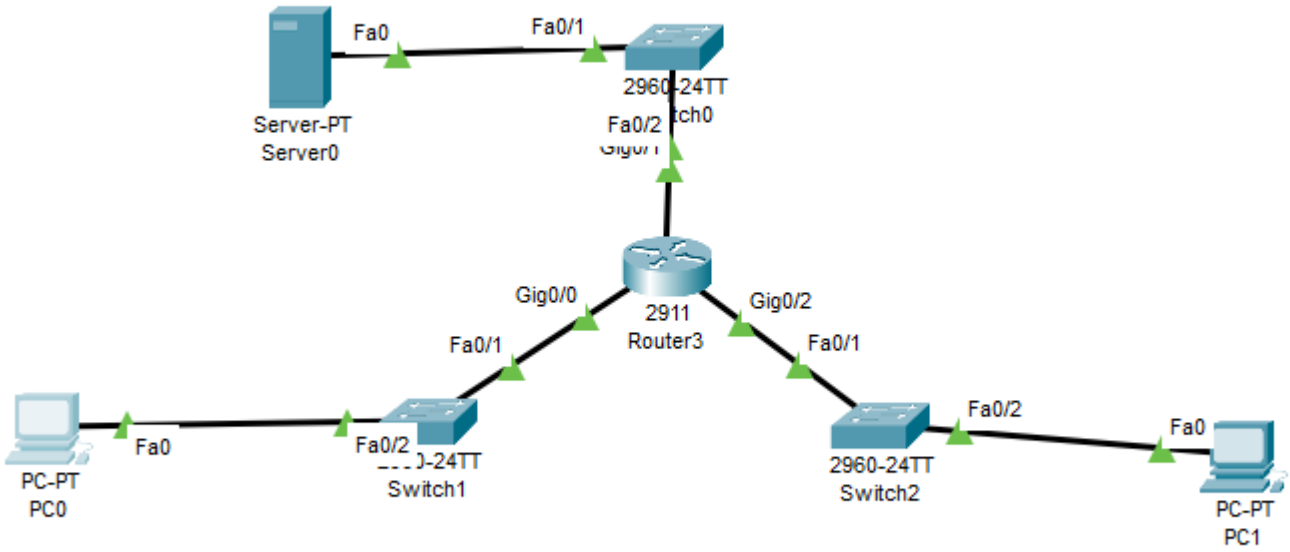
VSIT

Security in Computing
Practical #3

Name	Sanjeev Gupta	**Roll Number**	21302B0023
Class	TYBSc IT	**Division**	C
Subject/Course	Security in Computing		
Topic	Configuring Extended ACLs		

1 Configure, Apply and Verify an Extended Numbered ACL
2 Extended Numbered ACL



DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK	DEFAULT GATEWAY
Server 0	Fa0	172.22.34.2	255.255.255.192	172.22.34.1
Router	Gig0/1	172.22.34.1	255.255.255.192	NA
	Gig0/0	172.22.34.65	255.255.255.224	
	Gig0/2	172.22.34.97	255.255.255.240	
PC0	Fa0	172.22.34.66	255.255.255.224	172.22.34.65
PC1	Fa0	172.22.34.98	255.255.255.240	172.22.34.97

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure an ACL to permit FTP and ICMP.

a. From global configuration mode on R1, enter the following command to determine the first valid number for an extended access list.

R1(config)# access-list?

b. Add 100 to the command, followed by a question mark.

R1(config)# access-list 100?

c. To permit FTP traffic, enter permit, followed by a question mark.

R1(config)# access-list 100 permit?

d. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. Therefore, enter tcp to further refine the ACL help.
R1(config)# access-list 100 permit tcp ?
e. Notice that we could filter just for PC1 by using the host keyword or we could allow any host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.
R1(config)# access-list 100 permit tcp 172.22.34.64?
f. Calculate the wildcard mask determining the binary opposite of a subnet mask.
11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31
g. Enter the wildcard mask, followed by a question mark.
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31?
h. Configure the destination address. In this scenario, we are filtering traffic for a single destination, which is the server. Enter the host keyword followed by the server's IP address.
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62?
i. Notice that one of the options is <cr> (carriage return). In other words, you can press Enter and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the eq keyword, followed by a question mark to display the available options. Then, enter ftp and press Enter.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?(shows protocols)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
j. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC1 to Server. Note that the access list number remains the same and no particular type of ICMP traffic needs to be specified.
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
k. All other traffic is denied, by default.

```
Router(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.2 eq ftp
Router(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.2
```

Step 2: Apply the ACL on the correct interface to filter traffic.
From R1's perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.
R1(config)# interface gigabit Ethernet 0/0
R1(config-if) # Ip access-group 100 in

```
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#
```

Step 3: Verify the ACL implementation.
a. Ping from PC1 to Server. If the pings are unsuccessful, verify the IP addresses before

continuing.
b. FTP from PC1 to Server. The username and password are both cisco.
PC> ftp 172.22.34.62
c. Exit the FTP service of the Server.
ftp> quit
d. Ping from PC1 to PC2. The destination host should be unreachable, because the traffic was not
explicitly permitted.
PC1:

```
C:\>ping 172.22.34.2

Pinging 172.22.34.2 with 32 bytes of data:

Reply from 172.22.34.2: bytes=32 time<1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 172.22.34.2
Trying to connect...172.22.34.2
Connected to 172.22.34.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

```
C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Part 2: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access and ICMP.
a. Named ACLs start with the Ip keyword. From global configuration mode of R1, enter the following command, followed by a question mark.
R1(config)# Ip access-list?
b. You can configure named standard and extended ACLs. This access list filters both source and
destination IP addresses; therefore, it must be extended. Enter HTTP_ONLY as the name. (For Packet Tracer scoring, the name is case-sensitive.)
R1(config)# Ip access-list extended HTTP_ONLY
c. The prompt changes. You are now in extended named ACL configuration mode. All devices on
the PC2 LAN need TCP access. Enter the network address, followed by a question mark.
R1(config-ext-nacl)# permit tcp 172.22.34.96?
d. An alternative way to calculate a wildcard is to subtract the subnet mask from 255.255.255.255.
255.255.255.255
- 255.255.255.240

= 0. 0. 0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15?
e. Finish the statement by specifying the server address as you did in Part 1 and filtering www traffic.
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
f. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC2 to Server. Note: The prompt remains the same and a specific type of ICMP traffic does not need to be specified.
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
g. All other traffic is denied, by default. Exit out of extended named ACL configuration mode.
Step 2: Apply the ACL on the correct interface to filter traffic.
From R1's perspective, the traffic that access list HTTP_ONLY applies to is inbound from the network connected to Gigabit Ethernet 0/1 interface. Enter the interface configuration mode and apply the ACL.
R1(config)# interface gigabit Ethernet 0/1
R1(config-if) # Ip access-group HTTP_ONLY in

```
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended HTTP_ONLY
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.2
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.2 eq www
Router(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.2
Router(config-ext-nacl)#interface gigabitEthernet 0/2
Router(config-if)#ip access-group HTTP_ONLY in
Router(config-if)#exit
Router(config)#
```

Step 3: Verify the ACL implementation.

a. Ping from PC2 to Server. The ping should be successful, if the ping is unsuccessful, verify the IP

addresses before continuing.

b. FTP from PC2 to Server. The connection should fail.

c. Open the web browser on PC2 and enter the IP address of Server as the URL. The connection should be successful.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.2

Pinging 172.22.34.2 with 32 bytes of data:

Reply from 172.22.34.2: bytes=32 time=1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127
Reply from 172.22.34.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ftp 172.22.34.2
Trying to connect...172.22.34.2
Connected to 172.22.34.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
```