Практическое задание 4

4.1: Стандартные списки доступа (Standard IP Access-Lists)

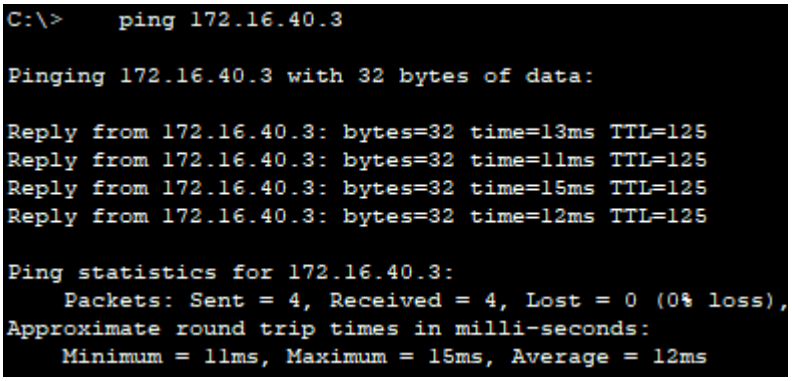
В этой лабораторной Вы заблокируете доступ к сети `172.16.40.0` от узла `Host F`.

> ⚠ **Внимание**
>
> Нужно использовать настроенную в предыдущих заданиях, работоспособную лабораторную топологию "Standard Lab".

Шаг 1. Проверка доступности хоста `HostE` с хоста `HostF`

Выполните команду для проверки доступности `HostE` с хоста `HostF`:

```
ping 172.16.40.3
```



Убедились, что соединение устанавливается корректно.

Шаг 2. Настройка списка доступа на маршрутизаторе `2600A` для блокировки доступа от HostF к подсети `172.16.40.0/24`

Стандартные списки доступа используют номера от `1` до `99` и фильтруют трафик только по IP-адресу источника. Создайте список, который блокирует доступ от узла HostF (`172.16.50.3`) и разрешает весь остальной трафик:

```
config terminal
access-list 10 deny host 172.16.50.3
access-list 10 permit any
```

> ✎ **Примечание**

Стандартные списки доступа рекомендуется применять как можно ближе к `сети назначения`, чтобы избежать излишнего блокирования другого трафика.

Шаг 3. Применение списка доступа к интерфейсу

Примените созданный список доступа на интерфейсе маршрутизатора, через который проходит трафик в подсеть `172.16.40.0/24`. В данном примере это интерфейс `serial 0/0`. Укажите, что список должен обрабатываться для входящего трафика:

```
interface serial 0/0
ip access-group 10 in
```

Шаг 4. Проверка результата

Убедитесь, что узел `HostF` больше не может отправлять пакеты (например, с помощью команды `ping`) на подсеть `172.16.40.0`. Попробуйте выполнить следующую команду с `HostF`:

```
ping 172.16.40.3
```

```
C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Reply from 172.16.20.2: Destination host unreachable.
Reply from 172.16.20.2: Destination host unreachable.
Reply from 172.16.20.2: Destination host unreachable.
Reply from 172.16.20.2: Destination host unreachable.

Ping statistics for 172.16.40.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Как видно, появилось сообщение `Destination host unreachable`, указывающее на то, что пакеты больше не достигают назначения.

Шаг 5. Проверка доступности подсети `172.16.40.0` с других устройств

Для проверки убедитесь, что остальные устройства в сети по-прежнему имеют доступ к подсети `172.16.40.0`. В качестве примера выполните команду `ping` с маршрутизатора `2600C` на хост `172.16.40.3`:

```
ping 172.16.40.3
```

```
2600C#ping 172.16.40.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.40.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/12 ms
```

> **Примечание**
>
> Эта лабораторная конфигурация является частью более крупной задачи и будет использоваться для выполнения лабораторной работы 4.2. Убедитесь, что все изменения сохранены, чтобы их можно было применить в последующих заданиях.

4.2: Проверка работы стандартных списков доступа

Помимо проверки списков доступа с помощью команд `ping`, `traceroute`, или `telnet`, существуют дополнительные способы их диагностики.

Шаг 1. Просмотр всех списков доступа

Чтобы отобразить все существующие списки доступа на маршрутизаторе, выполните следующую команду:

```
show access-list
```

```
2600A#    show access-list
Standard IP access list 10
    10 deny host 172.16.50.3 (4 match(es))
    20 permit any (191 match(es))
```

Шаг 2. Просмотр конкретного списка доступа

Если необходимо просмотреть только определённый список, например, список с номером 10, используйте команду:

```
show access-list 10
```

```
2600A#show access-list 10
Standard IP access list 10
    deny host 172.16.50.3
    permit any (52 match(es))
```

Шаг 3. Определение интерфейсов, где применены списки доступа

Для проверки, на каких интерфейсах маршрутизатора применены списки доступа, выполните следующую команду:

```
show ip interface
```

```
Serial0/0 is up, line protocol is up (connected)
  Internet address is 172.16.20.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 10
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Шаг 4. Просмотр списков доступа в текущей конфигурации

Чтобы просмотреть списки доступа и их применение в текущей конфигурации устройства, выполните команду:

```
show running-config
```

```
!
interface Serial0/0
 description connection to 2600C
 ip address 172.16.20.2 255.255.255.0
 encapsulation ppp
 ip access-group 10 in
!
```

> **Примечание**
>
> Эта лабораторная конфигурация используется для выполнения следующей лабораторной работы — `4.3`. Убедитесь, что все проверки выполнены корректно, чтобы избежать ошибок в следующих заданиях.

4.3: Применение списков доступа к линиям VTY

Для ограничения доступа к командной строке маршрутизатора по `telnet` или `ssh` можно использовать стандартные списки доступа.

1. Сначала создаётся стандартный список доступа, который разрешает доступ с определённых адресов, с которых вы планируете работать в командной строке.
2. Затем этот список применяется к линии `VTY` с помощью команды `access-class`.

В этой лабораторной запрещается `telnet`-доступ с узла `HostF` на маршрутизатор `2600A`.

Шаг 1. Удаление ненужного списка доступа

Удалите существующий список доступа на маршрутизаторе `2600A`:

```
config terminal
no access-list 10
```

Шаг 2. Удаление применения списка доступа

Снимите ранее настроенное применение списка доступа:

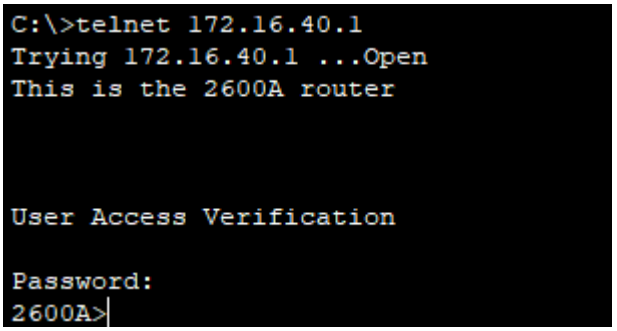
```
interface serial 0/0
no ip access-group 10 in
exit
```

Шаг 3. Проверка `Telnet`-доступа с узла `HostF`

Убедитесь, что с узла `HostF` можно выполнить `telnet` на маршрутизатор `2600A`:

- На узле HostF:
  1. Откройте `Desktop → Command Prompt`.
  2. Выполните команду:

     ```
     telnet 172.16.40.1
     ```



Если `telnet` доступен, настройку можно продолжать.

Шаг 4. Настройка списка доступа для ограничения Telnet-доступа

Создайте список доступа на маршрутизаторе 2600A, который запрещает telnet с узла HostF (172.16.50.3) и разрешает со всех других адресов:

```
config terminal
access-list 20 deny host 172.16.50.3
access-list 20 permit any
exit
```

Шаг 5. Применение списка к линиям VTY

Примените созданный список доступа ко всем линиям VTY маршрутизатора:

```
line vty 0 4
access-class 20 in
exit
```

Шаг 6. Проверка блокировки Telnet-доступа с узла HostF

Попробуйте снова выполнить telnet с HostF. Доступ должен быть заблокирован, и вы должны увидеть сообщение об ошибке.

```
C:\>telnet 172.16.40.1
Trying 172.16.40.1 ...
% Connection refused by remote host
C:\>
```

Шаг 7. Проверка разрешения Telnet-доступа с маршрутизатора 2600C

Убедитесь, что telnet с маршрутизатора 2600C на 2600A остаётся разрешён:

```
telnet 172.16.20.2
```

```
2600C#telnet 172.16.20.2
Trying 172.16.20.2 ...Open
This is the 2600A router


User Access Verification

Password:
2600A>
```

Примечание

Эта лабораторная конфигурация используется для выполнения задания `4.4`. Убедитесь, что настройки сохранены.

4.4: Расширенные списки доступа (Extended IP Access-Lists)

В этой лабораторной работе мы удалим стандартный список доступа с маршрутизатора `2600A`, создадим новый расширенный список, и настроим его для блокировки `Telnet`-доступа с узла `HostF` в подсеть `172.16.40.0`, при этом разрешив использование других сетевых служб.

Шаг 1. Удаление стандартного списка доступа

Удалите ранее созданный стандартный список доступа, чтобы он больше не применялся:

```
config terminal
no access-list 10
exit
```

Шаг 2. Проверка доступа с узла `HostF`

Убедитесь, что узел `HostF` может выполнять `ping` на `172.16.40.1` и `172.16.40.3`.

```
C:\>ping 172.16.40.1

Pinging 172.16.40.1 with 32 bytes of data:

Reply from 172.16.40.1: bytes=32 time=8ms TTL=253
Reply from 172.16.40.1: bytes=32 time=13ms TTL=253
Reply from 172.16.40.1: bytes=32 time=17ms TTL=253
Reply from 172.16.40.1: bytes=32 time=14ms TTL=253

Ping statistics for 172.16.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 17ms, Average = 13ms

C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Request timed out.
Reply from 172.16.40.3: bytes=32 time=13ms TTL=125
Reply from 172.16.40.3: bytes=32 time=15ms TTL=125
Reply from 172.16.40.3: bytes=32 time=10ms TTL=125

Ping statistics for 172.16.40.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 15ms, Average = 12ms
```

Шаг 3. Создание расширенного списка доступа

Создайте расширенный список доступа для блокировки `Telnet`-доступа с узла `HostF` на подсеть `172.16.40.0`, но при этом разрешите другие виды трафика:

```
config terminal
access-list 110 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet
access-list 110 permit ip any any
exit
```

Шаг 4. Применение списка доступа к интерфейсу

Примените созданный список доступа к интерфейсу `Serial 0/0` для входящих пакетов:

```
interface serial 0/0
ip access-group 110 in
exit
```

Шаг 5. Проверка конфигурации

1. С узла `HostF` попытайтесь выполнить `telnet` на адрес `172.16.40.1`. Доступ должен быть заблокирован.

```
telnet 172.16.40.1
```

```
C:\>telnet 172.16.40.1
Trying 172.16.40.1 ...
% Connection timed out; remote host not responding
```

2. Убедитесь, что другие устройства могут выполнять `telnet` на `172.16.40.1` без ограничений.

```
C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Reply from 172.16.40.3: bytes=32 time=12ms TTL=125
Reply from 172.16.40.3: bytes=32 time=20ms TTL=125
Reply from 172.16.40.3: bytes=32 time=11ms TTL=125
Reply from 172.16.40.3: bytes=32 time=5ms TTL=125

Ping statistics for 172.16.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 20ms, Average = 12ms
```

```
2600C#telnet 172.16.40.1
Trying 172.16.40.1 ...Open
This is the 2600A router



User Access Verification

Password:
2600A>
```

> **Примечание**
>
> Эта конфигурация будет использована для выполнения задания `4.5`. Убедитесь, что она корректна и сохранена.

4.5: Проверка расширенных списков доступа

В этом задании мы будем использовать команды из лабораторной работы `4.2` для проверки работы расширенных списков доступа.

Шаг 1. Просмотр всех списков доступа

Выполните следующую команду на маршрутизаторе `2600A`, чтобы отобразить все существующие списки доступа:

```
show access-list
```

```
2600A#show access-list
Standard IP access list 20
    10 deny host 172.16.50.3 (5 match(es))
    20 permit any (4 match(es))
Extended IP access list 110
    10 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (36 match(es))
    20 permit ip any any (64 match(es))
```

Шаг 2. Проверка списка `110`

Для проверки содержимого созданного ранее списка доступа с номером `110`, выполните:

```
show access-list 110
```

```
2600A#show access-list 110
Extended IP access list 110
    deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (36 match(es))
    permit ip any any (71 match(es))
```

Шаг 3. Просмотр только IP списков доступа

Отобразите только `IP` списки доступа, применённые на маршрутизаторе:

```
show ip access-list
```

```
2600A#show ip access-list
Standard IP access list 20
    10 deny host 172.16.50.3 (5 match(es))
    20 permit any (4 match(es))
Extended IP access list 110
    10 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (36 match(es))
    20 permit ip any any (73 match(es))
```

Шаг 4. Проверка интерфейсов с применёнными списками доступа

Чтобы определить, на каких интерфейсах маршрутизатора применены списки доступа, выполните:

```
show ip interface
```

```
Serial0/0 is up, line protocol is up (connected)
  Internet address is 172.16.20.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 110
```