Лабораторная работа. Настройка и проверка ACL-списков для IPv6

Топология

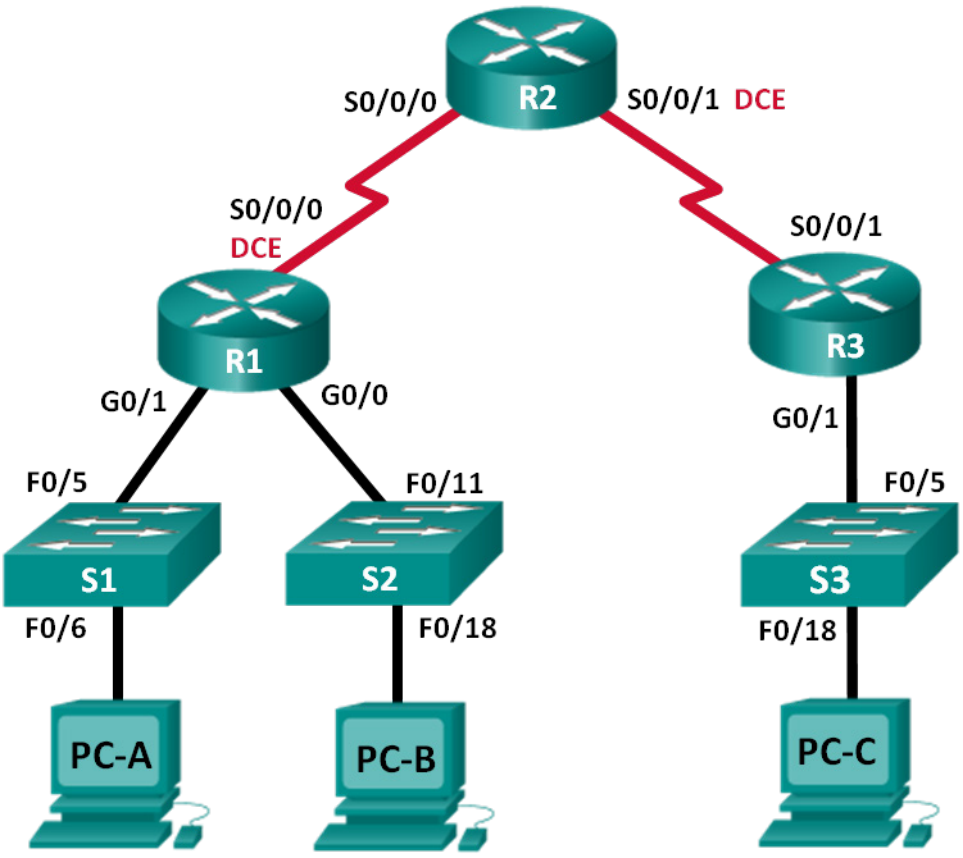


Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

Часть 2. Конфигурация устройств и проверка подключения

Часть 3. Настройка и проверка ACL-списков для IPv6

Часть 4. Редактирование ACL-списков для IPv6

Исходные данные/сценарий

Фильтрация IPv6-трафика путём создания ACL-списков для IPv6 и их применения на интерфейсах аналогична способу, по которому вы создавали именованные ACL-списки для IPv4. В IPv6 определены расширенные и именованные ACL-списки. Стандартные и нумерованные ACL-списки больше не используются для IPv6. Чтобы применить ACL-список IPv6 на интерфейсе vty, следует использовать новую команду **ipv6 traffic-filter**. Команда **ipv6 access-class** до сих пор используется для применения ACL-списков IPv6 на интерфейсах.

В рамках лабораторной работы вам предстоит применить правила фильтрации IPv6, а затем убедиться в правильной работе списков для ограничения доступа. Также вам нужно будет внести изменения в ACL-список IPv6 и очистить счётчики совпадений.

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 интерфейсе маршрутизатора в конце этой 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:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель);
- 3 компьютера (под управлением 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: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам нужно настроить топологию сети и при необходимости удалить все конфигурации.

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IPv6-адреса на всех ПК.

Настройте глобальный индивидуальный IPv6-адрес в соответствии с таблицей адресации. Используйте локальный адрес канала **FE80::1** для шлюза по умолчанию на всех ПК.

Шаг 2: Настройте коммутаторы.

a. Отключите поиск DNS.

b. Назначьте имя узла.

c. Назначьте имя домена для **ccna-lab.com**.

d. Зашифруйте все незашифрованные пароли.

e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.

f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.

g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.

j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.

k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.

l. Назначьте IPv6-адрес для VLAN 1 в соответствии с таблицей адресации.

m. От имени администратора отключите все неактивные интерфейсы.

Шаг 3: Настройте базовые параметры на всех маршрутизаторах.

a. Отключите поиск DNS.

b. Назначьте имя узла.

c. Назначьте имя домена для **ccna-lab.com**.

d. Зашифруйте все незашифрованные пароли.

e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.

f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.

g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.

j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.

k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.

Шаг 4: Настройте IPv6-параметры на маршрутизаторе R1.

a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/0, G0/1 и S0/0/0.

b. Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.

c. На интерфейсе S0/0/0 установите тактовую частоту 128000.

d. Включите интерфейсы.

e. Включите IPv6-маршрутизацию одноадресной передачи.

f. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Шаг 5: Настройте параметры IPv6 на маршрутизаторе R2.

a. Настройте индивидуальный IPv6-адрес на интерфейсах S0/0/0 и S0/0/1.

b. Настройте локальный IPv6-адрес канала на интерфейсах S0/0/0 и S0/0/1. На обоих интерфейсах используйте **FE80:: 2** в качестве локального адреса канала.

c. На интерфейсе S0/0/1 установите тактовую частоту со значением 128000.

d. Включите интерфейсы.

e. Включите IPv6-маршрутизацию одноадресной передачи.

f. Настройте статические IPv6-маршруты для маршрутизации трафика на подсети LAN, подключенные к маршрутизаторам R1 и R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Шаг 6: Настройте параметры IPv6 на маршрутизаторе R3.

a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/1 и S0/0/1.

b. Настройте локальный IPv6-адрес канала на интерфейсах G0/1 и S0/0/1. На обоих интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.

c. Включите интерфейсы.

d. Включите IPv6-маршрутизацию одноадресной передачи.

e. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

Шаг 7: Проверка соединения.

a. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии.

b. Подключитесь по Telnet к маршрутизатору R1 со всех компьютеров в топологии.

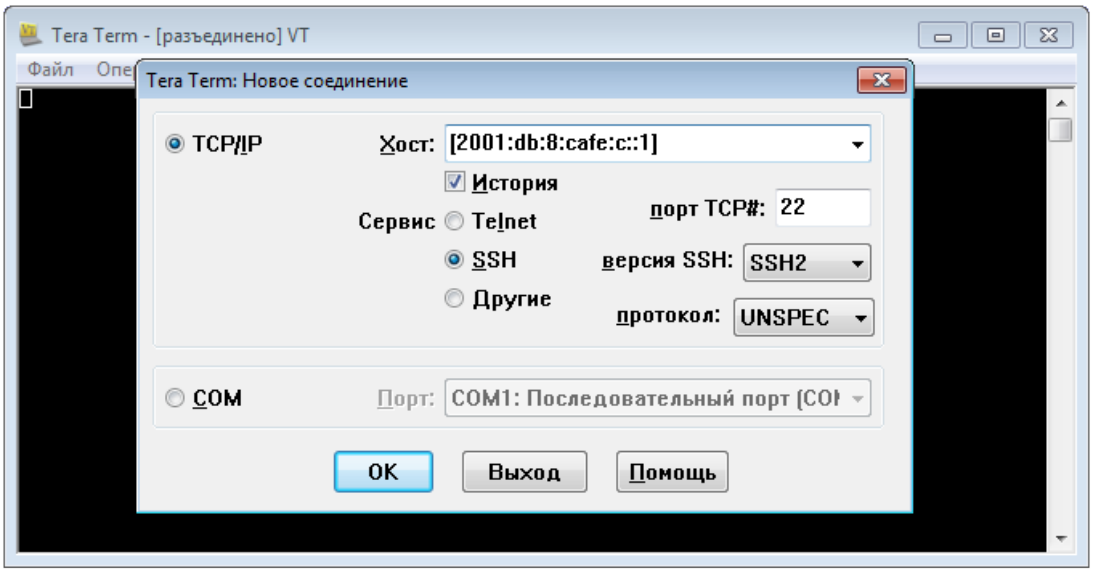
c. Подключитесь по SSH к маршрутизатору R1 со всех компьютеров в топологии.

d. Подключитесь по Telnet к коммутатору S1 со всех компьютеров в топологии.

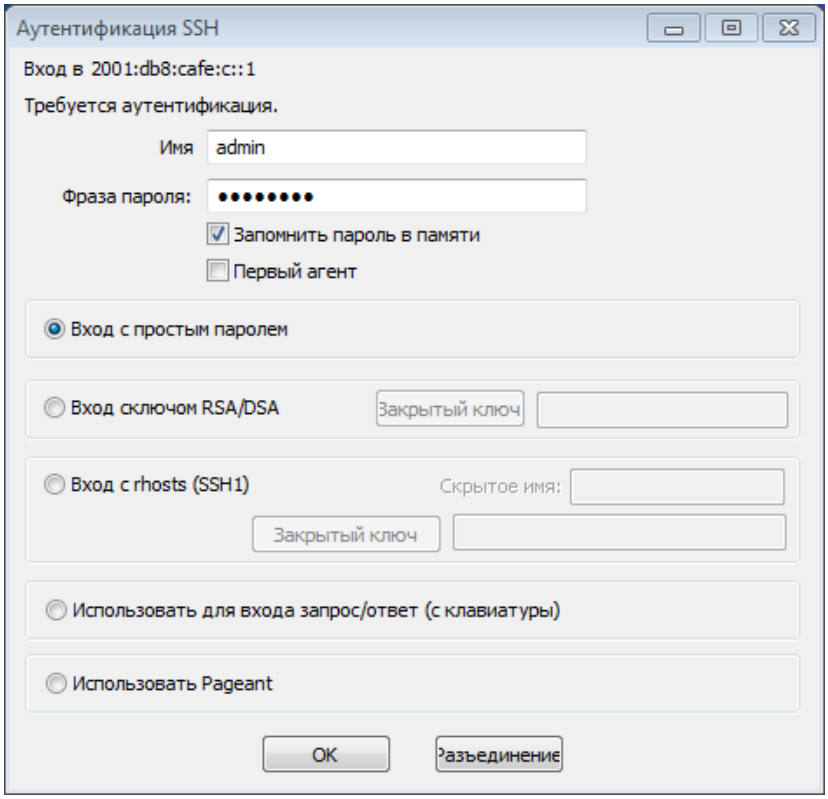
e. Подключитесь по SSH к коммутатору S1 со всех компьютеров в топологии.

f. Теперь выявите и устраните неполадки с подключением, поскольку ACL-списки, которые вы создадите в третьей части лабораторной работы, ограничат доступ к определённым областям сети.

Примечание. В соответствии с требованиями Tera Term IPv6-адрес назначения должен быть в скобках. Введите IPv6-адрес, как показано, нажмите **OK**, а затем нажмите **Continue (Продолжить)**, чтобы принять предупреждение системы безопасности и подключиться к маршрутизатору.



Введите настроенные учётные данные пользователя (имя пользователя **admin**, пароль **classadm**) и в диалоговом окне SSH Authentication (Аутентификация SSH) выберите **Use plain password to log in (Использовать незашифрованный пароль)**. Для продолжения нажмите кнопку **OK**.



Часть 3: Настройка и проверка ACL-списков для IPv6

Шаг 1: Настройте и проверьте ограничения VTY на маршрутизаторе R1.

a. Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64. Все узлы должны обладать доступом к маршрутизатору R1 только через telnet.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
R1(config-ipv6-acl)# permit tcp any any eq 22
```

b. Примените ACL-список под именем RESTRICT-VTY на линиях VTY маршрутизатора R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

c. Отобразите новый ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```

d. Убедитесь, что ACL-список RESTRICT-VTY пропускает только Telnet-трафик из сети 2001:db8:acad:a::/64.

Каким образом ACL-список RESTRICT-VTY разрешает доступ к маршрутизатору R1 через Telnet только для узлов из сети 2001:db8:acad:a::/64?

Какую функцию выполняет второе правило permit в ACL-списке RESTRICT-VTY?

Шаг 2: Ограничьте доступ через Telnet к сети 2001:db8:acad:a::/64.

a. Создайте ACL-список под именем RESTRICTED-LAN, который заблокирует доступ через Telnet к сети 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

b. Примените ACL-список RESTRICTED-LAN на интерфейсе G0/1 для всего исходящего трафика.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

c. Подключитесь по Telnet к коммутатору S1 от узлов PC-B и PC-C, чтобы проверить ограничение Telnet. Подключитесь по SSH к коммутатору S1 от узла PC-B, чтобы убедиться, что к этому узлу по-прежнему можно получить доступ через SSH. При необходимости выявите и устраните любые неполадки.

d. Используйте команду **show ipv6 access-list**, чтобы просмотреть ACL-список RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
    permit ipv6 any any (45 matches) sequence 30
```

Обратите внимание, что каждое правило определяет количество попаданий или совпадений, возникших с момента применения ACL-списка на интерфейсе.

e. Используйте команду **clear ipv6 access-list**, чтобы сбросить счётчики совпадений для ACL-списка RESRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

f. Снова отобразите ACL-список с помощью команды **show access-lists**, чтобы убедиться, что счётчики удалены.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any sequence 30
```

Часть 4: Редактирование ACL-списков для IPv6

В четвёртой части вам предстоит внести изменения в ACL-список RESTRICTED-LAN, созданный в предыдущей части лабораторной работы. Перед внесением изменений в ACL-список рекомендуется удалить его из интерфейса, на котором он применён. Завершив редактирование, снова примените ACL-список на интерфейсе.

Примечание. Многие сетевые администраторы делают копию ACL-списка и вносят изменения в копии. После изменения копии администратор удаляет старый ACL-список и применяет на интерфейсе отредактированный вариант. Благодаря этому ACL-список можно не удалять, пока отредактированная копия не будет готова для применения.

Шаг 1: Удалите ACL-список из интерфейса.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Шаг 2: Используйте команду show access-lists, чтобы просмотреть ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (36 matches) sequence 30
```

Шаг 3: Создайте новую запись в ACL-списке, используя последовательную нумерацию.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a
eq 23 sequence 15
```

Какую функцию выполняет добавленная разрешающая запись permit?

Шаг 4: Создайте новое правило ACL, вставив его в конец списка.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Примечание. Данная разрешающая запись используется только для того, чтобы продемонстрировать добавление записи в конец ACL-списка. Для данной строки списка не должно быть совпадений, поскольку предыдущая запись permit совпадает со всем.

Шаг 5: Используйте команду show access-lists, чтобы просмотреть изменения ACL-списка.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
```

```
        permit ipv6 any any (124 matches) sequence 30
        permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Примечание. Для выполнения любой команды привилегированного режима в режиме глобальной конфигурации или подрежиме можно использовать команду **do**.

Шаг 6: Удалите запись ACL-списка.

Используйте команду **no**, чтобы удалить только что добавленное правило permit.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Шаг 7: Используйте команду do show access-lists RESTRICTED-LAN, чтобы просмотреть ACL-список.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (214 matches) sequence 30
```

Шаг 8: Снова примените список ACL RESTRICTED-LAN на интерфейсе G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Шаг 9: Проверьте изменения в ACL-списке.

От узла PC-B подключитесь к коммутатору S1 по Telnet. При необходимости выявите и устраните любые неполадки.

Вопросы на закрепление

1. Из-за чего счётчик совпадений для записи **permit ipv6 any any** списка RESTRICTED-LAN продолжает расти?

2. Какую команду следует использовать, чтобы сбросить счётчики для ACL-списка на каналах VTY?

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.