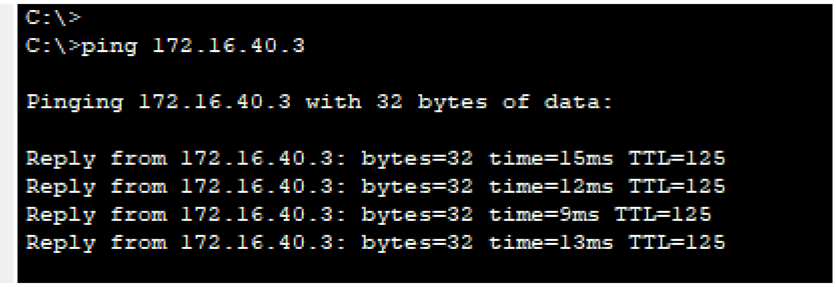
Лабораторная работа №4.

Списки доступа

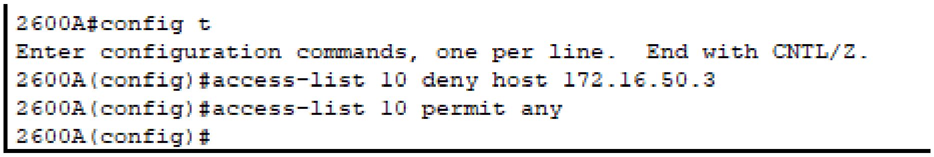
В этой лабораторной заблокируется доступ к сети 172.16.40.0 от узла Host F. Используется лабораторная топология настроенная в предыдущих заданиях.

1. Проверьте нормально ли выполняется ping хоста Host E с хоста Host F.



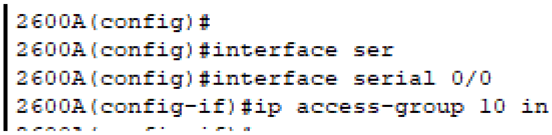
```
C:\>
C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Reply from 172.16.40.3: bytes=32 time=15ms TTL=125
Reply from 172.16.40.3: bytes=32 time=12ms TTL=125
Reply from 172.16.40.3: bytes=32 time=9ms TTL=125
Reply from 172.16.40.3: bytes=32 time=13ms TTL=125
```

2. На маршрутизаторе 2600A создайте список доступа, который заблокирует доступ от узла F на подсеть 172.16.40.0.



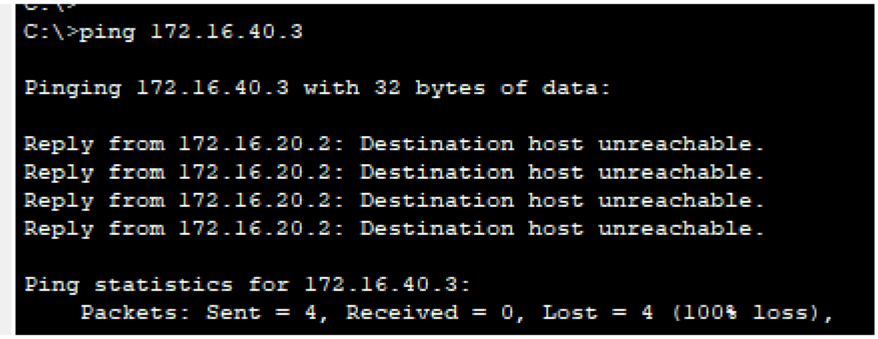
```
2600A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
2600A(config)#access-list 10 deny host 172.16.50.3
2600A(config)#access-list 10 permit any
2600A(config)#
```

3. Применим список доступа к интерфейсу serial 0/0 маршрутизатора 2600A для входящего в интерфейс потока пакетов.



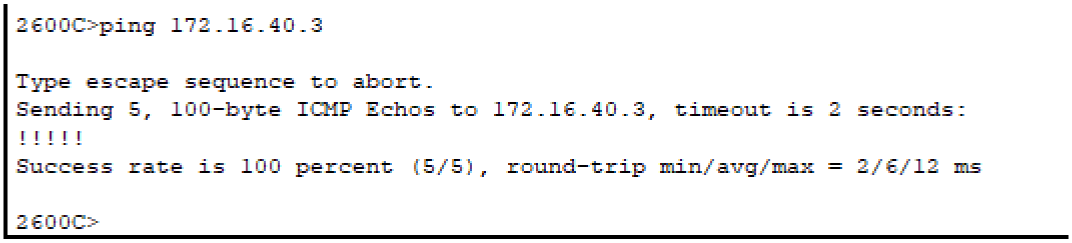
```
2600A(config)#
2600A(config)#interface ser
2600A(config)#interface serial 0/0
2600A(config-if)#ip access-group 10 in
```

4. Убедимся, что узел F не может больше пинговать 172.16.40.3.



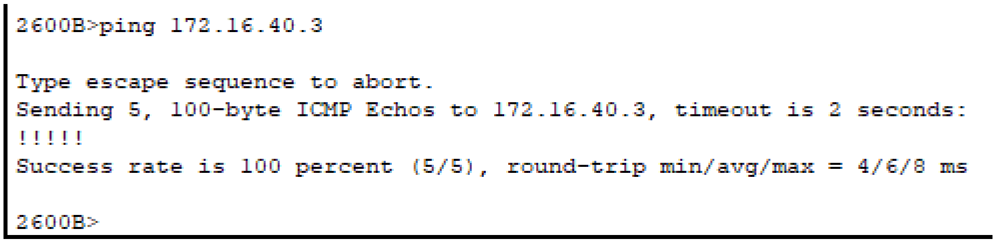
```
C:\>ping 172.16.40.3

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),
```

5. Проверьте, что все остальные устройства по-прежнему могут пинговать подсеть 172.16.40.0.
Сделайте, например, Ping с 2600C на 172.16.40.3.
2600C:



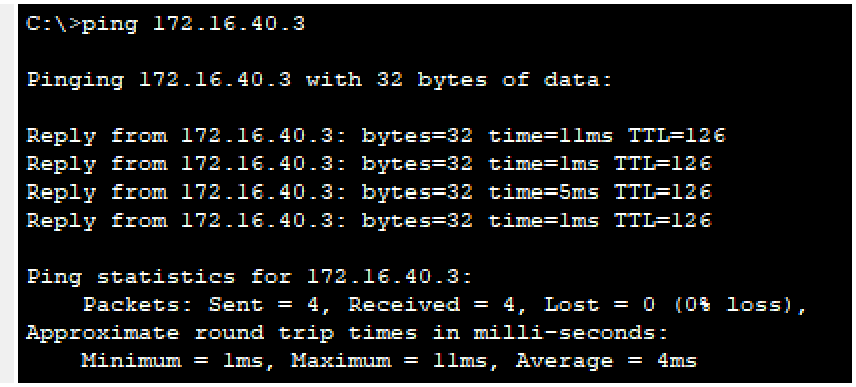
```
2600C>ping 172.16.40.3

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 = 2/6/12 ms

2600C>
```

2600B:



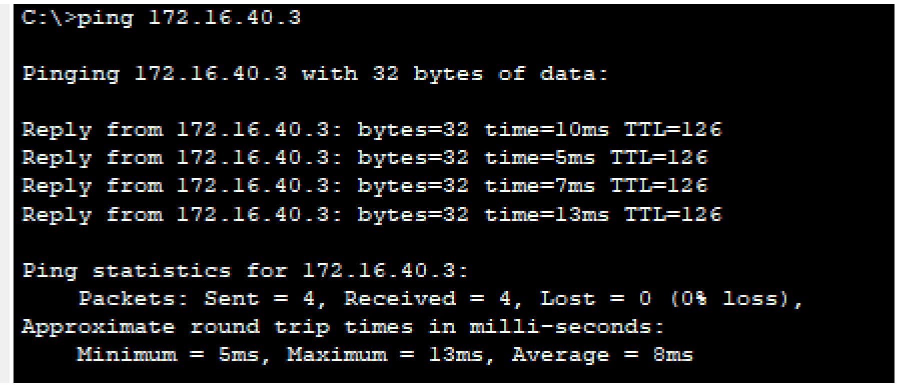
```
2600B>ping 172.16.40.3

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 = 4/6/8 ms

2600B>
```

HostA:



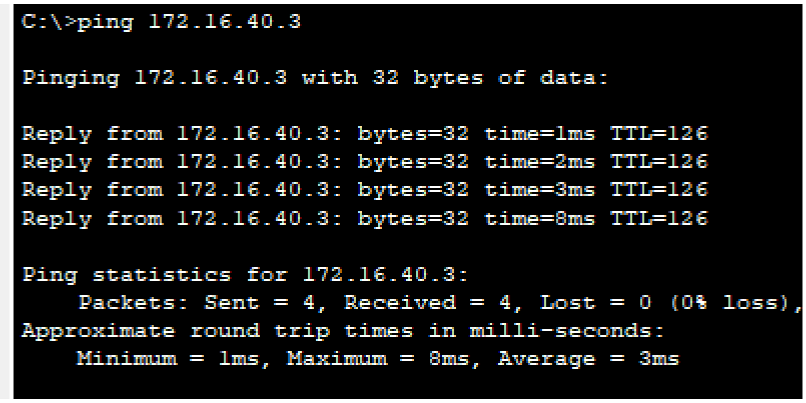
```
C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Reply from 172.16.40.3: bytes=32 time=11ms TTL=126
Reply from 172.16.40.3: bytes=32 time=1ms TTL=126
Reply from 172.16.40.3: bytes=32 time=5ms TTL=126
Reply from 172.16.40.3: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms
```

HostG:



```
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=10ms TTL=126
Reply from 172.16.40.3: bytes=32 time=5ms TTL=126
Reply from 172.16.40.3: bytes=32 time=7ms TTL=126
Reply from 172.16.40.3: bytes=32 time=13ms TTL=126

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 = 13ms, Average = 8ms
```

HostD:

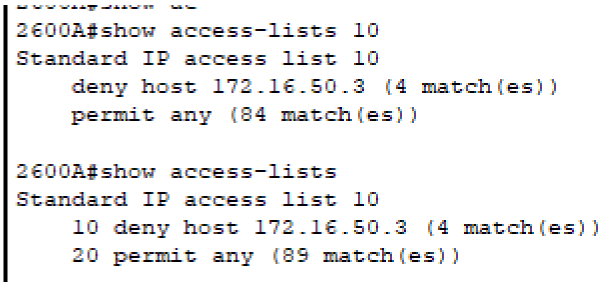


```
C:\>ping 172.16.40.3

Pinging 172.16.40.3 with 32 bytes of data:

Reply from 172.16.40.3: bytes=32 time=1ms TTL=126
Reply from 172.16.40.3: bytes=32 time=2ms TTL=126
Reply from 172.16.40.3: bytes=32 time=3ms TTL=126
Reply from 172.16.40.3: bytes=32 time=8ms TTL=126

Ping statistics for 172.16.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

4.2: Проверка работы стандартных списков доступа

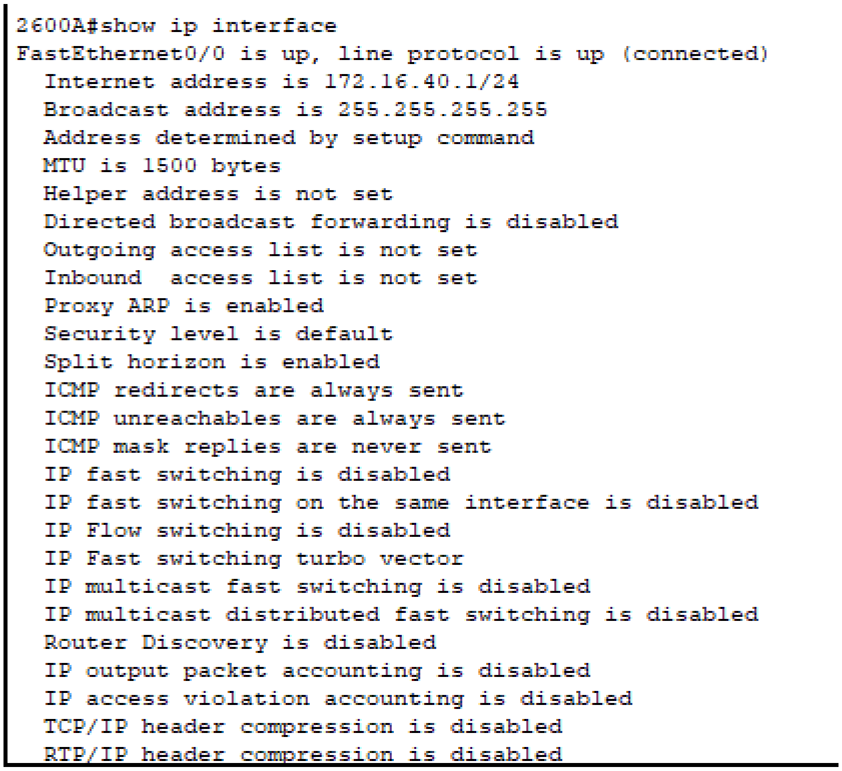
1. Выполните на 2600A show access-list
2. Можно также посмотреть конкретный список, например, 10.

   1 и 2



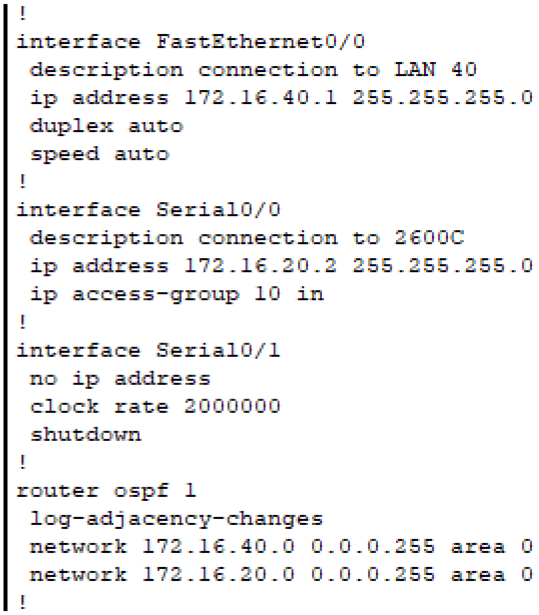
```
2600A#show access-lists 10
Standard IP access list 10
    deny host 172.16.50.3 (4 match(es))
    permit any (84 match(es))

2600A#show access-lists
Standard IP access list 10
    10 deny host 172.16.50.3 (4 match(es))
    20 permit any (89 match(es))
```

3. Для определения на каких интерфейсах применены списки доступа, выполните show ip interface.



```
2600A#show ip interface
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 172.16.40.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  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
```

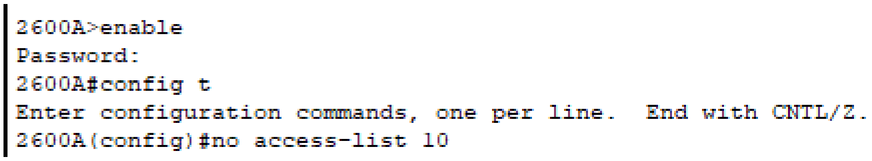
4. Также можно посмотреть списки и их применения в конфигурации running-config.



```
!
interface FastEthernet0/0
 description connection to LAN 40
 ip address 172.16.40.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 description connection to 2600C
 ip address 172.16.20.2 255.255.255.0
 ip access-group 10 in
!
interface Serial0/1
 no ip address
 clock rate 2000000
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.16.40.0 0.0.0.255 area 0
 network 172.16.20.0 0.0.0.255 area 0
!
```

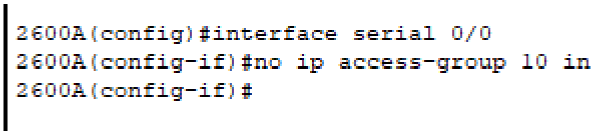
4.3: Применение списков доступа к линиям VTY

1. Удалим ненужный список доступа на 2600A.



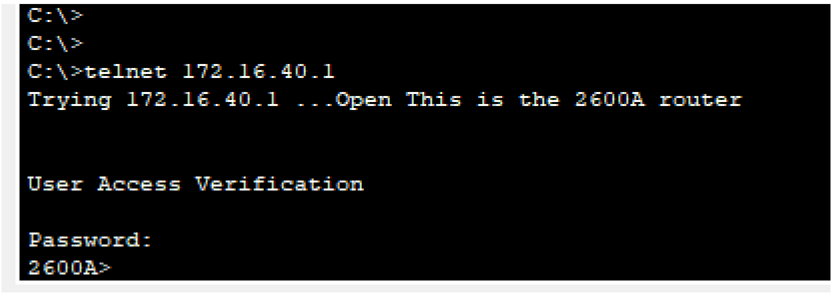
```
2600A>enable
Password:
2600A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
2600A(config)#no access-list 10
```

2. Удалим применение списка.



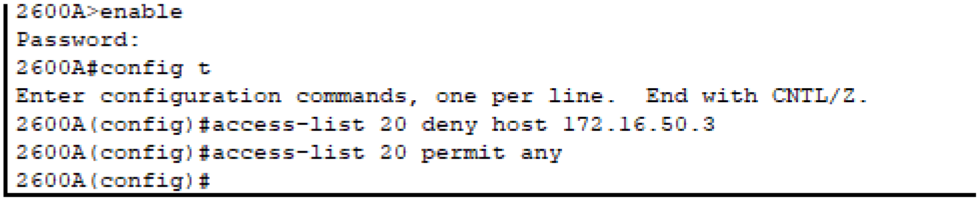
```
2600A(config)#interface serial 0/0
2600A(config-if)#no ip access-group 10 in
2600A(config-if)#
```

3. Проверьте, что с узла F можно выполнить telnet на маршрутизатор 2600A.



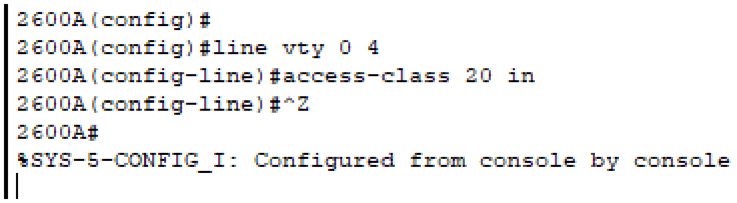
```
C:\>
C:\>
C:\>telnet 172.16.40.1
Trying 172.16.40.1 ...Open This is the 2600A router


User Access Verification

Password:
2600A>
```

4. На маршрутизаторе 2600 заблокируйте telnet-доступ с узла F, но разрешите с любых других адресов.



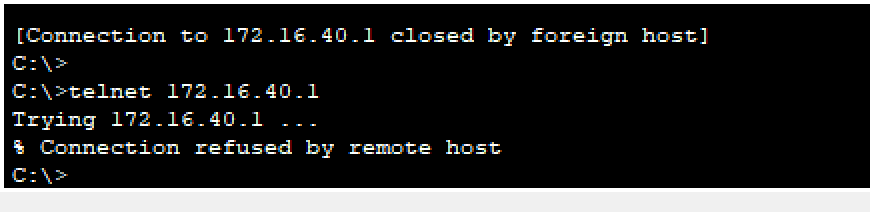
```
2600A>enable
Password:
2600A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
2600A(config)#access-list 20 deny host 172.16.50.3
2600A(config)#access-list 20 permit any
2600A(config)#
```

5. Примените список к линиям 0,1,2,3,4 VTY.



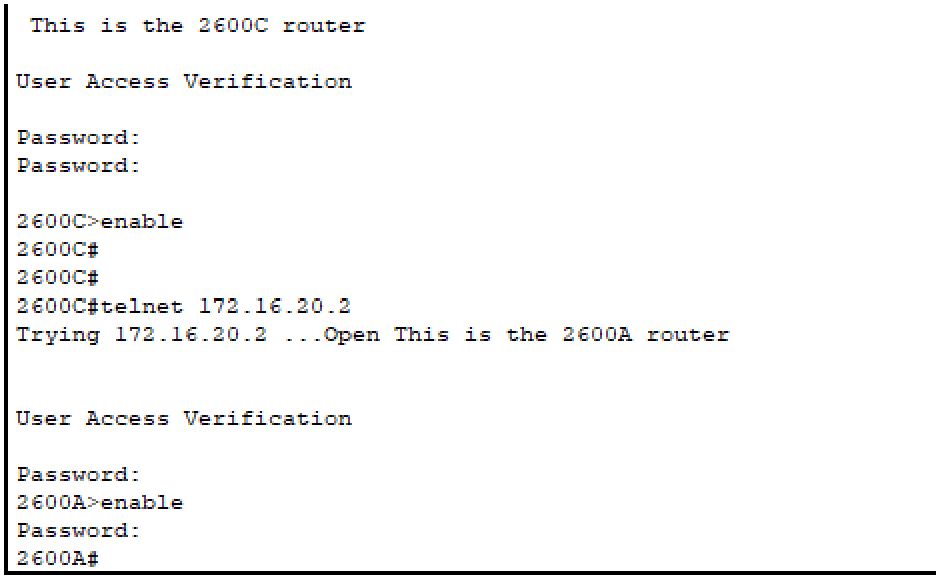
```
2600A(config)#
2600A(config)#line vty 0 4
2600A(config-line)#access-class 20 in
2600A(config-line)#^Z
2600A#
%SYS-5-CONFIG_I: Configured from console by console
|
```

6. Убедитесь, что теперь нельзя сделать telnet с узла F на 2600A.



```
[Connection to 172.16.40.1 closed by foreign host]
C:\>
C:\>telnet 172.16.40.1
Trying 172.16.40.1 ...
% Connection refused by remote host
C:\>
```

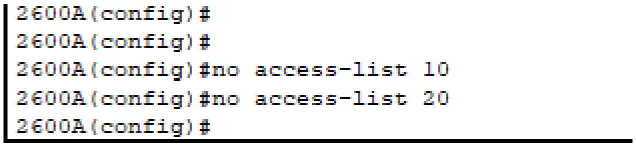
7. Убедитесь, что можно сделать telnet с 2600C на 2600A.



```
 This is the 2600C router

User Access Verification

Password:
Password:

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


User Access Verification

Password:
2600A>enable
Password:
2600A#
```

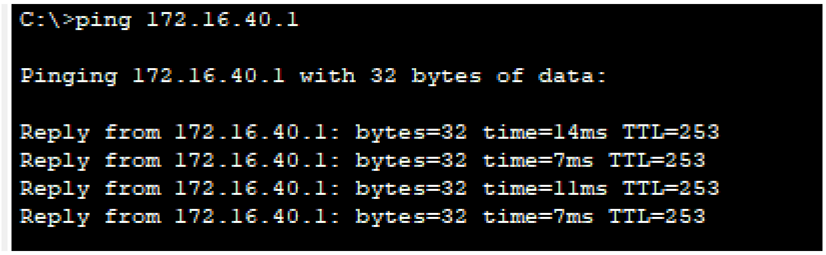
4.4: Расширенные списки доступа (Extended IP Access-Lists)

1. Удаляем стандартный список доступа с 2600A из прошлой лабораторной

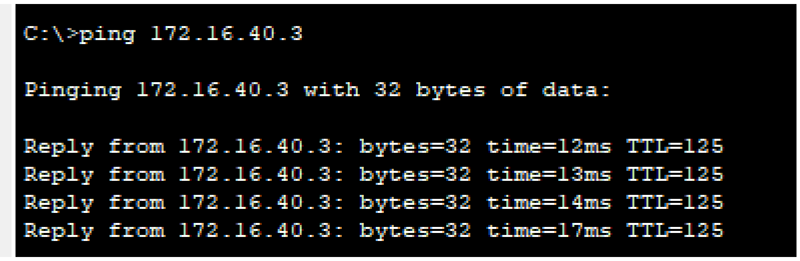


```
2600A(config)#
2600A(config)#
2600A(config)#no access-list 10
2600A(config)#no access-list 20
2600A(config)#
```

2. Проверяем, что хост F может теперь выполнять ping на 172.16.40.1 и 172.16.40.3.

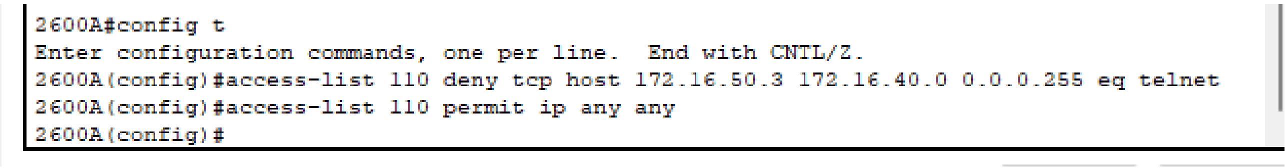


```
C:\>ping 172.16.40.1

Pinging 172.16.40.1 with 32 bytes of data:

Reply from 172.16.40.1: bytes=32 time=14ms TTL=253
Reply from 172.16.40.1: bytes=32 time=7ms TTL=253
Reply from 172.16.40.1: bytes=32 time=11ms TTL=253
Reply from 172.16.40.1: bytes=32 time=7ms TTL=253
```



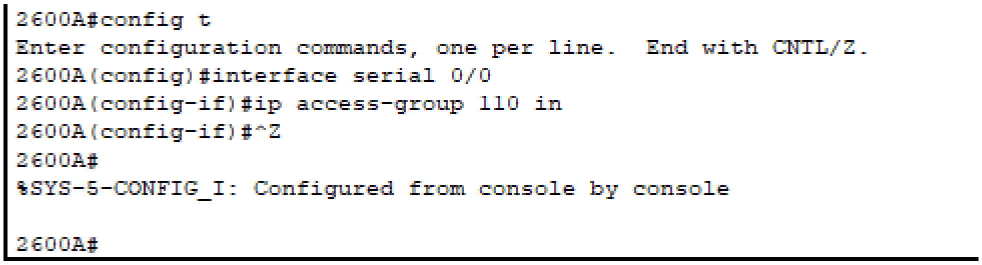
```
C:\>ping 172.16.40.3

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=13ms TTL=125
Reply from 172.16.40.3: bytes=32 time=14ms TTL=125
Reply from 172.16.40.3: bytes=32 time=17ms TTL=125
```

3. Создаем список доступа на 2600A для блокирования telnet-доступа в подсеть 172.16.40.0, но, тем не менее, позволяем хосту F делать ping на хост E.



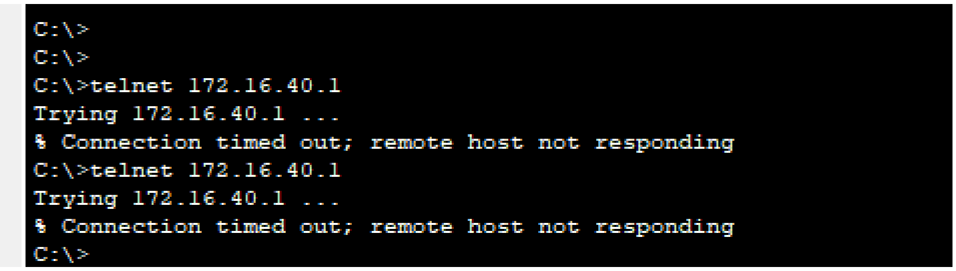
```
2600A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
2600A(config)#access-list 110 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet
2600A(config)#access-list 110 permit ip any any
2600A(config)#
```

4. Применяем сформированный таким образом расширенный список доступа к последовательному интерфейсу 0/0 маршрутизатора 2600A для входящих пакетов.



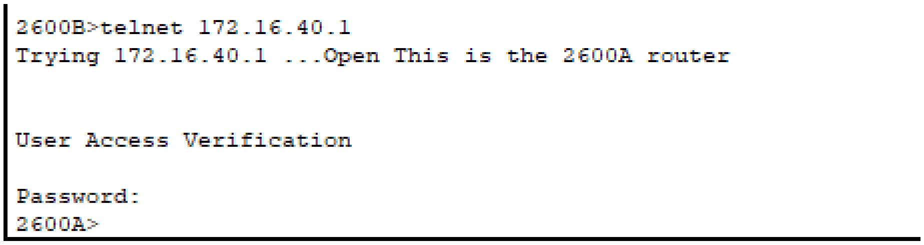
```
2600A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
2600A(config)#interface serial 0/0
2600A(config-if)#ip access-group 110 in
2600A(config-if)#^Z
2600A#
%SYS-5-CONFIG_I: Configured from console by console

2600A#
```

5. Проверяем, пытаясь сделать telnet на 172.16.40.1 с хостаF. Все прочие устройства должны иметь возможность делать telnet на 172.16.40.1.
HostF



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

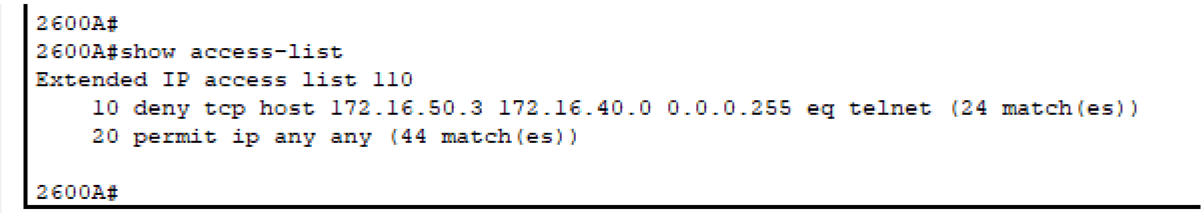
2600B



```
2600B>telnet 172.16.40.1
Trying 172.16.40.1 ...Open This is the 2600A router


User Access Verification

Password:
2600A>
```

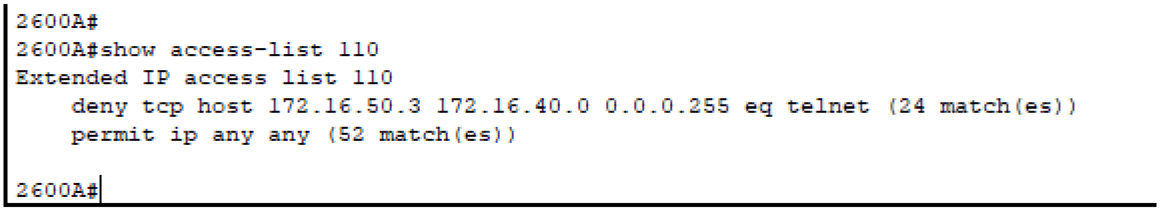
4.5: Проверка расширенных списков доступа

1. На 2600А выполните show access-list



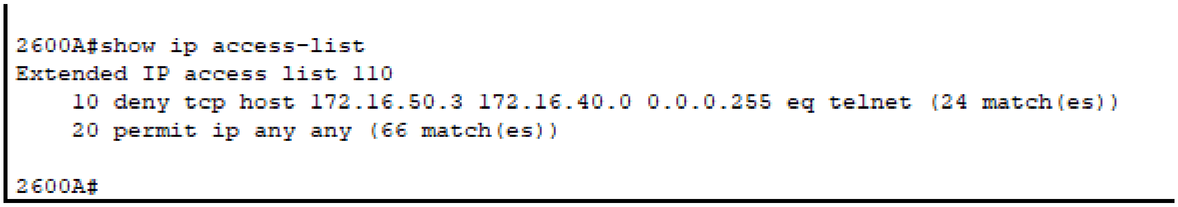
```
2600A#
2600A#show access-list
Extended IP access list 110
    10 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (24 match(es))
    20 permit ip any any (44 match(es))

2600A#
```

2. Проверьте список 110 с помощью show access-list 110.



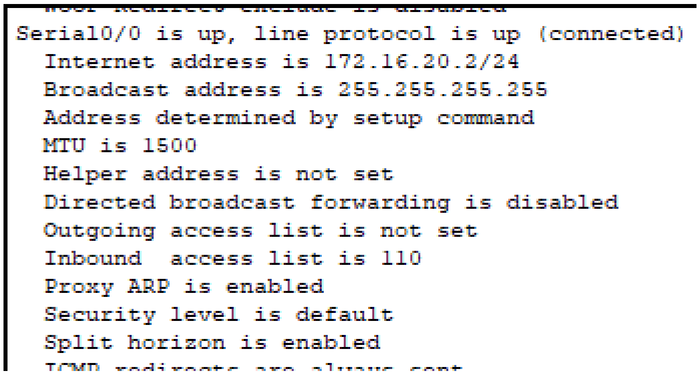
```
2600A#
2600A#show access-list 110
Extended IP access list 110
    deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (24 match(es))
    permit ip any any (52 match(es))

2600A#
```

3. Выполните просмотр только IP списков



```
2600A#show ip access-list
Extended IP access list 110
    10 deny tcp host 172.16.50.3 172.16.40.0 0.0.0.255 eq telnet (24 match(es))
    20 permit ip any any (66 match(es))

2600A#
```

4. Для определения на каких интерфейсах применены списки доступа выполните show ip interface



```
  WCCP Redirect exclude is disabled
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
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
```

....