



Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ИУК «Информатика и управление»

КАФЕДРА ИУК4 «Программное обеспечение ЭВМ и информационные технологии»

ДОМАШНЯЯ РАБОТА №1

ДИСЦИПЛИНА: «Компьютерные сети и интернет технологии»

Выполнил: студент гр. ИУК4-62Б

(Подпись)

(Губин Е.В.)
(Ф.И.О.)

Проверил:

(Подпись)

(Прудяк П.Н.)
(Ф.И.О.)

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:

- Оценка:

Калуга , 2025

Цель: формирование практических навыков работы с сетевыми адаптерами.

Задачи:

1. Создание компьютерной сети в рабочей области логической топологии
2. Настройка на компьютерах и локальном сервере ip-адресов
3. Создание сегментов локальной сети посредством vlan на коммутаторе и sub-интерфейсов на маршрутизаторе
4. Подключение локальной сети к провайдеру
5. Настройка перегруженного NAT
6. Настройка access-листа
7. Настройка статического NAT

Результат выполнения работы:

Для начала расставим все необходимые элементы как показано на рисунке 1

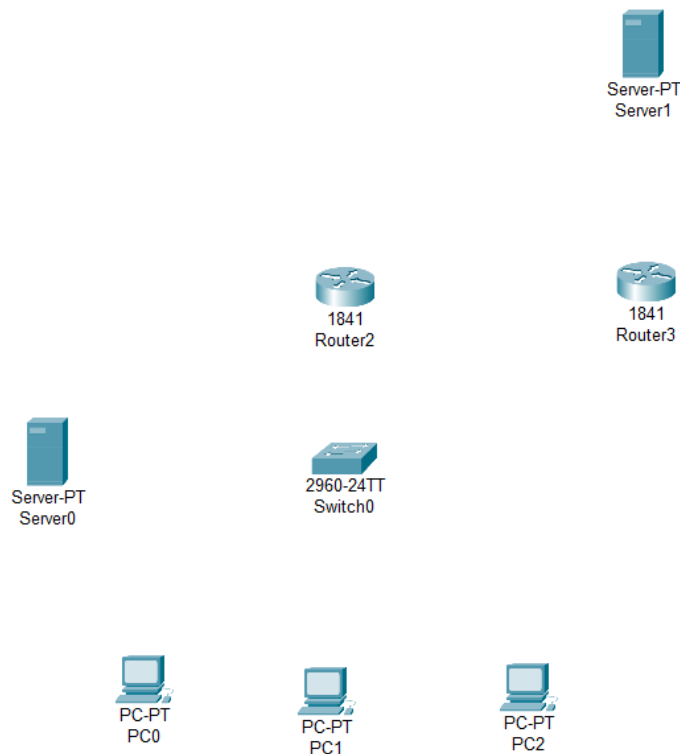


Рис.1 – «Схема расположения элементов в сети»

Сеть будет состоять из трех компьютеров, сервера, коммутатора 2960 и маршрутизатора 1841. Для имитации провайдера и выхода в интернет добавим сервера и маршрутизатор 1841.

Создадим два сегмента сети. Компьютеры определим во vlan 2, сервер определим во vlan 3.

Настроим коммутатор. Создадим vlan 2 и vlan 3 (см. рисунок 2)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name users
Switch(config-vlan)#exit
Switch(config)#^
% Invalid input detected at '^' marker.

Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name server
Switch(config-vlan)#exit
Switch(config)#
```

Рис.2 – «Создание vlan 2, vlan 3»

Подключим компьютеры к портам коммутатора fa0/1, fa0/2, fa0/3 и настроим эти порты во vlan 2 (рисунок 3)

```
Switch(config)#int range Fa0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#
```

Рис.3 – «Подключение портов коммутатора к vlan 2»

Далее подключим сервер к порту коммутатора fa0/4 и определим этот порт во vlan 3, как показано на рисунке 4

```
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 3
```

Рис.4 – «Подключение порта коммутатора к vlan3»

Так же подключим маршрутизатор к порту коммутатора fa0/5 и настроим его как trunk-порт (рисунок 5)

```
Switch(config)#int Fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#exit
```

Рис.5 – «Настройка trunk-порта»

Теперь необходимо настроить маршрутизатор. Проверим, к какому порту подключен маршрутизатор к коммутатору – fa0/0. Поднимем интерфейс (см. рисунок 6)

```
Router(config)#int Fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
```

Рис.6 – «Настройка интерфейса fa0/0 маршрутизатора»

Создадим также sub-интерфейс для vlan 2 и vlan 3 (см. рисунок 7, 8)

```
Router(config)#int fa0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 10.11.25.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Рис.7 – «Настройка суб-интерфейса vlan2»

```
Router(config)#int fa0/0.3
Router(config-subif)#ip address 10.11.26.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Рис.8 – «Настройка суб-интерфейса vlan3»

Настроим Ip-адрес, маску и шлюз для компьютера PC0 (см. рисунок 9)

IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	10.11.8.2
Subnet Mask	255.255.255.0
Default Gateway	10.11.8.1
DNS Server	0.0.0.0

Рис.9 – «Настройка компьютера PC0»

Такую же настройку проведем для PC1, PC2 и Server0 (рисунок 10, 11, 12 соответственно)

IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	10.11.8.3
Subnet Mask	255.255.255.0
Default Gateway	10.11.8.1
DNS Server	0.0.0.0

Рис.10 – «Настройка компьютера PC1»

IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	10.11.8.4
Subnet Mask	255.255.255.0
Default Gateway	10.11.8.1
DNS Server	0.0.0.0

Рис.11 – «Настройка компьютера PC2»

IP Configuration	
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	10.11.9.2
Subnet Mask	255.255.255.0
Default Gateway	10.11.9.1
DNS Server	0.0.0.0

Рис.12 – «Настройка компьютера Server0»

Проверим связь компьютера PC0 со шлюзом, другими компьютерами и сервером. Связь есть (см. рисунок 13)

```

C:\>ping 10.11.26.2

Pinging 10.11.26.2 with 32 bytes of data:

Request timed out.
Reply from 10.11.26.2: bytes=32 time<1ms TTL=127
Reply from 10.11.26.2: bytes=32 time<1ms TTL=127
Reply from 10.11.26.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.11.26.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.11.25.3

Pinging 10.11.25.3 with 32 bytes of data:

Reply from 10.11.25.3: bytes=32 time<1ms TTL=128
Reply from 10.11.25.3: bytes=32 time<1ms TTL=128
Reply from 10.11.25.3: bytes=32 time<1ms TTL=128
Reply from 10.11.25.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.11.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.11.25.1

Pinging 10.11.25.1 with 32 bytes of data:

Reply from 10.11.25.1: bytes=32 time<1ms TTL=255
Reply from 10.11.25.1: bytes=32 time<1ms TTL=255
Reply from 10.11.25.1: bytes=32 time<1ms TTL=255
Reply from 10.11.25.1: bytes=32 time=8ms TTL=255

Ping statistics for 10.11.25.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

```

Рис.13 – «Проверка работы локальной сети»

Мы настроили локальную сеть. Теперь необходимо настроить доступ к сети Интернет, симулировав провайдера посредством роутера и сервера, приняв, что провайдер нам выделил статический IP адрес.

Предположим, что на маршрутизаторе провайдера интерфейсу fa0/0 соответствует ip-адрес

Настроим маршрутизатор провайдера, как показано на рисунке 14

```

Router(config)#int fa0/0
Router(config-if)#ip address 195.111.62.91 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

```

Рис.14 – «Настройка порта fa0/0 маршрутизатора провайдера»

Сервер провайдера подключен к маршрутизатору через порт fa0/1, сконфигурируем его, как показано на рисунке 15

```

Router(config-if)#int fa0/1
Router(config-if)#ip address 195.111.72.91 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

```

Рис.15 – «Настройка порта fa0/1 маршрутизатора провайдера»

Настроим ip-адрес, маску и шлюз для сервера провайдера (рисунок 16)

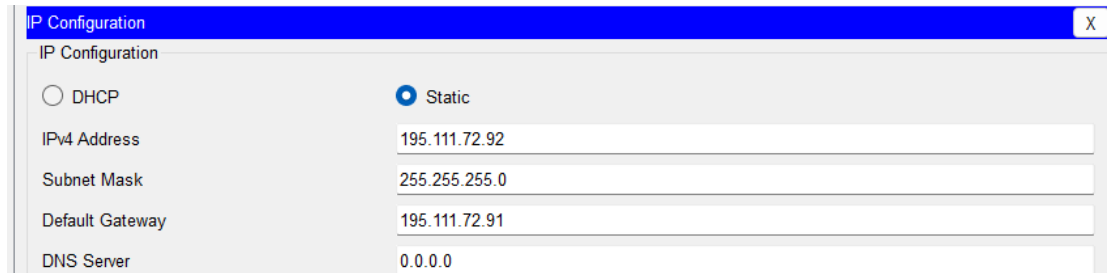


Рис.9 – «Настройка компьютера Server1 провайдера»

Далее необходимо на маршрутизаторе сети предприятия для интерфейса fa0/1 прописать ip-адрес, который нам выделил провайдер (см. рисунок 17)

```
Router(config)#int fa0/1
Router(config-if)#ip address 192.111.62.92 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
```

Рис.9 – «Настройка порта fa0/1 маршрутизатора сети»

Добавим шлюз по умолчанию через ip-адрес провайдера (рисунок 18)

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.111.62.91
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
```

Рис.9 – «Настройка шлюза по умолчанию маршрутизатора сети»

Проверим связь с провайдером и доступность сервера провайдера (см. рисунок 19)

```
Router#ping 195.111.62.91

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.111.62.91, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 195.111.72.92

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.111.72.92, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Рис.9 – «Проверка связи с сервером провайдера»

Теперь попробуем проверить связь компьютера PC0 с сервером провайдера (рисунок 20)


```

C:\>ping 195.111.72.2

Pinging 195.111.72.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 195.111.72.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Рис.20 – «Проверка связи PC0 с сервером провайдера»

Связи нет, так как в сети используются «серые» адреса и маршрутизатор провайдера ничего не знает об этой сети. Обеспечим нашим компьютерам выход в интернет с помощью технологии NAT.

Вернемся к настройке маршрутизатора сети предприятия (router5). Интерфейс fa0/1 для NAT будет являться внешним, а интерфейсы fa0/0.2, fa0/0.3 будут для NAT внутренними (см. рисунок 21)

```

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/0.2
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.3
Router(config-subif)#ip nat inside
Router(config-subif)#end
Router#

```

Рис.21 – «Настройка интерфейсов для NAT»

Теперь нужно создать access-листы, которые будут характеризовать, какой именно трафик мы будем проводить через NAT. Создадим access-лист с именем FOR-NAT с указанием сетей, как показано на рисунке 22

```

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#permit 10.11.25.0 0.0.0.255
Router(config-std-nacl)#permit 10.11.26.0 0.0.0.255
Router(config-std-nacl)#end

```

Рис.22 – «Настройка access-листа»

Добавим NAT возможность проводить с инсайда с использованием access-листа, когда трафик проходит через интерфейс fa0/1 (рисунок 23)

```

Router(config)#ip nat inside source list FOR-NAT int fa0/1 overload
Router(config)#end
Router#

```

Рис.23 – «Добавление возможности проводить трафик»

Проверим доступ к серверу провайдера с PC0 – видим, что связь есть (см. рисунок 24)

```
C:\>ping 195.111.72.92

Pinging 195.111.72.92 with 32 bytes of data:

Request timed out.
Reply from 195.111.72.92: bytes=32 time<1ms TTL=126
Request timed out.
Reply from 195.111.72.92: bytes=32 time<1ms TTL=126

Ping statistics for 195.111.72.92:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис.24 – «Проверка доступа PC0 к серверу провайдера»

Можем посмотреть наши обращения через маршрутизатор router 5 (рисунок 25)

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 195.111.62.92:89    10.11.25.2:89    195.111.72.92:89  195.111.72.92:89
```

Рис.25 – «Список обращений через локальный маршрутизатор»

Проверим связь между сервером в сети и сервером провайдера (рисунок 26)

```
C:\>ping 195.111.72.92

Pinging 195.111.72.92 with 32 bytes of data:

Request timed out.
Reply from 195.111.72.92: bytes=32 time<1ms TTL=126
Request timed out.
Reply from 195.111.72.92: bytes=32 time<1ms TTL=126

Ping statistics for 195.111.72.92:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис.26 – «Проверка связи между сервером сети и локальным сервером»

Мы настроили PAT. Далее настроим статический NAT, то есть обеспечим доступ к нашему локальному серверу из внешней сети.

Перейдем в конфигурацию сервера, выберем http, откроем index.html и заменим сайт Cisco Packet Tracer на BMSTU. Нужно сделать так, чтобы обращение из внешней сети к нашему маршрутизатору транслировалось на наш локальный веб-сервер.

Настроим статический NAT. Для этого вернемся в настройки маршрутизатора (см. рисунок 27)

```
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#ip nat inside source static tcp 10.11.26.2 80 195.111.62.92 80  
Router(config)#end  
Router#
```

Рис.27 – «Настройка локального маршрутизатора для статического NAT»

Попробуем зайти в настройки внешнего сервера и набрать в браузере ip-адрес внешнего интерфейса маршрутизатора (см. рисунок 28).

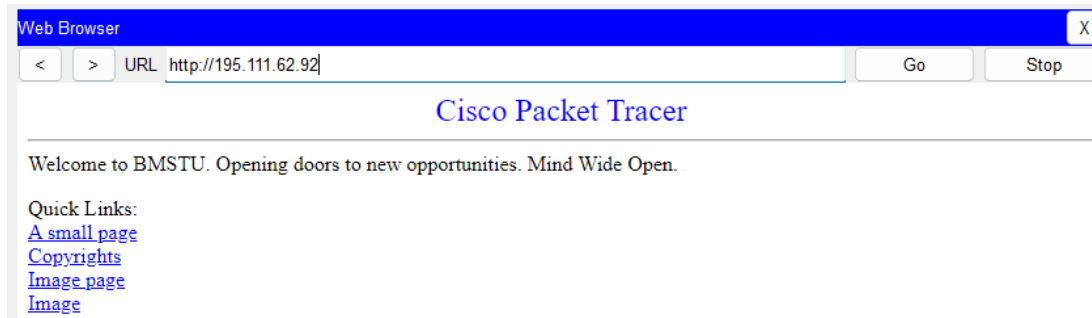


Рис.28 – «Проверка связи внешнего сервера и сервера локальной сети»

Видим веб-страницу нашего локального сервера, при этом наш сервер не имеет «белого» ip-адреса. Таким образом, мы настроили статический NAT.

Конечная схема сети выглядит следующим образом (рисунок 29)

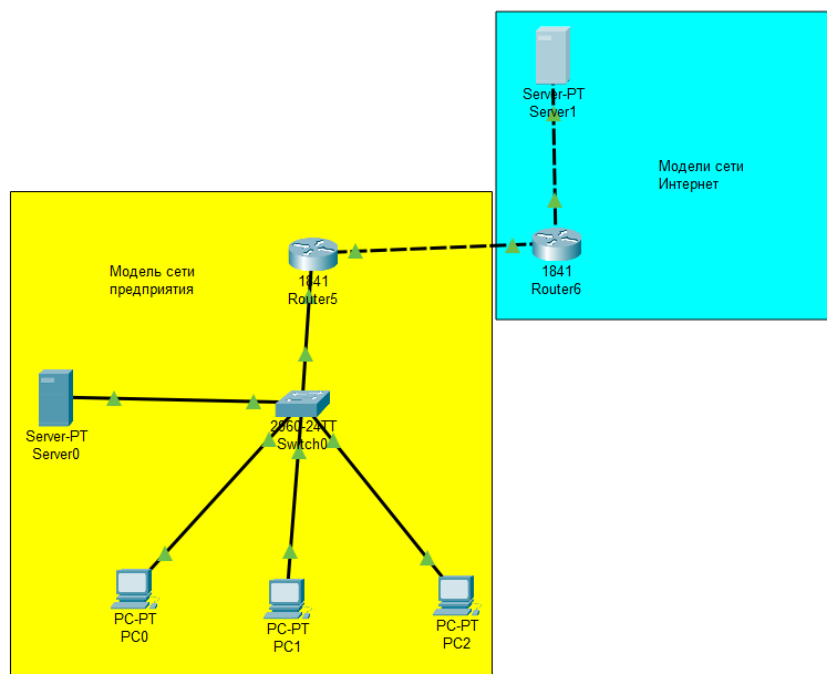


Рис.29 – «Схема конечной сети»

Вывод: таким образом, в ходе выполнения лабораторной работы были сформированы практические навыки работы с сетевыми адаптерами.

Ответы на контрольные вопросы.

1. Классификация видов NAT:

1. Static NAT (Статический NAT) – отображение одного IP-адреса в другой. Постоянное соответствие между публичным и частным IP.
2. Dynamic NAT (Динамический NAT) – назначение публичного IP-адреса для частного IP из пула адресов, что позволяет использовать множество частных адресов с ограниченным числом публичных.
3. PAT (Port Address Translation) – вид динамического NAT, который отображает множество частных IP-адресов на один публичный, различая их по номеру порта (NAT с трансляцией портов).

2. Входящий и исходящий трафик:

1. Исходящий трафик – это данные, которые отправляются с устройства в сеть (например, запросы от клиента на сервер).
2. Входящий трафик – это данные, которые поступают на устройство из сети (например, ответы сервера на запросы клиента).

3. Способы применения ACL (Access Control Lists):

1. Ограничение доступа к определённым ресурсам сети (например, блокировка доступа к портам, протоколам или IP-адресам).
2. Защита от несанкционированных подключений.
3. Реализация политик безопасности на маршрутизаторах и коммутаторах.
4. Фильтрация трафика на основе IP-адресов, портов и протоколов.

4. Пример записи ACL:

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 any  
access-list 101 deny ip any any
```

Эта запись разрешает трафик от сети 192.168.1.0/24 к любому адресу и запрещает все остальные подключения.

5. Способы подключения к маршрутизатору:

1. Через консольный порт (используя консольный кабель и терминальное ПО).
2. Через SSH (Secure Shell) для удалённого управления.
3. Через Telnet (менее безопасный вариант).
4. Через Web-интерфейс (например, если поддерживается HTTP/HTTPS интерфейс управления).

6. Вариант настройки Static NAT:

```
ip nat inside source static 192.168.1.10 203.0.113.5
```

В этом примере частный IP-адрес 192.168.1.10 будет отображаться как публичный IP-адрес 203.0.113.5.