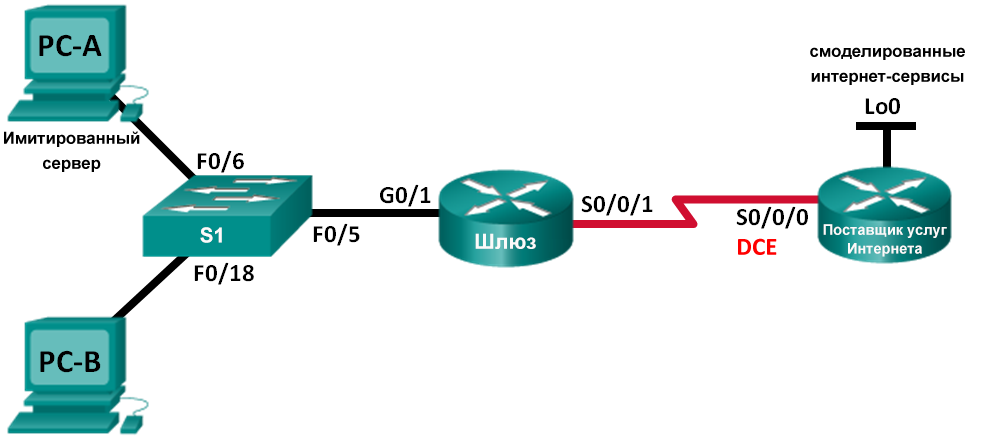
**Лабораторная работа NAT-4. Настройка динамического и статического NAT**

# Топология



# Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| Шлюз | G0/1 | 192.168.1.1 | 255.255.255.0 | — |
|  | S0/0/1 | 209.165.201.18 | 255.255.255.252 | — |
| ISP | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252 | — |
|  | Lo0 | 192.31.7.1 | 255.255.255.255 | — |
| 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 соединения**

**Часть 2. Настройка и проверка статического NAT**

**Часть 3. Настройка и проверка динамического NAT**

# Общие сведения/сценарий

Преобразование (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узлам в пределах частной сети. NAT используют для сокращения количества 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 маршрут используется на участке от интернет-провайдера до маршрутизатора, являющегося шлюзом, в то время как маршрут по умолчанию используется на участке от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

**Примечание**. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание**. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файлов загрузочной настройки. Если вы не уверены, обратитесь к инструктору.

# Необходимые ресурсы

* 2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
* 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель).
* 2 ПК (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 согласно топологии.

# Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например, IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

**Шаг 1: Создайте сеть согласно топологии.**

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

**Шаг 2: Настройте узлы ПК.**

**Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.**

**Шаг 4: Произведите базовую настройку маршрутизаторов.**

1. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
2. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

no ip domain-lookup service password-encryption enable secret class banner motd #

Unauthorized access is strictly prohibited. # line con 0 password cisco login logging synchronous line vty 0 4 password cisco login

1. Настройте имена хостов в соответствии с топологией.
2. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

**Шаг 5: Для симуляции создайте веб-сервер на ISP.**

1. Создайте локального пользователя с именем **webuser** с зашифрованным паролем **webpass**.

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

1. Включите службу HTTP-сервера на маршрутизаторе ISP.

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

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

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

**Шаг 6: Настройте статическую маршрутизацию.**

1. Создайте статический маршрут на маршрутизаторе ISP до диапазона назначенных публичных сетевых адресов 209.165.200.224/27 маршрутизатора Gateway

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**

**Шаг 7: Сохранение текущей конфигурации в качестве начальной.**

**Шаг 8: Проверьте подключение к сети.**

1. С компьютеров отправьте эхо-запросы на интерфейс G0/1 маршрутизатора Gateway. Выполните отладку, 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.

# Часть 2: Настройка и проверка статического преобразования NAT

В статическом NAT используется сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес и быть доступными из Интернета.

**Шаг 1: Настройте статическое сопоставление.**

Статическая привязка должна быть настроена для преобразования маршрутизатором частного внутреннего адреса сервера 192.168.1.20 в публичный адрес 209.165.200.225 и обратно. Это позволит пользователю из Интернета получить доступ к компьютеру PC-A. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ из Интернета.

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

**Шаг 2: Задайте интерфейсы.**

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

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: Протестируйте настройку.**

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. На компьютере ПК A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) маршрутизатора ISP. Если эхо-запрос не прошел, выполните отладку. На маршрутизаторе Gateway просмотрите 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 ПК A отправил ICMP-запрос (эхо-запрос) на адрес ISP 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

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

**Примечание**. Для успешной передачи эхо-запросов в рамках этой лабораторной может потребоваться отключение межсетевого экрана на компьютере ПК A.

1. С компьютера ПК A подключитесь по Telnet к интерфейсу Lo0 ISP 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 запроса ICMP может устареть, из-за чего он будет удален из таблицы NAT.

Какой протокол использовался для этого преобразования? \_\_\_\_\_\_\_\_\_\_\_\_ Укажите номера используемых портов.

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

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

1. Поскольку статический NAT настроен для ПК A, убедитесь в успешном прохождении эхо-запроса от ISP до ПК A по публичному адресу через статический NAT (209.165.200.225).
2. На 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 в удаленной сети ISP. Для успешной отправки эхо-запроса от ISP, внутренний глобальный адрес статического NAT 209.165.200.225 был преобразован во внутренний локальный адрес компьютера ПК A (192.168.1.20).

1. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на маршрутизаторе, являющемся шлюзом.

Gateway# **show ip nat statistics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 0:02:12 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**. Показанный результат приведен исключительно в качестве примера. Полученные вами результаты могут не совпадать с ним.

# Часть 3: Настройка и проверка динамического преобразования (NAT)

При динамическом преобразовании NAT используется пул публичных адресов, которые назначаются в порядке очереди («первым пришел — первым обслужили»). Когда внутреннее устройство запрашивает доступ к внешней сети, динамическое преобразование NAT назначает доступный публичный IPv4-адрес из пула. Динамическое преобразование 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 список контроля доступа (ACL-список), соответствующий диапазону частных IP-адресов локальной сети.**

ACL-список 1 используется для обеспечения возможности преобразования сети 192.168.1.0/24.

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

**Шаг 3: Убедитесь, что настройки интерфейсов NAT все еще действительны.**

Чтобы проверить настройки 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 NAT из внутреннего списка адресов источника на пул внешних адресов.**

**Примечание**. Помните, что имена пула NAT регистрозависимы, 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: Протестируйте настройку.**

1. С ПК B отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) маршрутизатора ISP. Если эхо-запрос не прошел, выполните отладку. На маршрутизаторе Gateway просмотрите 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 ПК B?

192.168.1.21 = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Когда ПК B отправил сообщение ICMP на адрес ISP 192.31.7.1, в таблицу была добавлена динамическая запись NAT с указанным протоколом ICMP.

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

1. На компьютере ПК B откройте веб-браузер и введите IP-адрес имитируемого на ISP веб-сервера (интерфейс Lo0). При запросе войдите в систему под именем **webuser** и с паролем **webpass**. c. Выведите на экран 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 общеизвестные номер порта и сервис использовались? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

d. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на маршрутизаторе, являющемся шлюзом.

Gateway# **show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 0:06:40 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**. Показанный результат приведен исключительно в качестве примера. Полученные вами результаты могут не совпадать с ним.

**Шаг 7: Удалите запись статического NAT.**

На шаге 7 запись статического NAT удаляется, и можно просмотреть запись NAT.

1. Удалите статический NAT из части 2. При запросе об удалении дочерних записей введите **yes** (да).

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**

1. Очистите трансляции NAT и статистику.
2. Отправьте эхо-запрос к ISP (192.31.7.1) c обоих узлов.
3. Отобразите таблицу и статистику NAT.

Gateway# **show ip nat statistics**

Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 0:00:43 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**. Показанный результат приведен исключительно в качестве примера. Полученные вами результаты могут не совпадать с ним.

## Вопросы для повторения

1. Зачем нужно использовать NAT в сети?

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

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. В чем заключаются ограничения NAT?

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

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

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

## Сводная таблица по интерфейсам маршрутизаторов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Сводная таблица по интерфейсам 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 определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса. | | | | |