

Практическая работа № 8

Комплексная работа и настройка Nat.

Задание.

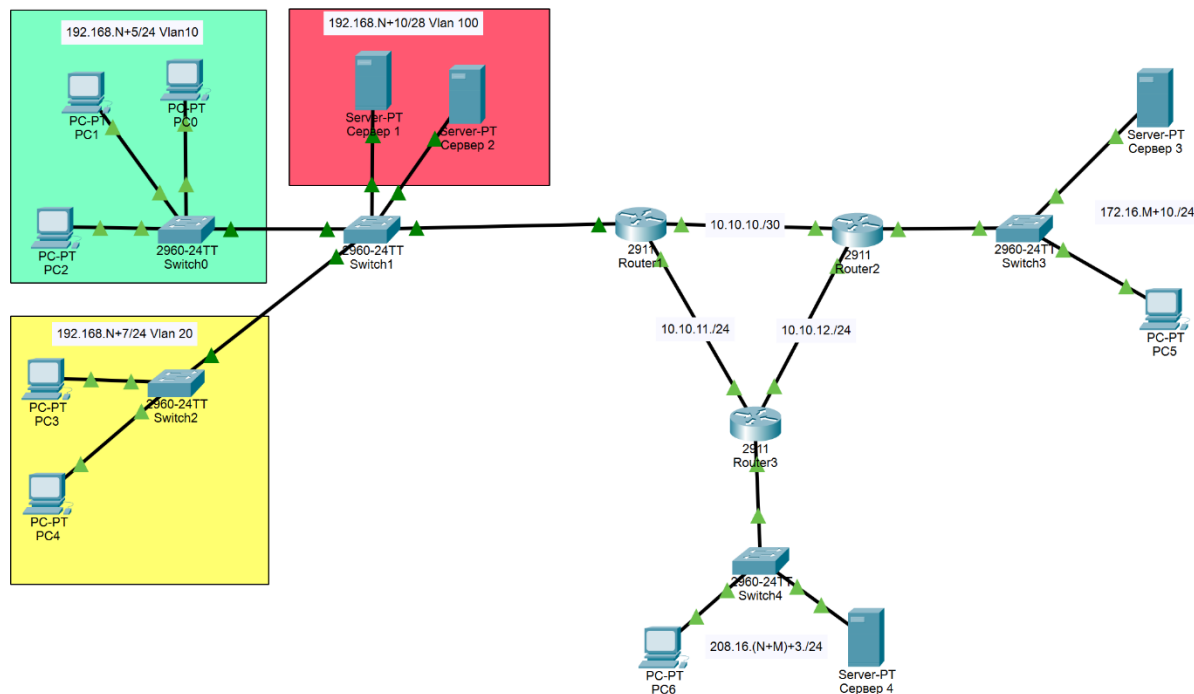


Рис.1

Шаг 1.

Создать в CPT топологию как на Рис.1

1. Назначить адреса Компьютерам и Серверам, (N последняя цифра студ. билета, M предпоследняя цифра).
2. Создать на Switch vlan и добавить на порты (vlan указаны на Рис. 1).
3. Настроить Switch и Router (+ Имя оборудования, description)
4. Настроить OSPF (На Router3 не анонсировать 208.16..)
5. Выполнить эхо-тестирования(ping), заполнить ip адреса в таблице 1.
6. Создать access-list.

К серверу 1 имеют доступ все кроме vlan 10

К серверу 3 имеют доступ только PC 4 и PC 5

Шаг 2.

Настроить Nat для подмены локальных адресов vlan 10.

Настройка NAT на Cisco-маршрутизаторах IOS включает следующие этапы

Определение множества внутренних (inside) и внешних (outside) адресов.

Выбор вида (алгоритма) трансляции (static, dynamic, overloading)

Выполнение команды настроек

Выполнение проверки трансляций

Три различных алгоритма NAT подразумевают следующее:

Static — Статический NAT выполняет преобразования IP адресов одинк одному, иначе говоря, одному адресу внутренней сети ставится в соответствие один адрес внешней. Такой вариант не дает никаких преимуществ с точки зрения экономии публичного адресного пространства.

Dynamic — Динамический NAT, выполняет преобразование внутреннего адреса/ов в один из пула внешних адресов. Разумеется, этот пул должен быть заранее задан.

Overloading перегружаемый NAT выполняет преобразование нескольких внутренних адресов в один внешний. Этот вариант мы и будем использовать

Настройка NAT выполняется на маршрутизаторе Router 1 с использованием следующей последовательности команд:

добавляем ACL-правило (критерий) для трафика, подлежащего NAT

Router1(config)#ip access-list extended myNat

Router1(config-ext-nacl)# permit ip 192.168.20.0 0.0.0.255 any

расширенный ACL-список myNat, в него записано правило о всех ipпакетах передаваемых из внутренней сети куда-либо.

Следующий шаг - назначение ролей интерфейсов для внутреннего и внешнего адресных пространств.

Router1 (config)#interface GigabitEthernet0/0

Router1 (config-if)#ip nat outside

Router1 (config)#interface GigabitEthernet0/1

Router1 (config-if)#ip nat inside

На завершающем шаге включаем сервис трансляции:

Router1 (config)#ip nat <inside | outside> source list <ACL_name | static> <interface | pool> <interfaceName | poolName > [overload]

! ip nat <inside | outside> – включение трансляции внутреннего / внешнего адресного пространства.

! source list <ACL_name | static> – адреса подлежащие трансляции могут быть представлены либо в виде ACL-списка, либо в виде статической ("жесткой") связи внутреннего и внешнего адресов.

! <interface | pool> – указание на физический интерфейс на котором будет выполняться преобразования, либо имя пула адресов из которого будут выбираться адреса для назначения. Разумеется, пул должен быть предварительно определен. Формат определения при желании можно посмотреть во встроенной системе помощи по командам.

! [overload] – необязательный параметр, указывающий на вид алгоритма трансляции. Как уже говорилось, преобразование каждого из адресов-источников в один адрес, как правило, внешнего интерфейса.

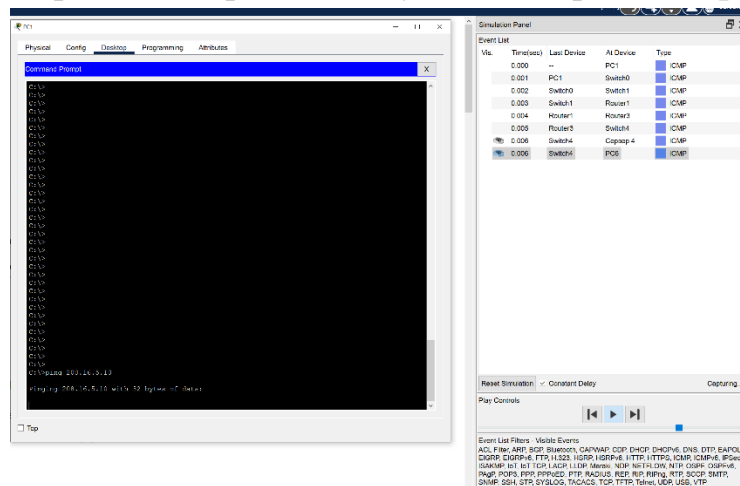
Применительно к нашему заданию команда будет выглядеть таким образом:

Router1 (config)#ip nat inside source list myNat interface GigabitEthernet0/0 overload

Не забываем добавить default маршрут на Router1 до Router3
Проводим эхо-тестирование с PC1 до PC6

Проверяем замену локальных адресов.

Переходим в режим симуляции и проводим ping



Открываем пакет на этапе

The screenshot displays a network simulation interface. On the left, a window titled "PDU Information at Device: Switch4" shows the "OSI Model" tab. It details the layers of an incoming packet from PC1 to Switch4. The packet is an Ethernet II frame with source MAC 0060.5CAD.3503 and destination MAC 0002.4AB1.7A10. The destination IP is 208.16.5.10. The packet is received on the FastEthernet0/2 interface.

On the right, the "Simulation Panel" shows an "Event List" table. A red arrow points to the event at 0.006 seconds, where the packet is received at PC6. The event list table is as follows:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	—	PC1	ICMP
	0.001	PC1	Switch0	ICMP
	0.002	Switch0	Switch1	ICMP
	0.003	Switch1	Router1	ICMP
	0.004	Router1	Router3	ICMP
	0.005	Router3	Switch4	ICMP
	0.006	Switch4	PC6	ICMP

Below the event list, there are controls for "Reset Simulation", "Constant Delay", and "Captured to: 0.006 s". At the bottom, there are "Event List Filters" and "Visible Events" sections.

Открываем Inbound PDU Details и проверяем что меняется ip адрес.

The screenshot shows the "Inbound PDU Details" window for the packet received at Switch4. It displays the structure of the packet in bytes and bits.

Ethernet II Header (Bytes):

- PREAMBLE: 101010...10
- DEST ADDR: 0002.4AB1.7A10
- SRC ADDR: 0060.5CAD.3503
- TYPE: 0x08
- DATA (VARIABLE LENGTH)
- FCS: 0x0000

IP Header (Bits):

- VER: 4, IHL: 5, DSCP: 0x00, TL: 128
- ID: 0x0064, FLGS: 0x0000, FRAG OFFSET: 0x0000
- TTL: 126, PRO: 0x01, CHKSUM
- SRC IP: 10.10.11.1 (indicated by a red arrow)
- DST IP: 208.16.5.10
- DATA (VARIABLE LENGTH)

ICMP Header (Bits):

- TYPE: 0x08, CODE: 0x00, CHECKSUM
- ID: 0x001b, SEQ NUMBER: 100

