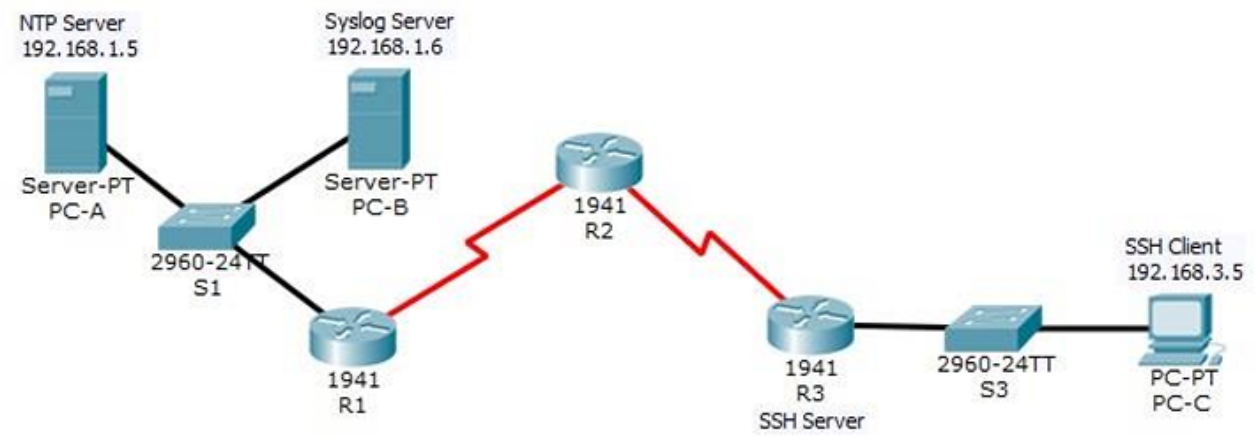
PRACTICAL 1

Practical 1 - Configure Routers

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

1A. OSPF MD5 authentication.

Step 1: Test connectivity. All devices should be able to ping all other IP addresses.

Step 2: Configure OSPF MD5 authentication for all the routers in area 0. Configure

OSPF MD5 authentication for all the routers in area 0.

R1(config)# router ospf 1

R1(config-router)# area 0 authentication message-digest

R2(config)# router ospf 1

R2(config-router)# area 0 authentication message-digest

R3(config)# router ospf 1

R3(config-router)# area 0 authentication message-digest

Step 3: Configure the MD5 key for all the routers in area 0. Configure an MD5 key on the serial

interfaces on R1, R2 and R3. Use the password MD5pa55 for key 1.

R1(config)# interface s0/0/0

R1(config-if)# ip ospf message-digest-key 1 md5 MD5pa55

R2(config)# interface s0/0/0

R2(config-if)# ip ospf message-digest-key 1 md5 MD5pa55

R2(config-if)# interface s0/0/1

R2(config-if)# ip ospf message-digest-key 1 md5 MD5pa55

R3(config)# interface s0/0/1

R3(config-if)# ip ospf message-digest-key 1 md5 MD5pa55

Step 4: Verify configurations.

a. Verify the MD5 authentication configurations using the commands show ip ospf interface. b.

Verify end-to-end connectivity.

1B. NTP.

Step 1: Enable NTP authentication on PC-A.

a. On PC-A, click NTP under the Services tab to verify NTP service is enabled.

b. To configure NTP authentication, click Enable under Authentication. Use key 1 and password NTPpa55

for authentication.

Step 2: Configure R1, R2, and R3 as NTP clients.

R1(config)# ntp server 192.168.1.5

R2(config)# ntp server 192.168.1.5

R3(config)# ntp server 192.168.1.5

Verify client configuration using the command show ntp status.

Step 3: Configure routers to update hardware clock. Configure R1, R2, and R3 to periodically

update the hardware clock with the time learned from NTP.

R1(config)# ntp update-calendar

R2(config)# ntp update-calendar

R3(config)# ntp update-calendar

Exit global configuration and verify that the hardware clock was updated using the command show clock.

Step 4: Configure NTP authentication on the routers. Configure NTP

authentication on R1, R2, and R3 using key 1 and password NTPpa55.

R1(config)# ntp authenticate

R1(config)# ntp trusted-key 1

R1(config)# ntp authentication-key 1 md5 NTPpa55

R2(config)# ntp authenticate

R2(config)# ntp trusted-key 1

R2(config)# ntp authentication-key 1 md5 NTPpa55

R3(config)# ntp authenticate

R3(config)# ntp trusted-key 1

R3(config)# ntp authentication-key 1 md5 NTPpa55

Step 5: Configure routers to timestamp log messages.

Configure timestamp service for logging on the routers.

R1(config)# service timestamps log datetime msec

R2(config)# service timestamps log datetime msec

R3(config)# service timestamps log datetime msec

1C. to log messages to the syslog server.

Step 1: Configure the routers to identify the remote host (Syslog Server) that will receive

logging messages.

R1(config)# logging host 192.168.1.6

R2(config)# logging host 192.168.1.6

R3(config)# logging host 192.168.1.6

The router console will display a message that logging has started.

Step 2: Verify logging configuration.

Use the command show logging to verify logging has been enabled.

Step 3: Examine logs of the Syslog Server.

From the Services tab of the Syslog Server's dialogue box, select the Syslog services button. Observe the

logging messages received from the routers.

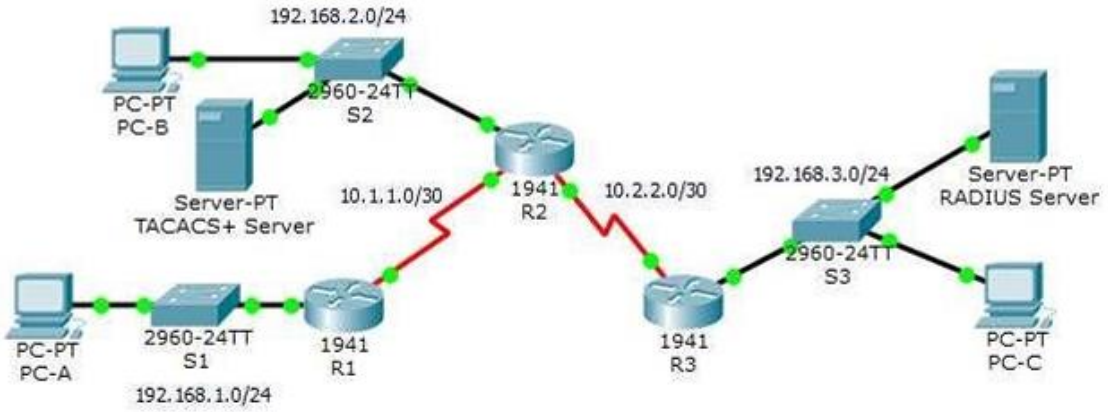
Note: Log messages can be generated on the server by executing commands on the router. For example,

entering and exiting global configuration mode will generate an informational configuration message. You may

need to click a different service and then click Syslog again to refresh the message display.

PRACTICAL 2

Practical 2 - Configure AAA Authentication



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

2A. Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA

Configure Local User Account on the Router:

1.Access the Router CLI
Connect to the router using the console or SSH.

2.Enable AAA on the Router

```
Router# configure terminal
Router(config)# aaa new-model
```

3.Create a Local User for Authentication

```
Router(config)# username admin privilege 15 secret Admin123
```

4.Configure Local Authentication for Console and VTY

```
Router(config)# aaa authentication login default local
Router(config)# line console 0
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# exit
```

Step 1: Configure domain name and crypto key for use with SSH.

a. Use ccnasecurity.com as the domain name on R1.

```
R1(config)# ip domain-name ccnasecurity.com
```

b. Create an RSA crypto key using 1024 bits.

```
R1(config)# crypto key generate rsa
```

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Step 2: Configure a named list AAA authentication method for the vty lines on R1.

Configure a named list called SSH-LOGIN to authenticate logins using local AAA.

R1(config)# aaa authentication login SSH-LOGIN local

Step 3: Configure the vty lines to use the defined AAA authentication method.

Configure the vty lines to use the named AAA method and only allow SSH for remote access.

R1(config)# line vty 0 4

R1(config-line)# login authentication SSH-LOGIN

R1(config-line)# transport input ssh R1(config-line)#

end

Step 4: Verify the AAA authentication method.

Verify the SSH configuration SSH to R1 from the command prompt of PC-A..

PC> ssh –l Admin1 192.168.1.1

Open

Password: admin1pa55

2B. Verify local AAA authentication from the Router console and the PC-A client

Step 1: Configure Local AAA Authentication on the Router

Access the Router CLI

Connect to the router using the console or SSH.

Enable AAA on the Router

```
Router# configure terminal
Router(config)# aaa new-model
```

Create a Local User for Authentication

```
Router(config)# username admin privilege 15 secret Admin123
```

Configure Local Authentication for Console and VTY

```
Router(config)# aaa authentication login default local
Router(config)# line console 0
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# exit
```

Step 2: Verify Local AAA Authentication from the Router Console

Log out of the router

```
Router# exit
```

Log back in via console

- You should be prompted for a username and password.
- Enter Username: admin
- Enter Password: Admin123
- If successful, you will get access to the router CLI.

Step 3: Verify Local AAA Authentication from PC-A Client

Option 1: Telnet Test

On PC-A, open the Command Prompt or Terminal.

Attempt to access the router via Telnet

telnet <router-ip>

When prompted, enter the username and password:

- Username: admin
- Password: Admin123

If successful, you should gain access to the router CLI.

Option 2: SSH Test

On PC-A, open the Command Prompt or Terminal.

Use SSH to connect to the router

ssh admin@<router-ip>

Enter the password when prompted

- Password: Admin123

If authentication succeeds, you will access the router CLI.

Step 4: Verify Authentication Logs (Optional)

To check authentication logs on the router, use:

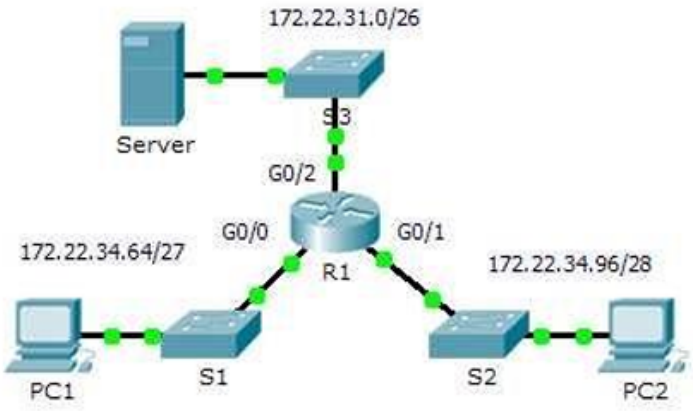
Router# show aaa sessions

Router# show users

PRACTICAL 3

Practical 3 - Configuring Extended ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

3. 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 ?

<1-99> IP standard access list

<100-199> IP extended access list

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

R1(config)# access-list 100 ?

deny

permit

Specify packets to reject

Specify packets to forward

remark Access list entry comment

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

R1(config)# access-list 100 permit ?

ahp Authentication Header Protocol

eigrp Cisco's EIGRP routing protocol

esp Encapsulation Security Payload

gre

Cisco's GRE tunneling icmp

Internet Control Message Protocol ip

Any Internet Protocol ospf OSPF

routing protocol tcp Transmission

Control Protocol udp User Datagram

Protocol

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 ?

A.B.C.D Source address

Any source host

single source host

host any A

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 ?

A.B.C.D Source wildcard bits

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 ?

A.B.C.D Destination address

host eq any Any destination Match only packets on a given port number

gt host Match only packets with a greater port number Match only

A single destination host

packets with a lower port number Match only

packets not on a given port number Match only

packets in the range of port numbers lt neq range Match only

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

?

dscp Match packets with given dscp value eq

Match only packets on a given port number established

gt Match only packets with a greater

established port number lt number neq

Match only packets with a lower port

Match only packets not on a given port

number precedence Match packets with given precedence value

range Match only packets in the range of port numbers

<cr>

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 ?

<0-65535> Port number ftp File

Transfer Protocol (21) pop3 Post Office

Protocol v3 (110) smtp Simple Mail

Transport Protocol (25) telnet Telnet (23)

www World Wide Web (HTTP, 80)

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.

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 gigabitEthernet 0/0

R1(config-if)# ip access-group 100 in

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.

PRACTICAL 4

Practical 4 - Configure IP ACLs to Mitigate Attacks and IPV6 ACLs

4A. Verify connectivity among devices before firewall configuration.

Step 1: Check Physical and Logical Connections

Ensure all cables are properly connected.

Verify interfaces are enabled on routers, switches, and PCs.

Run the following on each router/switch to check interface status:

show ip interface brief

Ensure interfaces are UP/UP and assigned correct IP addresses.

Step 2: Verify IP Address Configuration

On each PC, check the assigned IP:

Windows (Command Prompt):

ipconfig

Linux/macOS (Terminal):

ifconfig or ip a

On the router, verify interface IPs:

show running-config | section interface

Step 3: Test Connectivity Using Ping

From each PC to the Default Gateway (Router)

ping <router-ip>

Example:

ping 192.168.1.1

If successful, the PC can communicate with the router.

From Router to PC

ping <pc-ip>

Example:

ping 192.168.1.10

If successful, the router can reach the PC.

From PC to Another PC

ping <other-pc-ip>

If successful, devices can communicate within the same network.

From PC to Another Network

If multiple networks exist, try pinging a PC in another network:

ping <remote-pc-ip>

If unsuccessful, check routing settings.

Step 4: Verify Routing Configuration (For Multi-Network Setups)

On the router, check the routing table:

show ip route

Ensure routes to all networks exist.

If using Static Routes, verify they are correctly set:

show running-config | section ip route

Example of adding a static route:

ip route 192.168.2.0 255.255.255.0 192.168.1.2

If using Dynamic Routing (OSPF, EIGRP, etc.), check:

show ip protocols

show ip ospf neighbor # For OSPF

show ip eigrp neighbors # For EIGRP

Step 5: Test Connectivity Using Traceroute

From a PC, trace the path to another device:

tracert <destination-ip> # Windows

traceroute <destination-ip> # Linux/macOS

If the path stops unexpectedly, check for:

Misconfigured routes

Disabled interfaces

Incorrect subnet masks

Step 6: Verify DNS Resolution (If Applicable)

If testing internet connectivity, check if DNS resolution works:

nslookup google.com # Windows

dig google.com # Linux/macOS

If unsuccessful, check DNS settings on the router or PC.

Step 7: Ensure No Existing Firewall Rules Are Blocking Traffic

Before configuring a firewall, ensure no ACLs are blocking traffic:

show access-lists

show running-config | section access-list

Remove any ACLs temporarily if needed:

no access-list <ACL-ID>

Final Check

If all pings, traceroutes, and routing tests are successful, connectivity is verified, and you can proceed with firewall configuration.

4B. Use ACLs to ensure remote access to the routers is available only from management station PC-C.

Step 1: Identify IP Addresses

Router's management IP: (e.g., 192.168.1.1)

PC-C's IP: (e.g., 192.168.3.10)

Subnet Mask: 255.255.255.0

VTY lines used for SSH/Telnet: 0 - 4

Step 2: Enable SSH on the Router

Set a domain name

Router(config)# ip domain-name mynetwork.com

Generate SSH key (for SSH only)

Router(config)# crypto key generate rsa

Choose a key size of 1024 or higher.

Enable SSH & Local Authentication

Router(config)# ip ssh version 2

Router(config)# aaa new-model

Router(config)# username admin privilege 15 secret Admin123

Router(config)# line vty 0 4

Router(config-line)# login local

Router(config-line)# transport input ssh

Router(config-line)# exit

Step 3: Configure an ACL to Permit Only PC-C

Create an Access Control List (ACL)

Router(config)# access-list 100 permit tcp host 192.168.3.10 any eq 22

Router(config)# access-list 100 permit tcp host 192.168.3.10 any eq 23

Router(config)# access-list 100 deny tcp any any eq 22

Router(config)# access-list 100 deny tcp any any eq 23

Router(config)# access-list 100 permit ip any any

Permit SSH (port 22) & Telnet (port 23) only from PC-C.

Deny SSH/Telnet from any other device.

Allow all other traffic after applying restrictions.

Apply ACL to the VTY Lines

Router(config)# line vty 0 4

Router(config-line)# access-class 100 in

Router(config-line)# exit

Step 4: Verify the Configuration

Check the ACL

show access-lists 100

Ensure only PC-C is allowed for SSH/Telnet.

Test from PC-C

Try SSH/Telnet from PC-C:

ssh admin@192.168.1.1

or

telnet 192.168.1.1

Authentication should succeed.

Test from Any Other PC

Try SSH/Telnet from another device (e.g., PC-A or PC-B).

It should be denied.

Step 5: Monitor ACL Hits

To check if ACL is working:

show access-lists 100

show logging

4C. Configure ACLs on to mitigate attacks.

Step 1: Identify Common Threats & Protection Methods

Attack Type	**Mitigation Using ACLs**
Unauthorized Access	Allow only trusted management IPs
Denial of Service (DoS)	Limit ICMP and SYN flood attacks
Spoofing	Block private IPs on external interfaces
Malware Spread	Block unused or dangerous ports
Brute Force Attacks	Restrict SSH/Telnet access

Step 2: Create a Secure ACL

This ACL blocks malicious traffic while allowing legitimate communication.

Modify the IPs according to your network.

1. Block Private IP Spoofing (on Internet-Facing Interface)

Router(config)# ip access-list extended SECURE_ACL

Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any

Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any

Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any

✓ Blocks packets with private IPs from entering the internet-facing interface (anti-spoofing).

2. Block Unnecessary or Dangerous Services

Router(config-ext-nacl)# deny tcp any any eq 23 ! Block Telnet (use SSH instead)

Router(config-ext-nacl)# deny tcp any any eq 3389 ! Block Remote Desktop (RDP)

Router(config-ext-nacl)# deny udp any any eq 69 ! Block TFTP (used in attacks)

Router(config-ext-nacl)# deny udp any any eq 161 ! Block SNMP if not needed

Router(config-ext-nacl)# deny udp any any eq 514 ! Block syslog from unauthorized sources

✓ Prevents unauthorized remote access and exploitation of vulnerable services.

3. Prevent ICMP-Based Attacks

Router(config-ext-nacl)# deny icmp any any echo ! Block ICMP Ping (DDoS Prevention)

Router(config-ext-nacl)# deny icmp any any redirect ! Block malicious redirects

Router(config-ext-nacl)# permit icmp any any time-exceeded ! Allow traceroute functionality

Router(config-ext-nacl)# permit icmp any any unreachable ! Allow ICMP unreachable messages

✓ Limits ping-based DoS attacks while allowing necessary ICMP functions.

4. Restrict Remote Management (SSH Only from Admin PC)

Router(config-ext-nacl)# permit tcp host 192.168.3.10 any eq 22

Router(config-ext-nacl)# deny tcp any any eq 22

✓ Only allows SSH access from the Admin PC (192.168.3.10). Blocks others.

5. Allow Essential Traffic (Keep Network Functional)

Router(config-ext-nacl)# permit ip any any

✓ Ensures that legitimate traffic is not completely blocked.

Step 3: Apply the ACL to Interfaces

Apply ACL to the Internet-Facing Interface

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip access-group SECURE_ACL in

Router(config-if)# exit

✓ Applies ACL to filter incoming traffic from the internet.

Step 4: Verify and Monitor the ACL

Check ACL Configuration

show access-lists SECURE_ACL

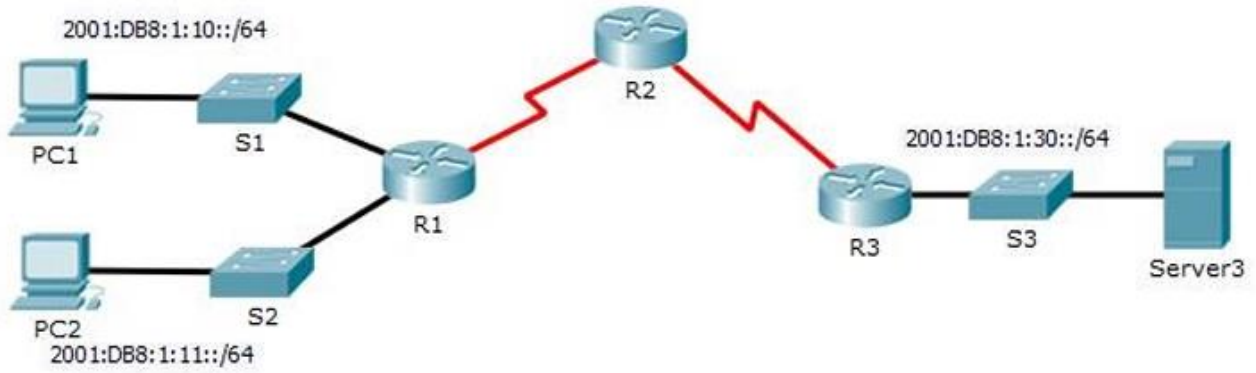
Monitor ACL Hits (Verify if Attacks are Blocked)

show ip access-list

show logging

4D. Configuring IPv6 ACLs

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named BLOCK_HTTP on R1 with the following statements. a.

Block HTTP and HTTPS traffic from reaching Server3.

R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www

R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443

b. Allow all other IPv6 traffic to pass.

R1(config)# permit ipv6 any any

Step 2: Apply the ACL to the correct interface. Apply the ACL on the

interface closest to the source of the traffic to be blocked.

R1(config)# interface GigabitEthernet0/1

R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in

Step 3: Verify the ACL implementation.

Verify that the ACL is operating as intended by conducting the following tests:

• Open the web browser of PC1 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website

should appear.

• Open the web browser of PC2 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website

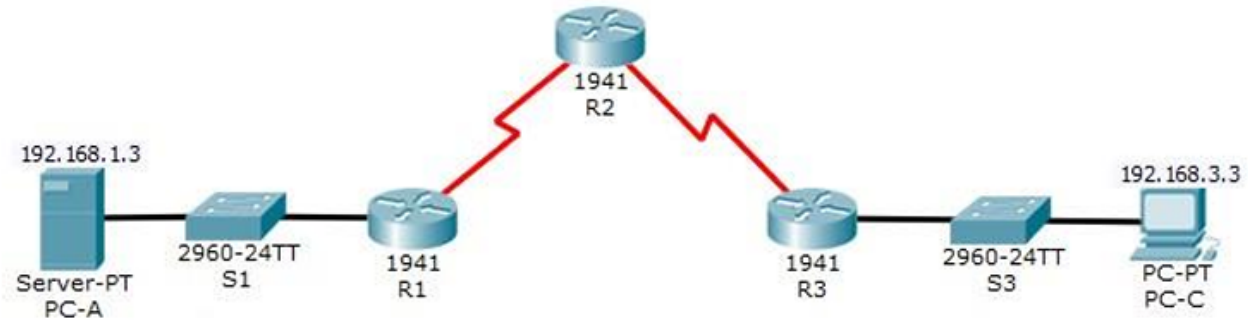
should be blocked.

• Ping from PC2 to 2001:DB8:1:30::30. The ping should be successful.

PRACTICAL 5

Practical 5 - Configuring a Zone-Based Policy Firewall

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

5. Configuring a Zone-Based Policy Firewall

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the zone-based policy firewall.

Step 1: From the PC-A command prompt, ping PC-C at 192.168.3.3.

Step 2: Access R2 using SSH.

a. From the PC-C command prompt, SSH to the S0/0/1 interface on R2 at 10.2.2.2. Use the username

Admin and password Adminpa55 to log in. PC> ssh -l Admin 10.2.2.2

b. Exit the SSH session.

Step 3: From PC-C, open a web browser to the PC-A server.

a. Click the Desktop tab and then click the Web Browser application. Enter the PC-A IP address

192.168.1.3 as the URL. The Packet Tracer welcome page from the web server should be displayed. b.

Close the browser on PC-C.

Part 2: Create the Firewall Zones on R3

Note: For all configuration tasks, be sure to use the exact names as specified.

Step 1: Enable the Security Technology package.

a. On R3, issue the show version command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the

package.

R3(config)# license boot module c1900 technology-package securityk9

c. Accept the end-user license agreement.

d. Save the running-config and reload the router to enable the security license.

e. Verify that the Security Technology package has been enabled by using the show version command.

Step 2: Create an internal zone. Use the zone security command

to create a zone named IN-ZONE. R3(config)# zone security

IN-ZONE

R3(config-sec-zone) exit

Step 3: Create an external zone. Use the zone security command to create a zone named OUT-ZONE.

R3(config-sec-zone)# zone security OUT-ZONE R3(config-sec

zone)# exit

Part 3: Identify Traffic Using a Class-Map

Step 1: Create an ACL that defines internal traffic.

Use the access-list command to create extended ACL 101 to permit all IP protocols from the 192.168.3.0/24

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any

Configuring a Zone-Based Policy Firewall (ZPF)

Step 2: Create a class map referencing the internal traffic ACL.

Use the class-map type inspect command with the match-all option to create a class map named IN

NETCLASS-MAP. Use the match access-group command to match ACL 101.

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP

R3(config-cmap)# match access-group 101

R3(config-cmap)# exit

Part 4: Specify Firewall Policies

Step 1: Create a policy map to determine what to do with matched traffic. Use the

policy-map type inspect command and create a policy map named IN-2-OUT-PMAP.

R3(config)# policy-map type inspect IN-2-OUT-PMAP

Step 2: Specify a class type of inspect and reference class map IN-NET-CLASS-MAP.

R3(config-pmap)# class type inspect IN-NET-CLASS-MAP

Step 3: Specify the action of inspect for this policy map.

The use of the inspect command invokes context-based access control (other options include pass and

drop).

R3(config-pmap-c)# inspect

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All

protocols will be inspected. Issue the exit command twice to leave config-pmap-c mode and

return to config mode.

R3(config-pmap-c)# exit

R3(config-pmap)# exit

Part 5: Apply Firewall Policies

Step 1: Create a pair of zones.

Using the zone-pair security command, create a zone pair named IN-2-OUT-ZPAIR. Specify the source and

destination zones that were created in Task 1.

R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination

OUTZONE

Step 2: Specify the policy map for handling the traffic between the two zones.

Attach a policy-map and its associated actions to the zone pair using the service-policy type inspect

command and reference the policy map previously created, IN-2-OUT-PMAP.

R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

R3(config-sec-zone-pair)# exit

R3(config)#

Step 3: Assign interfaces to the appropriate security zones.

Configuring a Zone-Based Policy Firewall (ZPF)

Use the zone-member security command in interface configuration mode to assign G0/1 to IN-ZONE and

S0/0/1 to OUT-ZONE.

R3(config)# interface g0/1

R3(config-if)# zone-member security IN-ZONE

R3(config-if)# exit

R3(config)# interface s0/0/1

R3(config-if)# zone-member security OUT-ZONE R3(config-if)#

exit

Step 4: Copy the running configuration to the startup configuration.

Part 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE

Verify that internal hosts can still access external resources after configuring the ZPF.

Step 1: From internal PC-C, ping the external PC-A server.

From the PC-C command prompt, ping PC-A at 192.168.1.3. The ping should succeed.

Step 2: From internal PC-C, SSH to the R2 S0/0/1 interface.

a. From the PC-C command prompt, SSH to R2 at 10.2.2.2. Use the username Admin and the password

Adminpa55 to access R2. The SSH session should succeed.

b. While the SSH session is active, issue the command show policy-map type inspect zone-pair sessions on R3 to view established sessions.

R3# show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR

Zone-pair: IN-2-OUT-ZPAIR

Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)

Match: access-group 101

Inspect

Number of Established Sessions = 1

Established Sessions

Session 175216232 (192.168.3.3:1028)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB

Created 00:00:25, Last heard 00:00:20

Bytes sent (initiator:responder) [1195:1256]

Class-map: class-default (match-any)

Match: any

Drop (default action)

0 packets, 0 bytes

What is the source IP address and port number?

_____

192.168.3.3:1028 (port 1028 is random)

What is the destination IP address and port number?

_____

10.2.2.2:22 (SSH = port 22)

Step 3: From PC-C, exit the SSH session on R2 and close the command prompt window.

Step 4: From internal PC-C, open a web browser to the PC-A server web page.

Enter the server IP address 192.168.1.3 in the browser URL field, and click Go. The HTTP session should

succeed. While the HTTP session is active, issue the command show policy-map type inspect zone-pair

sessions on R3 to view established sessions.

Note: If the HTTP session times out before you execute the command on R3, you will have to click the Go

button on PC-C to generate a session between PC-C and PC-A.

R3# show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR

Zone-pair: IN-2-OUT-ZPAIR

Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)

Match: access-group 101

Inspect

Number of Established Sessions = 1

Established Sessions

Session 565266624 (192.168.3.3:1031)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB

Created 00:00:01, Last heard 00:00:01

Bytes sent (initiator:responder) [284:552]

Class-map: class-default (match-any)

Match: any

Drop (default action)

0 packets, 0 bytes

What is the source IP address and port number?

_____

192.168.3.3:1031 (port 1031 is random)

What is the destination IP address and port number?

_____

192.168.1.3:80 (HTTP web = port 80)

Step 5: Close the browser on PC-C.

Part 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE

Verify that external hosts CANNOT access internal resources after configuring the ZPF.

Configuring a Zone-Based Policy Firewall (ZPF)

Step 1: From the PC-A server command prompt, ping PC-C.

From the PC-A command prompt, ping PC-C at 192.168.3.3. The ping should fail.

Step 2: From R2, ping PC-C.

From R2, ping PC-C at 192.168.3.3. The ping should fail.

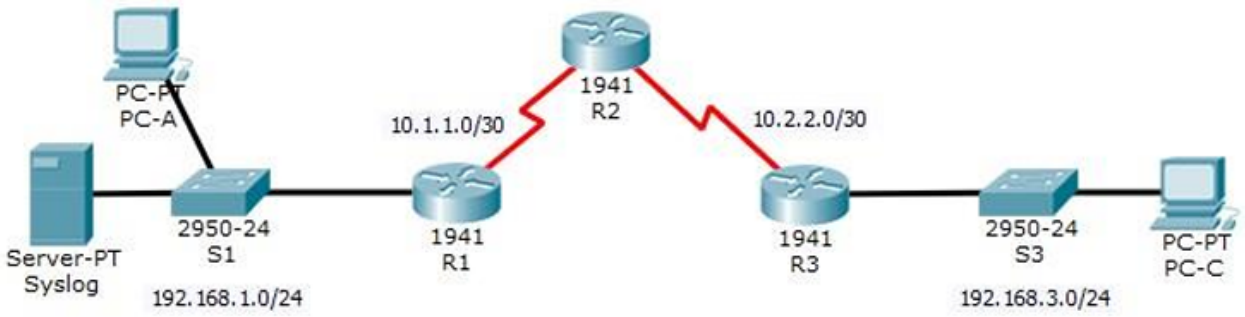
Step 3: Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.

PRACTICAL 6

Practical 6 - Configure IOS Intrusion Prevention System (IPS) Using the CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

6A. Enable IOS IPS.

Step 1: Enable the Security Technology package.

a. On R1, issue the show version command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the

package.

R1(config)# license boot module c1900 technology-package securityk9

c. Accept the end user license agreement.

d. Save the running-config and reload the router to enable the security license.

e. Verify that the Security Technology package has been enabled by using the show version command.

Step 2: Verify network connectivity.

a. Ping from PC-C to PC-A. The ping should be successful.

b. Ping from PC-A to PC-C. The ping should be successful.

Step 3: Create an IOS IPS configuration directory in flash. On R1, create a directory in flash using the mkdir command. Name the directory ipsdir.

R1# mkdir ipsdir

Create directory filename [ipsdir]? <Enter> Created

dir flash:ipsdir

Step 4: Configure the IPS signature storage location. On R1, configure the IPS signature storage location to be the directory you just created.

R1(config)# ip ips config location flash:ipsdir

Step 5: Create an IPS rule.

On R1, create an IPS rule name using the ip ips name name command in global configuration mode. Name the IPS rule iosips.

R1(config)# ip ips name iosips

Step 6: Enable logging.

IOS IPS supports the use of syslog to send event notification. Syslog notification is enabled by default. If logging console is enabled, IPS syslog messages display.

a. Enable syslog if it is not enabled.

R1(config)# ip ips notify log

Configure IOS Intrusion Prevention System (IPS) using CLI

b. If necessary, use the clock set command from privileged EXEC mode to reset the clock. R1#

clock set 10:20:00 10 january 2014

c. Verify that the timestamp service for logging is enabled on the router using the show run command.

Enable the timestamp service if it is not enabled.

R1(config)# service timestamps log datetime msec

d. Send log messages to the syslog server at IP address 192.168.1.50. R1(config)# logging host 192.168.1.50

Step 7: Configure IOS IPS to use the signature categories.

Retire the all signature category with the retired true command (all signatures within the signature release).

Unretire the IOS_IPS Basic category with the retired false command. R1(config)# ip ips signature

category

R1(config-ips-category)# category all

R1(config-ips-category-action)# retired true

R1(config-ips-category-action)# exit

R1(config-ips-category)# category ios_ips basic

R1(config-ips-category-action)# retired false

R1(config-ips-category-action)# exit

R1(config-ips-cateogry)# exit

Do you want to accept these changes? [confirm] <Enter>

Step 8: Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the ip ips name direction command in interface configuration mode.

Apply the rule outbound on the G0/1 interface of R1. After you enable IPS, some log messages will be sent to

the console line indicating that the IPS engines are being initialized.

Note: The direction in means that IPS inspects only traffic going into the interface. Similarly, out means that IPS inspects only traffic going out of the interface.

R1(config)# interface g0/1

R1(config-if)# ip ips iosips out Part

6B. Modify an IPS signature.

Step 1: Change the event-action of a signature.

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature action to alert and drop.

R1(config)# ip ips signature-definition

R1(config-sigdef)# signature 2004 0

R1(config-sigdef-sig)# status

R1(config-sigdef-sig-status)# retired false

R1(config-sigdef-sig-status)# enabled true

R1(config-sigdef-sig-status)# exit

R1(config-sigdef-sig)# engine

R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdefsig-engine)# event-action deny-packet-inline

R1(config-sigdef-sig-engine)# exit

R1(config-sigdef-sig)# exit

R1(config-sigdef)# exit

Do you want to accept these changes? [confirm] <Enter>

Step 2: Use show commands to verify IPS.

Use the show ip ips all command to view the IPS configuration status summary.

To which interfaces and in which direction is the iosips rule applied?

_____

G0/1 outbound.

Step 3: Verify that IPS is working properly.

a. From PC-C, attempt to ping PC-A. Were the pings successful? Explain.

_____

_

_____

_

The pings should fail. This is because the IPS rule for event-action of an echo request was set to “deny- packetinline”.

b. From PC-A, attempt to ping PC-C. Were the pings successful? Explain.

_____

_

_____

_

The ping should be successful. This is because the IPS rule does not cover echo reply. When PC-A pings

PC-C, PC-C responds with an echo reply.

Step 4: View the syslog messages.

a. Click the Syslog server.

b. Select the Services tab.

c. In the left navigation menu, select SYSLOG to view the log file.

Step 5: Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of which

required components have been completed.

!!!Script for R1

clock set 10:20:00 10 january 2014 mkdir

ipsdir

config

Configure IOS Intrusion Prevention System (IPS) using CLI

license boot module c1900 technology-package securityk9

yes end reload config t

ip ips config location flash:ipsdir

ip ips name iosips ip ips notify log

service timestamps log datetime msec

logging host 192.168.1.50

ip ips signature-category

category all retired true exit

category ios_ips basic retired

false exit exit interface

g0/1 ip ips iosips out exit ip

ips signature-definition

signature 2004 0 status

retired false enabled true

exit engine event-action

produce-alert event-action

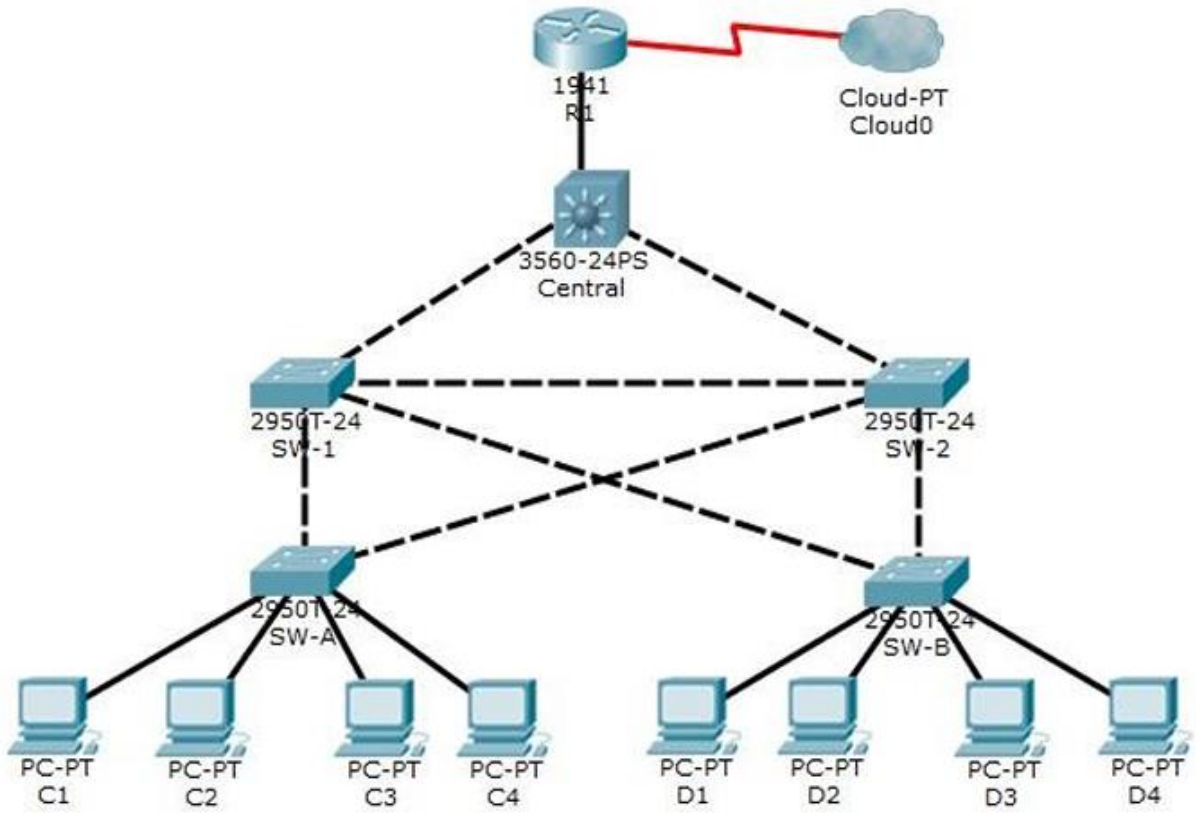
deny-packet-inline exit exit

exit

PRACTICAL 7

Practical 7 - Layer 2 Security

Topology



7A. Assign the Central switch as the root bridge.

Step 1: Determine the current root bridge.

From Central, issue the show spanning-tree command to determine the current root bridge, to see the ports

in use, and to see their status.

Which switch is the current root bridge?

_____

Current root is SW-1.

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Step 2: Assign Central as the primary root bridge. Using the spanning-tree vlan 1 root

primary command, and assign Central as the root bridge.

Central(config)# spanning-tree vlan 1 root primary

Step 3: Assign SW-1 as a secondary root bridge. Assign SW-1 as the secondary root bridge using

the spanning-tree vlan 1 root secondary command. SW-1(config)# spanning-tree vlan 1

root secondary

Step 4: Verify the spanning-tree configuration. Issue the show spanning

tree command to verify that Central is the root bridge.

Central# show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 24577

Address 00D0.D31C.634C

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Which switch is the current root bridge?

_____

Current root is Central

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

7B. Secure spanning-tree parameters to prevent STP manipulation attacks.

Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the SW-A and SW-B, use the spanning-tree portfast command.

SW-A(config)# interface range f0/1 - 4

SW-A(config-if-range)# spanning-tree portfast

SW-B(config)# interface range f0/1 - 4

SW-B(config-if-range)# spanning-tree portfast

Step 2: Enable BPDU guard on all access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU

guard on SW-A and SW-B access ports.

SW-A(config)# interface range f0/1 - 4

SW-A(config-if-range)# spanning-tree bpduguard enable

SW-B(config)# interface range f0/1 - 4

SW-B(config-if-range)# spanning-tree bpduguard enable

Note: Spanning-tree BPDU guard can be enabled on each individual port using the spanning-tree bpduguard enable command in interface configuration mode or the spanning-tree portfast bpduguard default command in global configuration mode. For grading purposes in this activity, please use the spanning-tree bpduguard enable command.

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the show spanning-tree command to determine the location of the root port on each switch.

On SW-1, enable root guard on ports F0/23 and F0/24. On SW-2, enable root guard on ports F0/23 and F0/24.

SW-1(config)# interface range f0/23 - 24

SW-1(config-if-range)# spanning-tree guard root

SW-2(config)# interface range f0/23 - 24

SW-2(config-if-range)# spanning-tree guard root

7C. Enable port security to prevent CAM table overflow attacks.

Step 1: Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on SW-A and SW-B. Set the maximum number of learned MAC addresses to 2, allow the MAC address to be learned dynamically, and set the violation to shutdown. Note: A switch port must be configured as an access port to enable port security.

SW-A(config)# interface range f0/1 - 22

SW-A(config-if-range)# switchport mode access

SW-A(config-if-range)# switchport port-security

SW-A(config-if-range)# switchport port-security maximum 2

SW-A(config-if-range)# switchport port-security violation shutdown SW

A(config-if-range)# switchport port-security mac-address sticky

SW-B(config)# interface range f0/1 - 22

SW-B(config-if-range)# switchport mode access

SW-B(config-if-range)# switchport port-security

SW-B(config-if-range)# switchport port-security maximum 2

SW-B(config-if-range)# switchport port-security violation shutdown

SW-B(config-if-range)# switchport port-security mac-address sticky

Why is port security not enabled on ports that are connected to other switch devices?

_____
_____
_____
_____
_____

Ports connected to other switch devices have a multitude of MAC addresses learned for that single port.

Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

Step 2: Verify port security.

a. On SW-A, issue the command show port-security interface f0/1 to verify that port security has been configured.

SW-A# show port-security interface f0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

b. Ping from C1 to C2 and issue the command show port-security interface f0/1 again to verify that the switch has learned the MAC address for C1.

Step 3: Disable unused ports.

Disable all ports that are currently unused.

SW-A(config)# interface range f0/5 - 22

SW-A(config-if-range)# shutdown

SW-B(config)# interface range f0/5 - 22

SW-B(config-if-range)# shutdown

Step 4: Check results.

Your completion percentage should be 100%. Click Check Results to view feedback and verification of which of the required components have been completed.

!!!Script for Central

conf t

spanning-tree vlan 1 root primary end

!!!Script for SW-1 conf t

spanning-tree vlan 1 root secondary

interface range f0/23 - 24

spanning-tree guard root end

!!!Script for SW-2 conf t

interface range f0/23 - 24

spanning-tree guard root end

!!!Script for SW-A conf t interface range f0/1 - 4 spanning-tree portfast spanning-tree bpduguard enable interface range f0/1 - 22

switchport mode access

switchport port

security switchport port-security maximum 2

switchport port-security violation shutdown

switchport port-security mac-address sticky

interface range f0/5 - 22 shutdown end

!!!Script for SW-B conf t interface range f0/1 - 4

spanning-tree portfast

spanning-tree

bpduguard enable interface range f0/1 - 22

switchport mode access

switchport port

security switchport port-security maximum 2

switchport port-security violation shutdown

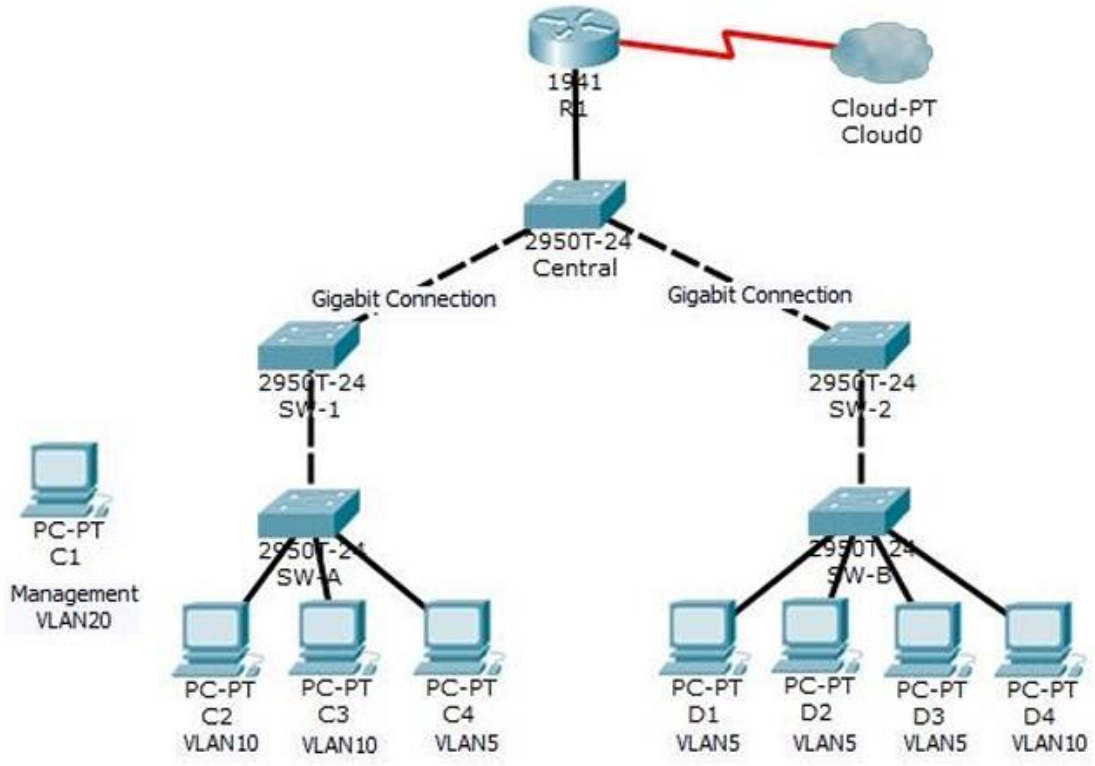
switchport port-security mac-address sticky

interface range f0/5 - 22 shutdown end

PRACTICAL 8

Practical 8 - Layer 2 VLAN Security

Topology



8. Layer 2 VLAN Security

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port F0/23 on SW-1 to port F0/23 on SW-2.

Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both SW-1 and SW-2, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

SW-1(config)# interface f0/23

SW-1(config-if)# switchport mode trunk

SW-1(config-if)# switchport trunk native vlan 15

SW-1(config-if)# switchport nonegotiate

SW-1(config-if)# no shutdown

SW-2(config)# interface f0/23

SW-2(config-if)# switchport mode trunk

SW-2(config-if)# switchport trunk native vlan 15

SW-2(config-if)# switchport nonegotiate

SW-2(config-if)# no shutdown

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For

security purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on SW-A.

SW-A(config)# vlan 20

SW-A(config-vlan)# exit

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

SW-A(config)# interface vlan 20

SW-A(config-if)# ip address 192.168.20.1 255.255.255.0

Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: SW-B, SW-1, SW-2, and Central.

SW-B(config)# vlan 20

SW-B(config-vlan)# exit

SW-1(config)# vlan 20

SW-1(config-vlan)# exit

SW-2(config)# vlan 20

SW-2(config-vlan)# exit

Central(config)# vlan 20

Central(config-vlan)# exit

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24

network.

SW-B(config)# interface vlan 20

SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# interface vlan 20

SW-1(config-if)# ip address 192.168.20.3 255.255.255.0

SW-2(config)# interface vlan 20

SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

Central(config)# interface vlan 20

Central(config-if)# ip address 192.168.20.5 255.255.255.0

Step 3: Connect and configure the management PC.

Connect the management PC to SW-A port F0/1 and ensure that it is assigned an available IP address within

the 192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20. Interface

F0/1 must be part of VLAN 20.

SW-A(config)# interface f0/1

SW-A(config-if)# switchport access vlan 20 SW-A(config-if)#

no shutdown

Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and Central.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

R1(config)# interface g0/0.3

R1(config-subif)# encapsulation dot1q 20

b. Assign an IP address within the 192.168.20.0/24 network.

R1(config)# interface g0/0.3

R1(config-subif)# ip address 192.168.20.100 255.255.255.0

Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the

management VLAN.

a. Create an ACL that allows only the Management PC to access the router. Example: (may vary

from student configuration)

R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255

R1(config)# access-list 101 permit ip any any

R1(config)# access-list 102 permit ip host 192.168.20.50 any

b. Apply the ACL to the proper interface(s).

Example: (may vary from student configuration)

R1(config)# interface g0/0.1

R1(config-subif)# ip access-group 101 in

R1(config-subif)# interface g0/0.2

R1(config-subif)# ip access-group 101 in

R1(config-subif)# line vty 0 4

R1(config-line)# access-class 102 in

Note: Access list 102 is used to only allow the Management PC (192.168.20.50 in this example) to access the router. This prevents an IP address change to bypass the ACL.

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity

requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. Verify only the Management PC can access the router. Use SSH to access R1 with username SSHadmin

and password ciscosshpa55.

PC> ssh -l SSHadmin 192.168.20.100

b. From the management PC, ping SW-A, SW-B, and R1. Were the pings successful? Explain.

_____

_____

_____

The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

c. From D1, ping the management PC. Were the pings successful? Explain.

_____

_____

_

_____

The ping should have failed because for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

Step 5: Check results.

Your completion percentage should be 100%. Click Check Results to view feedback and verification of which required components have been completed.

If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.

!!!

Script for SW-1 conf t

interface f0/23 switchport mode

trunk

switchport trunk native

vlan 15 switchport nonegotiate

no

shutdown vlan 20

exit

interface vlan 20

ip address 192.168.20.3 255.255.255.0

!!!

Script for SW-2 conf t

interface f0/23 switchport mode

trunk

switchport trunk native

vlan 15 switchport nonegotiate

no

shutdown vlan 20

exit

interface vlan 20

ip address 192.168.20.4 255.255.255.0

!!! Script for SW-A

conf t vlan 20

exit interface

vlan 20

ip address 192.168.20.1 255.255.255.0

interface f0/1 switchport access vlan

20 no shutdown

!!! Script for SW-B conf t vlan 20 exit

interface

vlan

20

192.168.20.2 255.255.255.0

ip address

!!! Script for Central conf t vlan 20 exit

interface

vlan

20

192.168.20.5 255.255.255.0

!!! Script for R1 conf

t

ip address

interface GigabitEthernet0/0.1 ip access-group
101 in interface GigabitEthernet0/0.2 ip access
group 101 in interface g0/0.3 encapsulation dot1q
20 ip address 192.168.20.100 255.255.255.0
access-list 101 deny ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip any any access-list
102 permit ip host 192.168.20.50 any line vty 0
4
access-class 102 in