Лабораторная работа. Настройка динамического и статического NAT

Топология

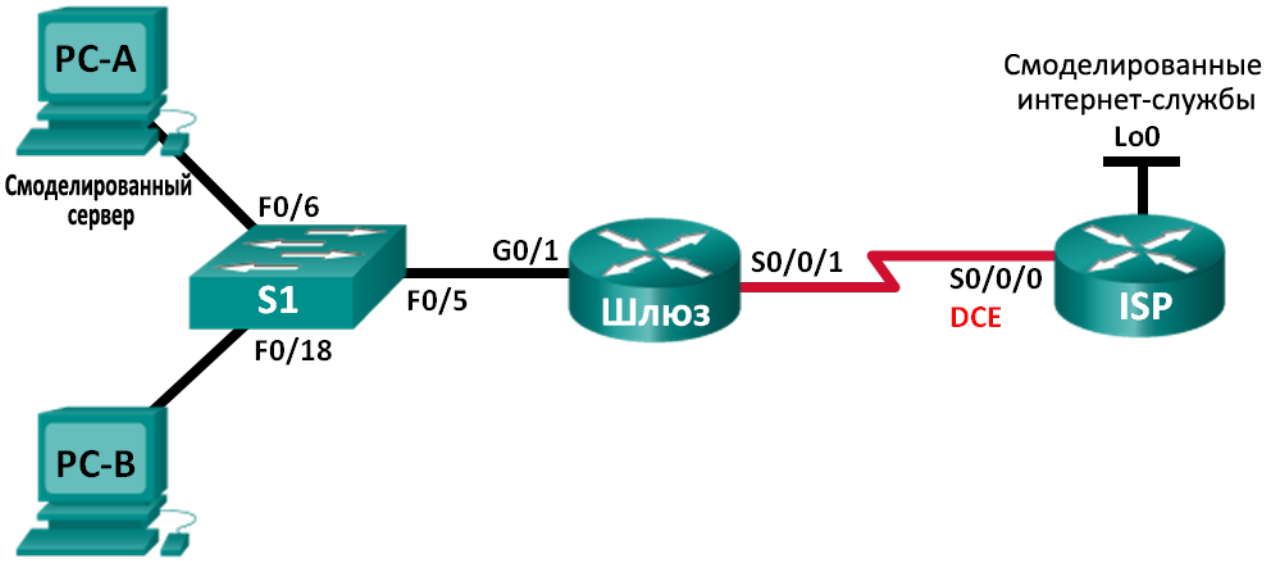

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
Интернет-провайдер	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (смоделированный сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка подключения

Часть 2. Настройка и проверка статического преобразования NAT

Часть 3. Настройка и проверка динамического преобразования NAT

Исходные данные/Сценарий

Преобразование сетевых адресов (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узловым устройствам в пределах частной сети. NAT используют для того, чтобы сократить количество публичных IP-адресов, используемых организацией, поскольку количество доступных публичных IPv4-адресов ограничено.

Согласно сценарию данной лабораторной работы интернет-провайдер выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическому распределению, а адреса от 209.165.200.242 до 209.165.200.254 — динамическому распределению. Статический маршрутом является путь от интернет-провайдера до шлюзового маршрутизатора, в то время как маршрут по умолчанию представлен в качестве пути от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и проверка подключения

В первой части вам предстоит настроить топологию сети и выполнить базовые настройки, например IP-адрес интерфейса, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с топологией и проведите все необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

c. Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

d. Присвойте имена устройствам в соответствии с топологией.

e. Назначьте **cisco** в качестве паролей консоли и VTY.

f. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 5: Создайте модель веб-сервера для интернет-провайдера.

a. Создайте локального пользователя под именем **webuser** с зашифрованным паролем **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Включите службу HTTP-сервера на маршрутизаторе интернет-провайдера.

```
ISP(config)# ip http server
```

c. Настройте сервис HTTP таким образом, чтобы он использовал локальную базу данных.

```
ISP(config)# ip http authentication local
```

Шаг 6: Настройте статическую маршрутизацию.

a. Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза, используя диапазон назначенных публичных сетевых адресов 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Шаг 7: Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 8: Проверьте сетевое соединение.

a. С узлов ПК отправьте эхо-запросы на интерфейс G0/1 на шлюзовом маршрутизаторе. Выявите и устраните неполадки, если эхо-запрос не проходит.

b. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

Часть 2: Настройка и проверка статического преобразования NAT

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования сетевых адресов особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из Интернета — например, для веб-сервера компании.

Шаг 1: Настройте статическое сопоставление.

Настроенная статическая привязка позволяет маршрутизатору осуществлять трансляцию адресов между частным внутренним адресом сервера 192.168.1.20 и публичным адресом 209.165.200.225. Благодаря этому пользователь может получить доступ к компьютеру PC-A через Интернет. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ через Интернет.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Шаг 2: Задайте интерфейсы.

Выполните команды **ip nat inside** и **ip nat outside** на интерфейсах.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Шаг 3: Проверьте конфигурацию.

a. Отобразите таблицу статических преобразований NAT с помощью команды **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

Во что был преобразован внутренний адрес локального узла?

192.168.1.20 =

Кем назначен внутренний глобальный адрес?

Кем назначен внутренний локальный адрес?

b. Из компьютера PC-A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера. Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Когда компьютер PC-A отправил ICMP-запрос (эхо-запрос) на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP?

Примечание. Для успешной передачи эхо-запросов в рамках этой лабораторной может потребоваться отключение брандмауэра.

c. От компьютера PC-A отправьте сообщение по Telnet на интерфейс интернет-провайдера Lo0 и отобразите таблицу NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
```

```
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23       192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                 ---
```

Примечание. NAT для ICMP-запроса может истечь, из-за чего он будет удалён из таблицы NAT.

Какой протокол использовался для этого преобразования?

Укажите номера используемых портов.

Внутренний глобальный/локальный:

Внешний глобальный/локальный:

d. Поскольку статический NAT настроен для компьютера PC-A, убедитесь в успешной отправке эхо-запроса от интернет-провайдера на компьютер PC-A с частным публичным NAT-адресом (209.165.200.225).

e. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT, чтобы проверить преобразование.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этот адрес — адрес источника удалённой сети интернет-провайдера. Для успешной отправки эхо-запроса от интернет-провайдера, внутренний глобальный статический NAT-адрес 209.165.200.225 был преобразован во внутренний локальный адрес компьютера PC-A. (192.168.1.20).

f. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом маршрутизаторе (Gateway).

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Часть 3: Настройка и проверка динамического преобразования NAT

Метод динамического преобразования сетевых адресов (динамический NAT) использует пул публичных адресов, которые присваиваются в порядке живой очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT присваивает доступный публичный IPv4-адрес из пула. Динамический NAT представляет собой сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами.

Шаг 1: Очистите данные NAT.

Перед добавлением динамических преобразований очистите все NAT и удалите статистику из части 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Шаг 2: Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.

Для трансляции адресов из сети 192.168.1.0/24 используется ACL1.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Шаг 3: Убедитесь, что конфигурации интерфейса NAT все ещё действительны.

Чтобы проверить конфигурации NAT, на маршрутизаторе Gateway выполните команду **show ip nat statistics**.

Шаг 4: Определите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Шаг 5: Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.

Примечание. Помните, что имена пула NAT чувствительны к регистру, а имя пула, вводимое здесь, должно совпадать с именем, использованным на предыдущем шаге.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Шаг 6: Проверьте конфигурацию.

a. Из компьютера PC-B отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера. Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

Как выглядит преобразованный внутренний адрес локального узла для компьютера PC-B?

192.168.1.21 =

Когда компьютер PC-B отправил ICMP-сообщение на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена динамическая запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP?

b. В компьютере PC-B откройте веб-браузер и введите IP-адрес смоделированного веб-сервера интернет-провайдера (интерфейс Lo0). При запросе войдите в систему под именем **webuser** и с паролем **webpass**.

c. Отобразите таблицу NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

Какой протокол использовался для этого преобразования?

Укажите номера используемых портов.

Внутренний:

Внешний:

Какие известные номер порта и сервис использовались?

d. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом маршрутизаторе (Gateway).

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
```

```
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Шаг 7: Удалите запись статического NAT.

На шаге 7 запись статического NAT удалена, вы можете просмотреть запись NAT.

a. Удалите статический NAT из части 2. При запросе об удалении дочерних записей введите **yes**.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Очистите преобразования NAT и статистику.

c. Отправьте эхо-запрос на интернет-провайдер (192.31.7.1) от обоих узлов.

d. Отобразите таблицу и статистику NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Вопросы на закрепление

1. Зачем нужно использовать NAT в сети?

2. Каковы ограничения NAT?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.