**Configuring Extended ACLs**

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

**Configure Switch and Router:**

**Step 1: Configure the IP address on switch**

SWA(config)#

int vlan 1

ip address 10.101.117.50 255.255.255.248

no shut

ip default-gateway 10.101.117.49

SWB(config)#

int vlan 1

ip address 10.101.117.34 255.255.255.240

no shut

ip default-gateway 10.101.117.33

SWC(config)#

int vlan 1

ip address 10.101.117.2 255.255.255.224

no shut

ip default-gateway 10.101.117.1

**Step 2: Configure the secret on all router and switch**

RTA/SW(config)# enable secret enpa55

**Step 3: Configure the console password on router and switch**

RTA/SW(config)#

line console 0

password conpa55

login

**Step 4: Test connectivity**

**Ping from PCA to PC-B.**

PCA>ping 10.101.117.35 (Successful)

**Ping from PCA to SWC.**

PCA>ping 10.101.117.2 (Successful)

**Ping from PCB to SWC.**

PCB>ping 10.101.117.2 (Successful)

**Part 1: Configure Switch and Router to support SSH Connection**

**Step 1: Configure domain name and crypto key for use with SSH. (all routers and switches)**

RTA/SW(config)# ip domain-name ccnasecurity.com

**Step 2: Configure users to login to SSH**

RTA/SW(config)# username admin secret adminpa55

**Step 3: Configure incoming vty lines**

RTA/SW(config)#

line vty 0 4

login local

crypto key generate rsa

How many bits in the modulus [512]: 1024

**Step 4: Verify the SSH Connection**

PCA> ssh -l Admin 10.101.117.34

Password: adminpa55

**SWB> connection**

PCA> ssh -l Admin 10.101.117.2

Password: adminpa55

**SWC> connection**

PCB> ssh -l Admin 10.101.117.50

Password: adminpa55

**SWA> connection**

PCB> ssh -l Admin 10.101.117.2

Password: adminpa55

**SWC> connection**

SWC> ssh -l Admin 10.101.117.50

Password: adminpa55

**SWA> connection**

SWC> ssh -l Admin 10.101.117.34

Password: adminpa55

**SWB>**

SWB> exit

**Part 2: Configure, Apply and Verify an Extended Numbered ACL**

**Step 1: Configure the extended ACL.**

RTA(config)# access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq 22

RTA(config)# access-list 199 permit icmp any any

**Step 2: Apply the extended ACL.**

RTA(config)# int gig0/2

RTA(config-if)# ip access-group 199 out

**Step 3: Verify the extended ACL implementation.**

1. **Ping from PCB to all of the other IP addresses in the network.**

PCB> ping 10.101.117.51 (Successful)

PCB> ping 10.101.117.2 (Successful)

1. **SSH from PCB to SWC.**
2. PCB> ssh -l Admin 10.101.117.2

Password:adminpa55

1. **Exit the SSH session to SWC.**

SWC>exit

1. **Ping from PCA to all of the other IP addresses in the network.**

PCA> ping 10.101.117.35 (Successful)

PCA> ping 10.101.117.2 (Successful)

1. **SSH from PCA to SWC**

PCA> ssh -l Admin 10.101.117.2

Connection timed out. Remote host not responding

1. **SSH from PCA to SWB.**

PCA> ssh -l Admin 10.101.117.34

Password: adminpa55

SWB >

1. **After logging into SWB, do not log out. SSH to SWC in privileged EXEC mode.**

SWB# ssh -l Admin 10.101.117.2

Password: adminpa55

SWC>