. Запретить ping из внешней сети.
   2.2. Запретить доступ из внешней сети к принтеру, размещенному во внутренней сети.
   2.3. Разрешить одному из ПК внутренней сети доступ к внешнему фтп-серверу.
   2.4. Разрешить одному из ПК внутренней сети доступ к внешнему mail-серверу.
   2.5. Запретить icmp трафик из внутрисети.
   2.6. Разрешить доступ из внутрисети ко внешнему WEB-серверу для всех ПК.
3. Выполнить настройку статической, динамической и динамической трансляции с использованием одного глобального адреса:
   3.1. 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.

3.2.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.

3.3. 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.

10.Результаты работы

Лабораторная работа выполняется индивидуально каждым студентом, либо группой по 2-3 человека.

В результате выполненной лабораторной работы студенты должны предоставить преподавателю отчет о проделанной работе в электронном виде, в котором будут присутствовать ”скриншоты” иллюстрирующие все задания лабораторной работы, с подробными описаниями.

Отвечая на вопросы преподавателя, студенты должны уверенно ориентироваться в изученном материале.