Лабораторная работа. Настройка и проверка стандартных списков контроля доступа для IPv4

Топология

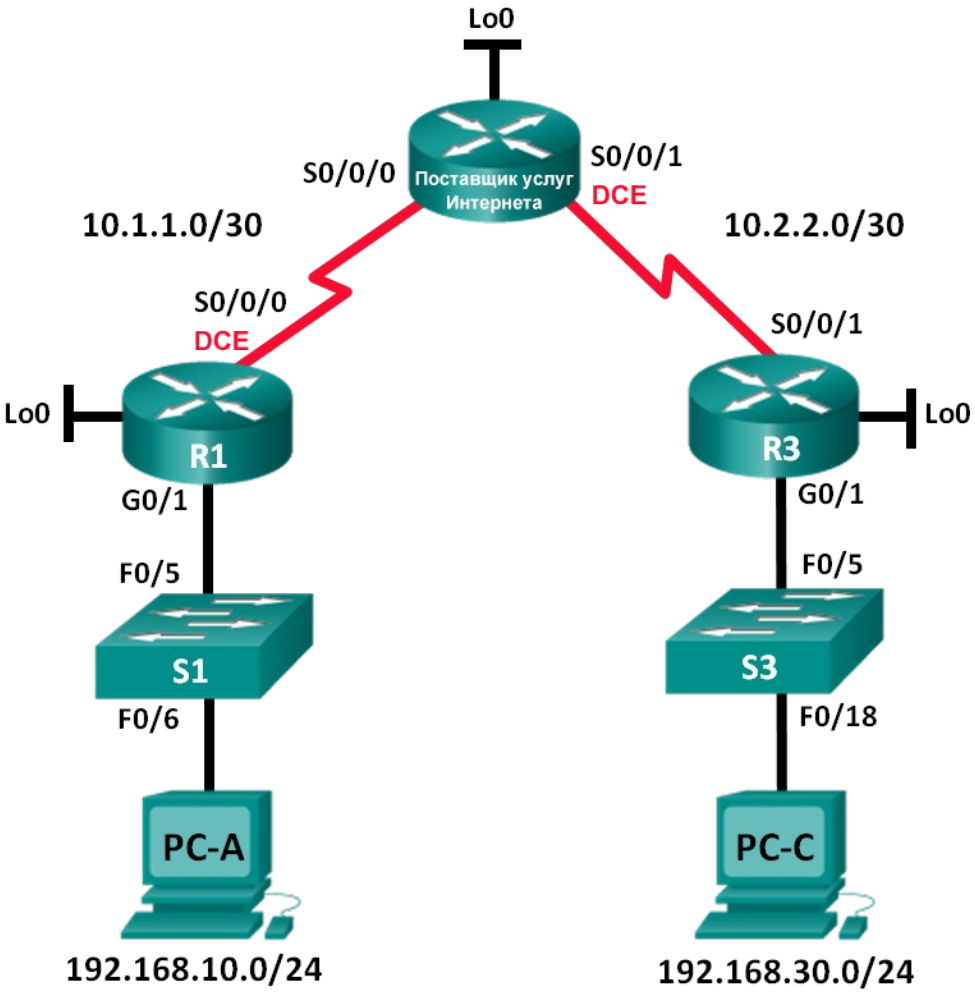

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	—
	Lo0	192.168.20.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
ISP	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
R3	G0/1	192.168.30.1	255.255.255.0	—
	Lo0	192.168.40.1	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Часть 2. Настройка устройств и проверка подключения

- Назначьте компьютерам статический IP-адрес.
- Настройте базовые параметры на маршрутизаторах.
- Настройте базовые параметры на коммутаторах.
- Настройте маршрутизацию OSPF на R1, ISP и R3.
- Проверьте наличие подключения между всеми устройствами.

Часть 3. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

- Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.
- Настройте, примените и проверьте работу стандартных именованных ACL-списков.

Часть 4. Изменение стандартного ACL-списка

- Измените и проверьте работу стандартного именованного ACL-списка.
- Проверьте работу ACL-списка.

Общие сведения/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP-сетями. Ценным навыком является умение применять соответствующие правила для фильтрации пакетов на основе установленной политики безопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

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). Можно использовать другие маршрутизаторы, коммутаторы и версии 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. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ 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: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети и при необходимости удалить все текущие настройки.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов 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 указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры маршрутизаторов.

a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.

b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
hostname R1
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
```

c. Присвойте имена устройствам в соответствии с топологией.

d. Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии с таблицей адресации.

e. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

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

g. Разрешите доступ по Telnet.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3: Настройка базовых параметров на коммутаторах (дополнительно).

a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобального конфигурирования.

b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в файл текущей конфигурации на коммутаторе.

```
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 15
password cisco
login
exit
```

c. Присвойте имена устройствам в соответствии с топологией.

d. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.

e. Настройка шлюза по умолчанию.

f. Разрешите доступ по Telnet.

g. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте маршрутизацию RIP на маршрутизаторах R1, ISP и R3.

a. Настройте протокол RIP версии 2 и анонсируйте все сети на маршрутизаторах R1, ISP и R3. Конфигурация OSPF для R1 и ISP приведена в справочных целях.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0

ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0
```

b. После настройки RIP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации со всеми сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 5: Проверьте наличие подключения между всеми устройствами.

Примечание. Соединение важно проверять **перед** настройкой и применением списков доступа! Удостовериться в правильной работе сети необходимо до начала фильтрации трафика.

a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешно ли выполнены эхо-запросы? _____

b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизаторе R3. Успешно ли выполнены эхо-запросы? _____

c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____

d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____

Часть 3: Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков

Шаг 1: Настройка стандартного именованного ACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называют оператором ACL-списка.

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?

_____

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

_____

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

_____

a. Настройте ACL-список на маршрутизаторе R3. В качестве номера списка доступа используйте 1.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c. Проверьте нумерованный ACL-список.

Использование команды **show** поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE?

_____

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применен список доступа?

_____

1) На маршрутизаторе R3 выполните команду **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) На маршрутизаторе R3 выполните команду **show ip interface g0/1**.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Выходные данные опущены
```

3) Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24. Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнена проверка связи? _____

4) Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнена проверка связи? _____

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d. Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C.

```
R1# ping 192.168.30.3
```

Успешно ли выполнен эхо-запрос? Поясните свой ответ.

_____

_____

_____

Шаг 2: Настройте стандартный именованный ACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешен только для узла PC-C. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

_____

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

_____

a. Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Взгляните на первую запись ACE в списке доступа и ответьте, можно ли записать это иначе?

_____

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Проверьте именованный ACL-список.

1) На R1 выполните команду **show access-lists.**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чем они заключаются?

_____

_____

_____

_____

_____

2) На маршрутизаторе R1 выполните команду **show ip interface g0/1**.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
```

```
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Данные опущены>
```

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP-адрес узла PC-A. Успешно ли выполнена проверка связи? _____

4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адрес G0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи? _____

5) Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи? _____

Часть 4: Изменение стандартного ACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В части 4 необходимо изменить один из ранее настроенных списков контроля доступа для соответствия новой политике безопасности.

Руководство решило, что пользователи из сети 209.165.200.224/27 должны получить полный доступ к сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех их маршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесена запись ACE **deny any**. Вам необходимо изменить ACL-список с именем BRANCH-OFFICE-POLICY.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделать двумя способами:

Вариант 1: Выполните команду **no access-list standard BRANCH-OFFICE-POLICY** в режиме глобальной конфигурации. Это исключит весь ACL-список из маршрутизатора. В зависимости от IOS маршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет отменена, и все пакеты будут пропускаться через маршрутизатор; либо, поскольку команда **ip access-group** в интерфейс G0/1 активна, фильтрация останется прежней. В любом случае, когда ACL-список будет удален, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстового редактора.

Вариант 2: ACL-списки можно изменить, не удаляя, добавив или удалив конкретные строки из ACL-списка. Этот вариант наиболее удобен, особенно в случае если ACL-список содержит много записей. При повторном вводе всего ACL-списка или при вырезании и копировании могут возникнуть ошибки. В изменении определенных строк в списках ACL нет ничего сложного.

Примечание. В ходе данной лабораторной работы используйте вариант 2.

Step 2: Изменение стандартного именованного ACL-списка.

a. На маршрутизаторе R1 в исполнительском режиме EXEC выполните команду **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

b. Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурации измените ACL-список с именем BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. Проверьте ACL-список.

1) На R1 выполните команду **show access-lists.**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny   any
```

Нужно ли вам применить список под именем BRANCH-OFFICE-POLICY на интерфейсе G0/1 маршрутизатора R1?

_____

_____

2) Из командной строки ISP выполните расширенный эхо-запрос. Проверьте, пропускает ли список ACL трафик из сети 209.165.200.224/27 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на ISP в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи?

_____

Вопросы для повторения

1. Как вы видите, стандартные ACL-списки достаточно эффективны и полезны. Почему вам может понадобиться использовать расширенные списки ACL?

_____

_____

_____

_____

2. В большинстве случаев при использовании именованного ACL-списка требуется введение большего количества строк, нежели при использовании нумерованного ACL-списка. Почему вы бы предпочли использовать именованный ACL-список, а не нумерованный?

_____

_____

_____

_____

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.