Configure, Apply and Verify an Extended Numbered ACL

1. **Configure an ACL to permit FTP and ICMP.**

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host**

**172.22.34.62 eq ftp**

R1(config)# **access-list 100 permit icmp 172.22.34.64 0.0.0.31 host**

**172.22.34.62**

1. **Apply the ACL on the correct interface to filter traffic.**

R1(config)# **interface gigabitEthernet 0/0**

Verify the ACL implementation.

* 1. a. Ping from **PC1** to **Server**. If the pings are unsuccessful, verify the IP addresses before continuing.
  2. b. FTP from **PC1** to **Server**. The username and password are both **cisco**.

1. PC> ftp 172.22.34.62
   1. c. Exit the FTP service of the **Server**.
2. ftp> quit
   1. d. Ping from **PC1** to **PC2**. The destination host should be unreachable, because the traffic was not explicitly permitted.

**Configure, Apply and Verify an Extended Named ACL**

1. **Configure an ACL to permit HTTP access and ICMP.**

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

1. **Apply the ACL on the correct interface to filter traffic.**

R1(config)# **interface gigabitEthernet 0/1**

R1(config-if)# **ip access-group HTTP\_ONLY in**

1. Verify the ACL implementation
2. a. Ping from **PC2** to **Server**. The ping should be successful, if the ping is unsuccessful, verify the IP addresses before continuing.
3. b. FTP from **PC2** to **Server**. The connection should fail.
4. c. Open the web browser on **PC2** and enter the IP address of **Server** as the URL. The connection should be successful.

**Configure, Apply and Verify an Extended Numbered ACL**

1. **Configure the extended ACL**

access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq 22

access-list 199 permit icmp any any

1. **Apply the extended ACL.**

ip access-group 199 out

**Verify the extended ACL implementation.**

1. a. Ping from **PCB** to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.
2. b. SSH from **PCB** to **SWC**. The username is **Admin**, and the password is **Adminpa55**.

PC> ssh -l Admin 10.101.117.2

1. c. Exit the SSH session to SWC.
2. d. Ping from **PCA** to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.
3. e. SSH from **PCA** to **SWC**. The access list causes the router to reject the connection.