




		Source				Destination				
R2(config)#										
access-list	100	deny	tcp	10.10.30.0	0.0.0.255	gt	49151	10.10.20.1	0.0.0.0	eq 23
	No.	Action	Protocol	IP	Wildcard	Qual.	Port	IP	Wildcard	Qual. Port

## Numbered Standard ACL

- 1) **Verify that all PCs have connectivity to each other, to R1 and to R2**  
Yes, all PCs are able to ping each other and the routers
- 2) **Configure and apply a numbered standard ACL on R1 which denies traffic from all hosts in the 10.0.2.0/24 subnet to R2**  
Access-list 1 deny 10.0.2.0 0.0.0.255 # Denies all Traffic especially from src 10.0.2.0/24  
Access-list 1 permit 10.0.1.0 0.0.0.255 # Accepts traffic from src 10.0.1.0/24  
Interface config f0/0  
Ip access-group 1 out
- 3) **Test that traffic is secured exactly as required**  
Verify PC1 and PC2 can Ping R2   
PC3 cannot ping R2   
PC3 can ping PC1 and PC2 

### PC3 to R2

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Ping statistics for 10.0.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

### PC3 to PC1

C:\>ping 10.0.1.10

Pinging 10.0.1.10 with 32 bytes of data:

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.1.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

### **PC3 to PC2**

C:\>ping 10.0.1.11

Pinging 10.0.1.11 with 32 bytes of data:

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.1.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

### **PC1 to R2**

C:\>ping 10.0.1.11

Pinging 10.0.1.11 with 32 bytes of data:

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Reply from 10.0.1.11: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.1.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

### **PC2 to R2**

C:\>ping 10.0.1.11

Pinging 10.0.1.11 with 32 bytes of data:

Reply from 10.0.1.11: bytes=32 time=16ms TTL=128

Reply from 10.0.1.11: bytes=32 time=5ms TTL=128

Reply from 10.0.1.11: bytes=32 time=6ms TTL=128

Reply from 10.0.1.11: bytes=32 time=3ms TTL=128

Ping statistics for 10.0.1.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 3ms, Maximum = 16ms, Average = 7ms

## Numbered Extended ACL

- 4) **Configure and apply a numbered extended ACL on R1 which permits telnet access from PC1 to R2. Telnet to R2 must be denied for all other PCs in the network**

**All other connectivity must be maintained**

**Don't change the existing ACL**

**Telnet access has already been enabled on R2. The password is "Flackbox"**

### **Answer:**

PC1 to R2:

[Connection to 10.0.0.2 closed by foreign host]

C:\>telnet 10.0.0.2

Trying 10.0.0.2 ...Open

User Access Verification

Password:

Password:

R2>

PC2 to R2:

C:\>telnet 10.0.0.2

Trying 10.0.0.2 ...

% Connection timed out; remote host not responding

PC3 to R2:

C:\>telnet 10.0.0.2

Trying 10.0.0.2 ...

% Connection timed out; remote host not responding

- 5 ) **Test that traffic is secured exactly as required. Use the command 'telnet 10.0.0.2' from the PCs to test and the password 'Flackbox'. Type 'exit' to leave the Telnet session.**

**Verify that PC1 can ping and Telnet to R2** 

**PC2 can ping R2 but not Telnet to it. PC3 cannot ping or Telnet to R2** 

**The PCs can all ping each other** 

- 6) **How many Telnet packets were permitted by the ACL?**

Standard IP access list 1

10 deny 10.0.2.0 0.0.0.255 (20 match(es))

20 permit 10.0.1.0 0.0.0.255 (193 match(es))

Extended IP access list 100

```
10 permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet (72 match(es))  
20 deny tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq telnet (12 match(es))  
30 permit ip any any
```

## Named Extended ACL

**7) Remove the numbered extended ACL you just configured from the interface.  
DO not delete the ACL**

R1(config-if)# no ip access-list 100


**8) Configure and apply a named extended ACL on R1 as follows:**

- **Permit Telnet from PC1 to R2. Telnet must be denied for all other pcs in the network**
- **Permit ping from PC2 to R2. Ping to R2 must be denied by all other PCs in the network**
- **All other connectivity must be maintained**


*Answer:*

```
ip access-list extended Flackbox-demo  
permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet  
deny icmp host 10.0.1.10 host 10.0.0.2  
permit icmp host 10.0.1.11 host 10.0.0.2  
permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

**9) Test that the traffic is secured as required:**

Verify that PC1 cannot ping R2 but can Telnet to it 

PC2 can ping R2 but cannot Telnet to it 

PC3 cannot ping or Telnet to R2 

The PCs can all ping each othe. 