**Практическая работа № 5**

**Настройка межсетевого взаимодействия узлов сети**

Цель работы: ознакомиться с настройкой сетевого оборудования фирмы Cisco, реализовать службу NAT.

**Краткие теоретические сведения об операционной системе Cisco IOS**

Для настройки сетевого оборудования в вашем распоряжении имеются разнообразные команды операционной системы Cisco IOS.

При входе в сетевое устройство командная строка имеет вид:

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#

Выход из привилегированного режима:

Switch# **disable**

Switch>

О переходе в привилегированный 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, подъинтерфейса, линии, сетевого устройства, карты маршрутов и т.п.

Для выхода из системы IOS необходимо набрать на клавиатуре команду exit (выход):

Switch> **exit**

Возможна работа в следующих режимах:

- 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:

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:

Switch#

- Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В том режиме приглашение имеет вид:

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 переходу 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(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**

**Практическое знакомство с Cisco IOS**

**Основные команды сетевого устройства**

1. Войдите сетевое устройство Router1

Router>

2. Мы хотим увидеть список всех доступных команд в этом режиме. Введите

команду, которая используется для просмотра всех доступных команд:

Router>**?**

Клавишу Enter нажимать не надо.

3. Теперь войдите в привилегированный режим

Router>**enable**

Router#

4. Просмотрите список доступных команд в привилегированном режиме

Router#**?**

5. Перейдём в режим конфигурации

Router#**config terminal**

Router(config)#

6. Имя хоста сетевого устройства используется для локальной идентификации.

Когда вы входите в сетевое устройство, вы видите Имя хоста перед символом режима (">" или "#"). Это имя может быть использовано для определения места нахождения.

Установите "Router1" как имя вашег сетевого устройства.

Router(config)#**hostname Router1**

Router1(config)#

7. Пароль доступа позволяет вам контролировать доступ в привилегированный

режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступу "parol".

Router1(config)#**enable password parol**

1. Давайте испытаем этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.

Router1>**en**

Password:**\*\*\*\*\***

Router1#

Здесь знаки: \*\*\*\*\* - это ваш ввод пароля. Эти знаки на экране не видны.

**Основные Show команды.**

Перейдите в пользовательский режим командой disable. Введите команду для просмотра всех доступных show команд.

Router1>**show ?**

1. Команда show version используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

2. Просмотр времени:

Router1>**show clock**

3. Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы Cisco IOS. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

Router1>**show flash**

4. ИКС сетевого устройства по умолчанию сохраняет10 последних введенных команд

Router1>**show history**

5. Две команды позволят вам вернуться к командам, введённым ранее. Нажмите на стрелку вверх или <ctrl> P.

6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере.

Нажмите на стрелку вниз или <ctrl> N

7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов

Router1>**show hosts**

8. Следующая команда выведет детальную информацию о каждом интерфейсе

Router1>**show interfaces**

9. Следующая команда выведет информацию о каждой telnet сессии:

Router1>**show sessions**

10. Следующая команда показывает конфигурационные параметры терминала:

Router1>**show terminal**

11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям:

Router1>**show users**

12. Команда

Router1>**show controllers**

показывает состояние контроллеров интерфейсов.

13. Перейдём в привилегированный режим.

Router1>**en**

14. Введите команду для просмотра всех доступных show команд.

Router1#**show ?**

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте следующие команды:

сохранение текущей конфигурации:

Router# **write memory**

Или

Router# **copy run start**

Просмотр сохраненной конфигурации:

Router# **Show configuration**

или

Router1#**show running-config**

В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.

16. Следующая команда позволит вам увидеть текущее состояние протоколов

третьего уровня:

Router#**show protocols**

**Введение в конфигурацию интерфейсов**

Рассмотрим команды настройки интерфейсов сетевого устройства.

На сетевом устройстве Router1 войдём в режим конфигурации:

Router1#**conf t**

Router1( config)#

2. Теперь ми хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:

Router1(config)#**interface FastEthernet0/0**

Router1( config-if)#

3. Посмотрим все доступные в этом режиме команды:

Router1(config-if)#**?**

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса:

Router1(config)#**int fa0/0**

Мы использовали сокращенное имя интерфейса.

4. Для каждой команды мы можем выполнить противоположную команду, поставивши перед ней слово no. Следующая команда включает этот интерфейс:

Router1(config-if)#**no shutdown**

5. Добавим к интерфейсу описание:

Router1(config-if)#**description Ethernet interface on Router 1**

Чтобы увидеть описание этого интерфейса, перейдите в привилегированный

режим и выполните команду show interface :

Router1(config-if)#**end**

Router1#**show interface**

6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2:

Router#**conf t**

Router(config)#**hostname Router2**

Войдём на интерфейс FastEthernet 0/0:

Router2(config)#**interface fa0/0**

Включите интерфейс:

Router2(config-if)#**no shutdown**

Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1.

Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством DTE (data terminal equipment), либо устройством связи DCE (data circuit):

Router1#**show controllers fa0/1**

Если видим сообщение:

DCE cable

то наш маршрутизатор является устройством связи и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.

Router1#**conf t**

Router1(config)#**int fa0/1**

Router1(config-if)#**clock rate ?**

Выберем частоту 64000

Router1(config-if)#**clock rate 64000**

и включаем интерфейс

Router1(config-if)#**no shut**

**Краткие теоретические сведения о NAT**

NAT (Network Address Translation) − трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах.

NAT используется чаще всего для осуществления доступа устройств из сети предприятия(дома) в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети.

Сеть предприятия обычно строится на частных IP адресах. Согласно RFC 1918 под частные адреса выделено три блока:

10.0.0.0 − 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 − 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 − 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей.

Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

Помимо возможности доступа во внешнюю сеть (Интернет), NAT имеет ещё несколько положительных сторон. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. А ещё эта технология позволяет экономить Глобальные IP адреса, так как под одним глобальным адресом в Интернет может выходить множество хостов.

Настройка NAT на маршрутизаторах Cisco под управлением IOS включает в себя следующие шаги

1. Назначить внутренний (Inside) и внешний (Outside) интерфейсы

Внутренним интерфейсом обычно выступает тот, к которому подключена локальная сеть. Внешним − к которому подключена внешняя сеть, например сеть Интернет провайдера.

2. Определить для кого (каких ip адресов) стоит делать трансляцию.

3. Выбрать какой вид трансляции использовать

4. Осуществить проверку трансляций

Существует три вида трансляции Static NAT, Dynamic NAT, Overloading (PAT).

Static NAT − Статический NAT, преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети.

Dynamic NAT − Динамический NAT, преобразование внутреннего адреса/ов в один из группы внешних адресов. Перед использованием динамической трансляции, нужно задать nat-пул внешних адресов

Overloading − позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому иногда такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

Список команд для настройки NAT:

обозначение Интернет интерфейса:

interface FastEthernet0/0

ip nat outside

обозначение локального интерфейса:

interface Vlan1

ip nat inside

создание списка IP, имеющего доступ к NAT:

ip access-list extended NAT

permit ip host 192.168.???.??? any

включение NAT на внешнем интерфейсе:

ip nat inside source list NAT interface FastEthernet0/0 overload

Посмотреть существующие трансляции можно командой "show ip nat translations".

Отладка запускается командой "debug ip nat"

Настройка Static NAT

router(config)#ip nat inside source static <local-ip> <global-ip>

router(config)#interface fa0/4

router(config-if)#ip nat inside

router(config)#interface fa0/4

router(config-if)#exit

router(config)#interface s0

router(config-if)#ip nat outside

Настройка Dynamic NAT

router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}

router(config)#access-list <acl-number> permit <source-IP> [source-wildcard]

router(config)#ip nat inside source list <acl-number> pool <name>

router(config)#interface fa0/4

router(config-if)#ip nat inside

router(config-if)#exit

router(config)#interface s0

router(config-if)#ip nat outside

Настройка Overloading

router(config)#access-list acl-number permit source-IP source-wildcard

router(config)#ip nat inside source list acl-number interface interface overload

router(config)#interface fa0/4

router(config-if)#ip nat inside

router(config-if)#exit

router(config)#interface s0

router(config-if)#ip nat outside

**Практическая реализация службы NAT**

Необходимо решить задачу вывода компьютеров локальной сети организации в интернет. Локальная сеть настроена в частной адресации – в сети 10.0.0.0, адреса которой не имеют выхода в интернет. Для решения этой задачи необходимо настроить службу NAT. Схема сети представлена на рис.3.1.

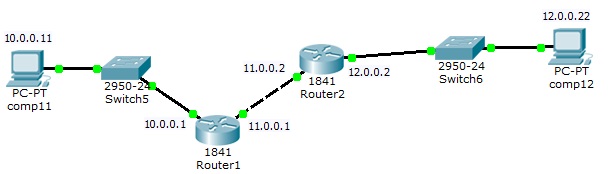


Рис. 3.1 − Схема сети

Создайте сеть, представленную на рис.3.1. Задайте имена устройств и адресацию, как показано на рисунке.

В данный момент NAT на роутере не настроен, мы можем убедиться в этом, используя режим симуляции.

Перейдите в этот режим и посмотрите состав пакета при прохождении через оба роутера (рис. 3.2).

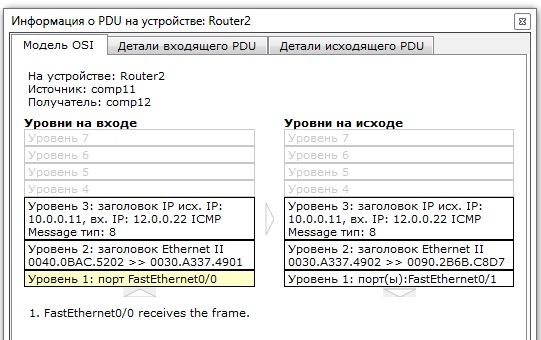


Рис.3.2 − Параметры пакета при прохождении Router2

При прохождении пакета через второй маршрутизатор IP адрес отправителя не изменился (10.0.0.11).

Сконфигурируем NAT на маршрутизаторе Router1.

Для настройки NAT на роутере нам необходимо будет выполнить следующие шаги:

1. зайти в настройки Router1, во вкладку CLI
2. для входа в режим администратора ввести команду enable (en)

Router>**en**

Для входа в режим настройки вводим команду config t

Router#**config t**

1. Интерфейс FastEthernet 0/0 наш внутренний интерфейс, к которому подключены рабочие станции. Для настройки NAT на роутере необходимо это обозначить в настройках. Это можно сделать при помощи следующих команд:

входим в настройки интерфейса:

Router(config)#**int** **FastEthernet 0/0**

объявляем интерфейс внутренним интерфейсом:

Router(config-if)#**ip nat inside**

выходим из настроек интерфейса

Router(config-if)#**exit**

1. Аналогично настраиваем интерфейс FastEthernet 0/1, который подключен к сети провайдера, лишь с тем различием, что он будет являться внешним интерфейсом NAT:

входим в настройки интерфейса:

Router(config)#**int FastEthernet 0/1**

объявляем интерфейс внешним интерфейсом NAT:

Router(config-if)#**ip nat outside**

выходим из настроек интерфейса:

Router(config-if)#**exit**

1. Задаем пул внешних адресов, в которые будут транслироваться внутренние адреса. Для задания пула, содержащего только один адрес – адрес внешнего интерфейса роутера - необходимо ввести команду:

Router(config)#**ip nat pool natpool 11.0.0.0 11.0.0.1 netmask 255.0.0.0**

При задании пула адресов необходимо указать первый и последний адреса из входящей в пул последовательности адресов. Если в пуле 1 необходимо указать его 2 раза.

1. Задаем список доступа:

Router(config)#**access-list 34 permit any**

**Важно**: 34 – число от 1 до 99 обозначает № списка доступа и задается администратором. Any – ключевое слово, означает, что список доступа будет разрешать пакеты с любым адресом отправителя.

1. Наконец вводим последнюю команду, которая, собственно, и включает NAT на Router0. Команда, бесспорно, является основной, но без задания всех предыдущих параметров она работать не будет.

Router(config)#**ip nat inside source list 34 pool natpool overload**

Данная команда говорит роутеру, что у всех пакетов, полученных на внутренний интерфейс и разрешенных списком доступа номер 34, адрес отправителя будет транслирован в адрес из NAT пула “natpool”. Ключ overload указывает, что трансляции будут перегружены, позволяя нескольким внутренним узлам транслироваться на один IP адрес.

Теперь NAT настроен. Можем убедиться в этом послав пакет из любой рабочей станции в подсети на сервер yandex.ru (пакет пройдет). Если мы рассмотрим прохождение пакета подробнее, перейдя в режим симуляции, то увидим, что при прохождении пакета через Router1 адрес отправителя изменился(NAT настроен).

**Контрольные вопросы**

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение вилланов по портам коммутатора?
5. Перечислите основные режимы конфигурации при настройке коммутатора.
6. Перечислите основные режимы конфигурации при настройке роутера.
7. Как посмотреть таблицу маршрутизации на роутере?
8. Какие команды формируют таблицу маршрутизации роутера?
9. Какими командами настраиваются вилланы на коммутаторе?
10. Какими командами настраивается взаимодействие между вилланами?
11. Опишите все возможные схемы работы службы NAT.
12. Какие частные IP адреса используются службой NAT в каждом классе адресов?
13. Перечислите преимущества и недостатки службы NAT.
14. Перечислите этапы настройки службы NAT.
15. Опишите схему проверки работы службы NAT.
16. Опишите основные проблемы в работе сервера NAT.