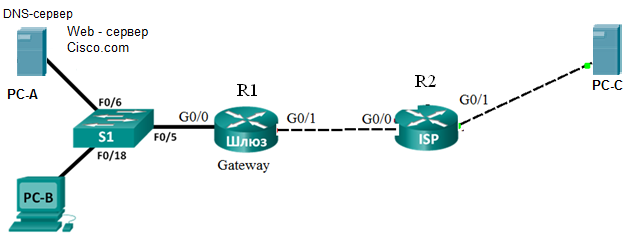
Практическое задание №4.

Настройка службы DHCP и статического NAT

1. Топология



1. Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| Шлюз | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
|  | G0/1 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | G0/0 | 209.165.201.17 | 255.255.255.252 | N/A |
|  | G0/1 | 192.31.7.1 | 255.255.255.0 | N/A |
| PC-A (смоделированный Web и DNS сервер) | NIC | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | DHCP | DHCP | DHCP |
| PC-C | NIC | 192.31.7.2 | 255.255.255.0 | 192.31.7.1 |

1. Задачи

Часть 1. Построение сети и проверка подключения

Часть 2. Выполнение настройки DHCPv4-сервера

Часть 3. Настройка и проверка статического преобразования NAT

1. 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.

1. Построение сети и проверка подключения
   1. Подключите кабели в сети в соответствии с топологией.

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

* 1. Настройте узлы ПК (PC-A и PC-C ), имеющие статические адреса соласно таблицы адресации.
  2. Выполните включение и нициализацию маршрутизаторов и коммутаторов.
  3. Настройте базовые параметры каждого маршрутизатора.
     1. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
     2. Присвойте имена устройствам в соответствии с топологией.
  4. Настройте статическую маршрутизацию.
     1. 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**

* + 1. 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**

* 1. Проверьте сетевое соединение.
     1. С узлов PC-A и PC-C отправьте эхо-запросы на интерфейсы соответствующих шлюзовых маршрутизаторов . Выявите и устраните неполадки, если эхо-запрос не проходит.
     2. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

1. Настройка DHCPv4-сервера

Для того чтобы автоматически назначить адресную информацию в сети, вам необходимо настроить маршрутизатор R1 в качестве сервера DHCPv4.

Выполните настройку сервера DHCPv4 на маршрутизаторе Gateway.

На маршрутизаторе R1 необходимо создать пул DHCP-адресов локальной сети.. Используйте имя **R1G1** для интерфейса G0/1 LAN. Также вам нужно исключить адреса, которые не будут назначаться из пула адресов. Исключать адреса рекомендуется в первую очередь, чтобы предотвратить их случайную аренду для других устройств.

В строках ниже приведены команды, необходимые для настройки служб DHCP на маршрутизаторе R1, включая те, что требуются для исключения DHCP-адресов и создания пулов DHCP.

R1(config)# **ip dhcp excluded-address 192.168.1.1 192.168.1.20**

R1(config)# **ip dhcp pool R1G1**

R1(dhcp-config)# **network 192.168.1.0 255.255.255.0**

R1(dhcp-config)# **default-router 192.168.1.1**

R1(dhcp-config)# **dns-server 192.31.17.2**

R1(dhcp-config)# **exit**

На PC-B выберите режим автоматического получения IP - адреса.

* 1. Запишите IP-параметры для компьютера PC-B.

На компьютере PC-B выполните команду **ipconfig /all**, чтобы убедиться, что компьютер получил информацию об IP-адресах от DHCP-сервера маршрутизатора R1. Запишите выделенный IP- адрес, а также IP- адрес шлюза **и** IP- адресDNS сервера.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Проверьте работу служб DHCP и аренды адресов на маршрутизаторе R1.
     1. На маршрутизаторе R1 выполните команду **show ip dhcp binding**, чтобы просмотреть список арендованных DHCP адресов.

Какая другая полезная информация для идентификации пользователя содержится в выходных данных, помимо арендованных IP-адресов?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. На маршрутизаторе R1 выполните команду **show ip dhcp show statistics**, чтобы отобразить статистику пула DHCP и активность сообщений.

Сколько типов сообщений DHCP представлено в выходных данных?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. На маршрутизаторе R1 выполните команду **show ip dhcp pool**, чтобы просмотреть настройки пула DHCP.

К чему относится показатель Current в выходных данных команды **show ip dhcp pool**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. На маршрутизаторе R1 выполните команду **show run | section dhcp**, чтобы просмотреть конфигурацию DHCP в текущей конфигурации.
    2. На маршрутизаторе R1 выполните команду show run interface для интерфейсов G0/0 и G0/1, чтобы просмотреть настройки ретранслятора DHCP в текущей конфигурации.

1. 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.

* 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**

* 1. Задайте интерфейсы.

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

Gateway(config)# **interface g0/0**

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

Gateway(config-if)# **interface g0/1**

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

* 1. Проверьте конфигурацию.
     1. 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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Из компьютера PC-A отправьте эхо-запрос на компьютер PC -C (192.31.7.2) 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 209.165.200.225:1 192.168.1.20:1 192.31.7.2:1 192.31.7.2:1

--- 209.165.200.225 192.168.1.20 --- ---

Когда компьютер PC-A отправил ICMP-запрос (эхо-запрос) на адрес интернет-провайдера 192.31.7.2, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. На компьютере PC-С в настройках IP- адресов установите IP- адрес DNS - сервера 209.165.200.225 (адрес статического NAT).
    2. На сервере PC-A в разделе службы включите поддержку служб HTTP и DNS. В базу службы DNS добавьте запись о ресурсах типа А : 1)имени Сisco.com соответствует адрес 209.168.200.225 На компьютере PC-С в браузере наберите имя web страницы Cisco.com.
    3. При правильной настройке сети отобразится внутренняя страница Cisco.
    4. Отобразите таблицу NAT на шлюзе (Gateway).

. Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

udp 209.165.200.225:53 192.168.1.20:53 192.31.7.2:1045 192.31.7.2:1045

--- 209.165.200.225 192.168.1.20 --- ---

tcp 209.165.200.225:80 192.168.1.20:80 192.31.7.2:1026 192.31.7.2:1026

tcp 209.165.200.225:80 192.168.1.20:80 192.31.7.2:1027 192.31.7.2:1027

tcp 209.165.200.225:80 192.168.1.20:80 192.31.7.2:1028 192.31.7.2:1028

tcp 209.165.200.225:80 192.168.1.20:80 192.31.7.2:1029 192.31.7.2:1029

tcp 209.165.200.225:80 192.168.1.20:80 192.31.7.2:1030 192.31.7.2:

Какой протокол использовался для этого преобразования? \_\_\_\_\_\_\_\_\_\_\_\_

Укажите номера используемых портов.

Внутренний глобальный/локальный: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Внешний глобальный/локальный: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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).

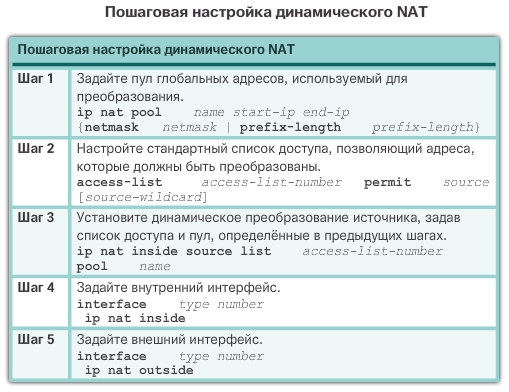
* + 1. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом

маршрутизаторе (Gateway).

Gateway# **show ip nat statistics**

* 1. Настройте динамический NAT.

Используя команды настроить динамическое преобразование для других узлов частной сети из диапазона выделенных глобальных адресов ***209.165.200.242 до 209.165.200.254***

******

* *Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255*
* *Router(config)#ip nat pool dynamic\_NAT 209.165.200.242 209.165.200.254 netmask 255.255.255.224*
* *Router(config)#ip nat inside source list 1 pool dynamic\_NAT*
* *Router(config)#****interface g0/0***
* *Router(config-if)#****ip nat inside***
* *Router(config-if)#****interface g0/1***
* *Router(config-if)#****ip nat outside***
  + 1. На сервере PC-С в разделе службы включите поддержку служб HTTP и DNS. В базу службы DNS добавьте запись о ресурсах типа А : 1)имени Сisco1.com соответствует адрес 192.31.17.2
    2. На компьютере PC-В в браузере наберите имя web страницы Cisco1.com. При правильной настройке сети отобразится внутренняя страница Cisco.
    3. Отобразите и поясните NAT таблицу для динамического преобразования.

1. Вопросы на закрепление
   1. Зачем нужно использовать NAT в сети?
   2. Принцип работы NAT
   3. Отличие статического, динамического NAT и PAT
   4. Cone NAT, Address-Restricted cone MAT, Port-Restricted cone NAT, Symmetric NAT
   5. Приведите способы с помощью которых можно обратиться к узлу за NAT из внешней сети
   6. Достоинства и недостатки NAT.
   7. Приведите основные этапы работы протокола DHCPv4
   8. Особенности функционирования протоколов динамического назначения IPv6-адресов: SLAAC, SLAAC+DHCPv6, DHCPv6.
   9. Работа протокола NDP

**Порядок выполнения работы:**

1. Настроить сеть по приведенной в задании топологии используя IP- адреса согласно варианта из таблицы.
2. Статический адрес внутреннему серверу частной сети задать фиксированным из списка исключенных IP-адресов и настроить для него статический NAT из блока публичных адресов, выделенных компании.
3. Для других узлов **частной** сети адрес раздать динамически с помощью протокола DHCP и настроить динамическое NAT- преобразование для оставшихся (*после выделения блока статических адресов*) публичных адресов.

**Индивидуальное задание к практической работе № 4**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **IP – адрес сети**  **LAN(внутренний, серый)** | **DHCP - pool** | **Кол-во DNS - серверов** | **IP - адрес сети WAN(между роутерами)** | **Публичный адрес**  **сети для NAT** |
| 1 | 192.168.50.0/26 | Искл. 1-пер/5-посл | 1 | 209.165.201.100/30 | 209.165.200.224/27 |
| 2 | 192.168.50.64/26 | Искл. 5-пер/1-посл | 1 | 209.165.201.104/30 | 209.166.200.224/27 |
| 3 | 192.168.50.128/26 | Искл. 5-пер/5-посл | 1 | 209.165.201.108/30 | 209.167.200.224/27 |
| 4 | 192.168.50.192/26 | Искл. 0-пер/10-посл | 1 | 209.165.201.112/30 | 209.168.200.224/27 |
| 5 | 192.168.100.0/24 | Искл. 10-пер/10-посл | 1 | 209.165.201.116/30 | 209.169.200.224/27 |
| 6 | 10.0.0.0/8 | 8192-посл. адреса | 1 | 209.165.201.120/30 | 209.170.200.224/27 |
| 7 | 10.64.0.0/10 | 8192-перв. адреса | 1 | 209.165.201.124/30 | 209.171.200.224/27 |
| 8 | 10.80.0.0/12 | 4096-посл. адреса | 1 | 209.165.201.128/30 | 209.172.200.224/27 |
| 9 | 10.84.0.0/14 | 4096-перв. адреса | 1 | 209.165.201.132/30 | 209.173.200.224/27 |
| 10 | 172.20.0.0/16 | 2048-посл. адреса | 1 | 209.165.201.136/30 | 209.174.200.224/27 |
| 11 | 172.20.64.0/18 | 2048-перв. адреса | 1 | 209.165.201.140/30 | 209.175.200.224/27 |
| 12 | 172.20.80.0/20 | 1024-посл. адреса | 1 | 209.165.201.144/30 | 209.176.200.224/27 |
| 13 | 172.20.84.0/22 | 256-посл. адреса | 1 | 209.165.201.148/30 | 209.177.200.224/27 |
| 14 | 172.27.128.0/17 | 512-посл. адреса | 1 | 209.165.201.152/30 | 209.178.200.224/27 |
| 15 | 172.27.160.0/19 | 512-перв. адреса | 1 | 209.165.201.156/30 | 209.179.200.224/27 |
| 16 | 172.27.168.0/21 | 256-перв. адреса | 1 | 209.165.201.160/30 | 209.180.200.224/27 |
| 17 | 172.27.170.0/23 | 128-перв. адреса | 1 | 209.165.201.164/30 | 209.181.200.224/27 |
| 18 | 10.128.0.0/9 | 8192-перв. адреса | 1 | 209.165.201.168/30 | 209.182.200.224/27 |
| 19 | 10.160.0.0/11 | 4096-перв. адреса | 1 | 209.165.201.172/30 | 209.183.200.224/27 |
| 20 | 10.168.0.0/13 | 2048-перв. адреса | 1 | 209.165.201.176/30 | 209.184.200.224/27 |
| 21 | 10.170.0.0/15 | 1024-перв. адреса | 1 | 209.165.201.180/30 | 209.185.200.224/27 |
| 22 | 192.168.150.0/27 | Искл. 7-пер/0-посл | 1 | 209.165.201.184/30 | 209.186.200.224/27 |
| 23 | 192.168.150.32/27 | Искл. 0-пер/7-посл | 1 | 209.165.201.188/30 | 209.187.200.224/27 |
| 24 | 192.168.150.64/27 | Искл. 1-пер/5-посл | 1 | 209.165.201.192/30 | 209.188.200.224/27 |
| 25 | 192.168.150.96/27 | Искл. 5-пер/1-посл | 1 | 209.165.201.196/30 | 209.189.200.224/27 |
| 26 | 192.168.150.128/27 | Искл. 3-пер/3-посл | 1 | 209.165.201.200/30 | 209.190.200.224/27 |
| 27 | 192.168.150.160/27 | Искл. 2-пер/5-посл | 1 | 209.165.201.204/30 | 209.191.200.224/27 |
| 28 | 192.168.150.192/27 | Искл. 5-пер/2-посл | 1 | 209.165.201.208/30 | 209.192.200.224/27 |
| 29 | 192.168.150.224/27 | Искл. 10-пер/0-посл | 1 | 209.165.201.212/30 | 209.193.200.224/27 |
| 30 | 192.168.200.0/24 | Искл. 5-пер/7-посл | 1 | 209.165.201.216/30 | 209.194.200.224/27 |