IPRC NGOMA
Integrated Polytechnic Regional College
RWANDA POLYTECHNIC

P.O. Box 35 KIBUNGO - RWANDA
Tel: +250 783 540 145
Email:info@iprcngoma.rp.ac.rw
www.iprcngoma.rp.ac.rw

INFORMATION AND COMMUNICATION TECHNOLOGY DEPARTMENT

INFORMATION TECHNOLOGY OPTION

COURSE CODE: ITLNS701

COURSE NAME: Network Security

CREDITS: 10

NETWORK SECURITY PRACTICE MANUAL

ADMINISTRATIVE DEPARTMENT: Information and Communication Technology (ICT)

Level7

Semester I

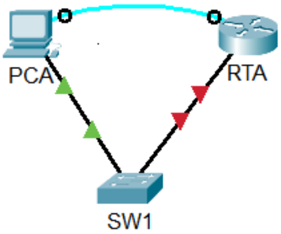
Academic year 2023-2024

Trainer's Name: NIYIBIZI Jean Paul

April 2024

Contents

1. Configure Secure Passwords and SSH



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0/0	172.16.1.1	255.255.255.0	N/A
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Blank Line, No additional information

Scenario

The network administrator has asked you to prepare **RTA** and **SW1** for deployment. Before they can be connected to the network, security measures must be enabled.

Instructions

Part 1: Configure Basic Security on the Router

a. Configure IP addressing on **PCA** according to the Addressing Table.

b. Console into **RTA** from the Terminal on PCA.

c. Configure the hostname as **RTA**.

d. Configure IP addressing on **RTA** and enable the interface.

e. Encrypt all plaintext passwords.

```
RTA(config)# service password-encryption
```

f. Set the minimum password length to 10.

```
RTA(config)# security passwords min-length 10
```

g. Set a strong secret password of your choosing.

Note: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

h. Disable DNS lookup.

```
RTA(config)# no ip domain-lookup
```

i. Set the domain name to **netsec.com** (case-sensitive for scoring in PT).

```
RTA(config)# ip domain-name netsec.com
```

j. Create a user of your choosing with a strong encrypted password.

```
RTA(config)# username any_user secret any_password
```

k. Generate 1024-bit RSA keys.

Note: In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue.

```
RTA(config)# crypto key generate rsa
The name for the keys will be: RTA.netsec.com
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
```

l. Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

m. Configure all VTY lines for SSH access and use the local user profiles for authentication.

```
RTA(config)# line vty 0 4
RTA(config-line)# transport input ssh
RTA(config-line)# login local
```

n. Set the EXEC mode timeout to 6 minutes on the VTY lines.

```
RTA(config-line)# exec-timeout 6
```

o. Save the configuration to NVRAM.

p. Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA**.

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

Part 2: Configure Basic Security on the Switch

Configure switch **SW1** with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

a. Console into **SW1** from the Terminal on PCA.

b. Configure the hostname as **SW1**.

c. Configure IP addressing on SW1 **VLAN1** and enable the interface.

d. Configure the default gateway address.

e. Disable all unused switch ports.

Note: On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the '**shutdown**' command. This would require accessing each port individually. There is a shortcut method for making modifications to several ports at once by using the **interface range** command. On **SW1** all ports except FastEthernet0/1 and GigabitEthernet0/1 can be shutdown with the following command:

```
SW1(config)# interface range F0/2-24, G0/2
SW1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively
down
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
```

The command used the port range of 2-24 for the FastEthernet ports and then a single port range of GigabitEthernet0/2.

f. Encrypt all plaintext passwords.

g. Set a strong secret password of your choosing.

h. Disable DNS lookup.

i. Set the domain name to **netsec.com** (case-sensitive for scoring in PT).

j. Create a user of your choosing with a strong encrypted password.

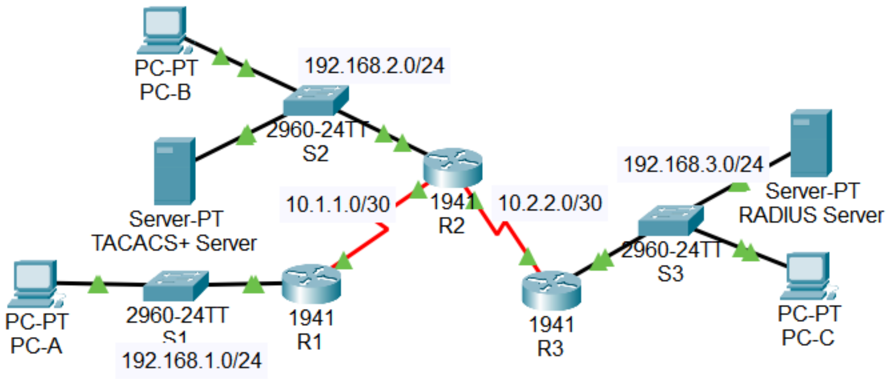
k. Generate 1024-bit RSA keys.

l. Configure all VTY lines for SSH access and use the local user profiles for authentication.

m. Set the EXEC mode timeout to 6 minutes on all VTY lines.

n. Save the configuration to NVRAM.

2. Packet Tracer - Configure Server-based Authentication with TACACS+ and RADIUS



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
R1	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
R2	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	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
R3	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

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
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

Blank Line, No additional information

Objectives

- Configure server-based AAA authentication using TACACS+.
- Verify server-based AAA authentication from the PC-B client.
- Configure server-based AAA authentication using RADIUS.
- Verify server-based AAA authentication from the PC-C client.

Background / Scenario

The network topology shows routers R1, R2 and R3. Currently, all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions.

You will configure router R2 to support server-based authentication using the TACACS+ protocol. The TACACS+ server has been pre-configured with the following:

- Client: **R2** using the keyword **tacacspa55**
- User account: **Admin2** and password **admin2pa55**

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol. The RADIUS server has been pre-configured with the following:

- Client: **R3** using the keyword **radiuspa55**
- User account: **Admin3** and password **admin3pa55**

The routers have also been pre-configured with the following:

- Enable secret password: **ciscoenpa55**
- OSPF routing protocol with MD5 authentication using password: **MD5pa55**

Note: The console and vty lines have not been pre-configured.

Note: Newer IOS images use more secure encryption hashing algorithm; however, the IOS version currently supported in Packet Tracer uses MD5. Always use the most secure option available on your physical equipment.

Part 1: Configure Server-Based AAA Authentication Using TACACS+ on R2

Step 1: Test connectivity.

- Ping from PC-A to PC-B.
- Ping from PC-A to PC-C.
- Ping from PC-B to PC-C.

Step 2: Configure a backup local database entry called Admin.

For backup purposes, configure a local username of Admin2 and a secret password of admin2pa55.

Step 3: Verify the TACACS+ Server configuration.

Click the TACACS+ Server. On the Services tab, click AAA. Notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 4: Configure the TACACS+ server specifics on R2.

Configure the AAA TACACS server IP address and secret key on R2.

Note: The commands tacacs-server host and tacacs-server key are deprecated. Currently, Packet Tracer does not support the new command tacacs server.

```
R2(config)# tacacs-server host 192.168.2.2

R2(config)# tacacs-server key tacacspa55
```

Step 5: Configure AAA login authentication for console access on R2.

Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.

Step 6: Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

Step 7: Verify the AAA authentication method.

Verify the user EXEC login using the AAA TACACS+ server.

Part 2: Configure Server-Based AAA Authentication Using RADIUS on R3

Step 1: Configure a backup local database entry called Admin.

For backup purposes, configure a local username of **Admin3** and a secret password of **admin3pa55**.

Step 2: Verify the RADIUS Server configuration.

Click the RADIUS Server. On the Services tab, click **AAA**. Notice that there is a Network configuration entry for **R3** and a User Setup entry for **Admin3**.

Step 3: Configure the RADIUS server specifics on R3.

Configure the AAA RADIUS server IP address and secret key on **R3**.

Note: The commands **radius-server host** and **radius-server key** are deprecated. Currently Packet Tracer does not support the new command **radius server**.

```
R3(config)# radius-server host 192.168.3.2

R3(config)# radius-server key radiuspa55
```

Step 4: Configure AAA login authentication for console access on R3.

Enable AAA on **R3** and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.

Step 5: Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

Step 6: Verify the AAA authentication method.

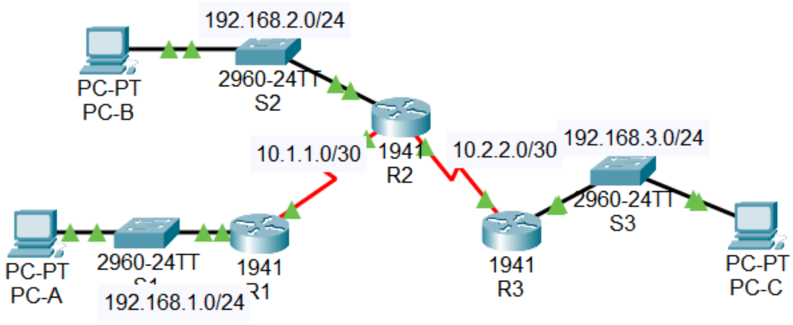
Verify the user EXEC login using the AAA RADIUS server.

Step 7: Check results.

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

end of document

3. Configure Local AAA for Console and VTY Access



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
R1	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
R2	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	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
R3	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
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

Blank Line, No additional information

Objectives

- Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC-A client.

Background / Scenario

The network topology shows routers R1, R2 and R3. Currently, all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions.

You will create a local user account and configure local AAA on router R1 to test the console and vty logins.

- User account: **Admin1** and password **admin1pa55**

The routers have also been pre-configured with the following:

- Enable secret password: **ciscoenpa55**
- OSPF routing protocol with MD5 authentication using password: **MD5pa55**

Note: The console and vty lines have not been pre-configured.

Note: Newer IOS images use more secure encryption hashing algorithm; however, the IOS version currently supported in Packet Tracer uses MD5. Always use the most secure option available on your physical equipment.

Part 1: Configure Local AAA Authentication for Console Access on R1

Step 1: Configure a local username on R1.

Configure a username of **Admin1** with a secret password of **admin1pa55**.

Step 2: Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for the console login to use the local database.

Step 3: Configure the line console to use the defined AAA authentication method.

Enable AAA on **R1** and configure AAA authentication for the console login to use the default method list.

Step 4: Verify the AAA authentication method.

Verify the user EXEC login using the local database.

Part 2: Configure Local AAA Authentication for vty Lines on R1

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

a. Use **netsec.com** as the domain name on R1.

b. Create an RSA crypto key using 1024 bits.

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.

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.

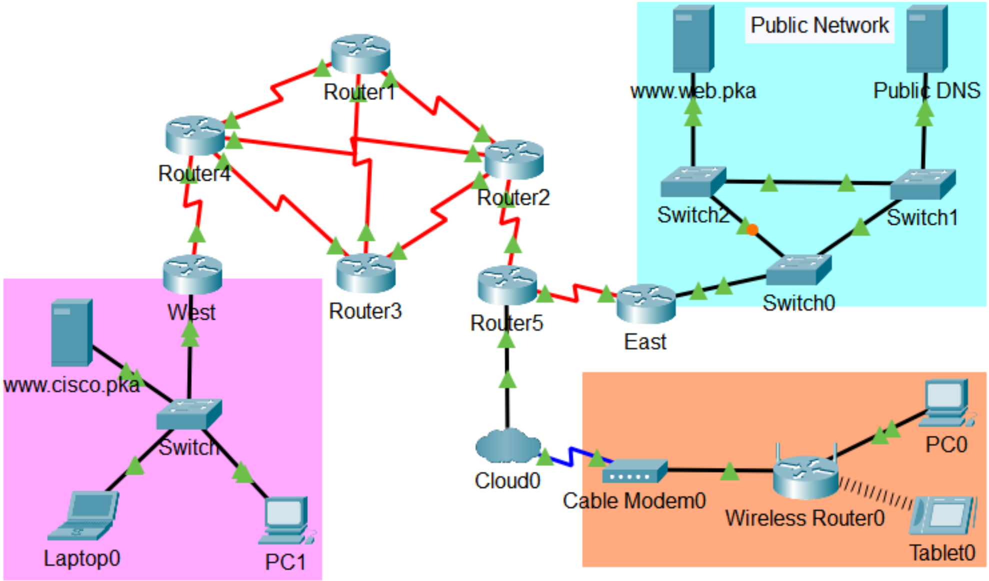
Step 4: Verify the AAA authentication method.

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

```
      PC> ssh –l Admin1 192.168.1.1
      Open
P     assword: admin1pa55
```

End of document

4. Identify Packet Flow



Objectives

In this activity, you will observe packet flow in a LAN and WAN topology. You will also observe how the packet flow path may change when there is a change in the network topology.

Part 1: Verify Connectivity

Part 2: Remote LAN Network Topology

Part 3: WAN Network Topology

Background / Scenario

Packet Tracer allows the design and creation of a simulated networking topology. In this activity, you are presented with a simplified topology to observe packet flow. You will explore how packets travel through the network using the simulation mode in Packet Tracer. You will also observe the changes in packet flow when there is a change in the network topology.

Required Resources

- Latest version of Packet Tracer installed

Instructions

Part 1: Verifying Connectivity

In this part, you will verify that you can access the other networks from devices on the Home Network.

a. Click **PC0**. Select the **Desktop** tab and open the **Web Browser**.

b. In the URL field, enter **www.cisco.pka** and press **Go**. Be sure to use the .pka domain, not the .com domain. It should be successful. You can click **Fast Forward Time** to speed up the process.

c. Repeat this for **www.web.pka**. It should be successful.

d. Exit the web browser when finished.

Part 2: Remote LAN Network Topology

In this part, you will use the simulation mode in Packet Tracer to observe how packets flow through a remote LAN network.

a. Switch to Simulation mode (Shift + S). Click **Show All/None** to clear all the selected event list filters.

b. Click **Edit Filters**. Select **DNS** under the IPv4 tab and **HTTP** under **Misc** tab.

c. Open a web browser on **PC0**. Enter **www.web.pka** and press **Go**.

Question:

Predict the packet path to resolve **www.web.pka** to an IP address. Record your prediction.

d. Click **Capture / Forward** until the webpage is displayed on PC0 to view the packet flow. Click **View Previous Events** when prompted by the Buffer Full dialog box.

After the IP address has been resolved, which path did HTTP packets travel to display the webpage? Record your observations.

e. Switch to Real time mode (Shift + R). Click the X icon in the right tool panel to select the Delete tool. Remove the link between Switch0 and Switch 1 from the Public Network to simulate a broken link. After 30 seconds, the network will learn of the broken link. You can click Fast Forward to speed up the process.

f. Select the Arrow tool above the Delete tool to de-select Delete.

g. Switch to Simulation mode (Shift + S). Open a web browser in **Tablet0** and navigate to **www.web.pka**. You can click Auto Capture/Play to have Packet Tracer forward the packets without your interaction. You can also move the Play Slider to the right to speed up the packet forwarding.

With a broken link in the LAN, how did the path change? Record your observation.

Part 3: WAN Network Topology

Step 1: PC0 to websites.

a. Remaining in Simulation mode, open a web browser on **PC0**. Enter **www.cisco.pka** and press **Go**.

Predict the packet path to resolve **www.cisco.pka** to an IP address. Record your prediction.

b. Click **Capture / Forward** until the webpage is displayed on PC0 to view the packet flow. Click **View Previous Events** when prompted by the Buffer Full dialog box.

After the IP address has been resolved, which path did HTTP packets travel to display the webpage? Record your observations.

c. Switch to Real time mode (Shift + R). Remove the link between Router4 and Router2 from the topology to simulate an inaccessible path. The routers are using Enhanced Interior Gateway Routing Protocol (EIGRP) to dynamically adjust routing tables to account for the deleted link.

d. Switch to Simulation mode (Shift + S). Open a web browser in **Tablet0** and navigate to **www.cisco.pka**.

With a broken link in the WAN, how would the path change? Record your observation.

e. Switch to Real time mode (Shift + R).

Step 2: PC1 to websites.

a. Click PC1 > Desktop and open a command prompt.

b. Enter **tracert www.web.pka** at the command.

```
PC> tracert www.web.pka
```

c. Match the IP addresses in the **tracert** results to the devices in the topology. Hover over the routers in the topology to view the IP addresses of the interfaces on the routers. If the popup does not stay active long enough, you can access router IP addresses in the following manner: Click the router > CLI > press Enter. Now enter the command **show ip interface brief** to getting a listing of the interfaces and IP addresses.

Trace Number	Device	Interface	IP Address
blank	blank	blank	blank
blank	blank	blank	blank
blank	blank	blank	blank
blank	blank	blank	blank
blank	blank	blank	blank
6	East	Serial 0/0/0	209.165.202.130
7	www.web.pka	NIC	209.165.202.132 / 192.168.2.254

Network address translation (NAT) is used to translate the private www.web.pka IP address of 192.168.2.254 to a routable IPv4 address of 209.165.202.132. In the tracert result, the first line of IPv4 address of 209.165.202.132 is for the G0/1 interface of East. The second line of IPv4 address of 209.165.202.132 displays the public IPv4 address of the web server.

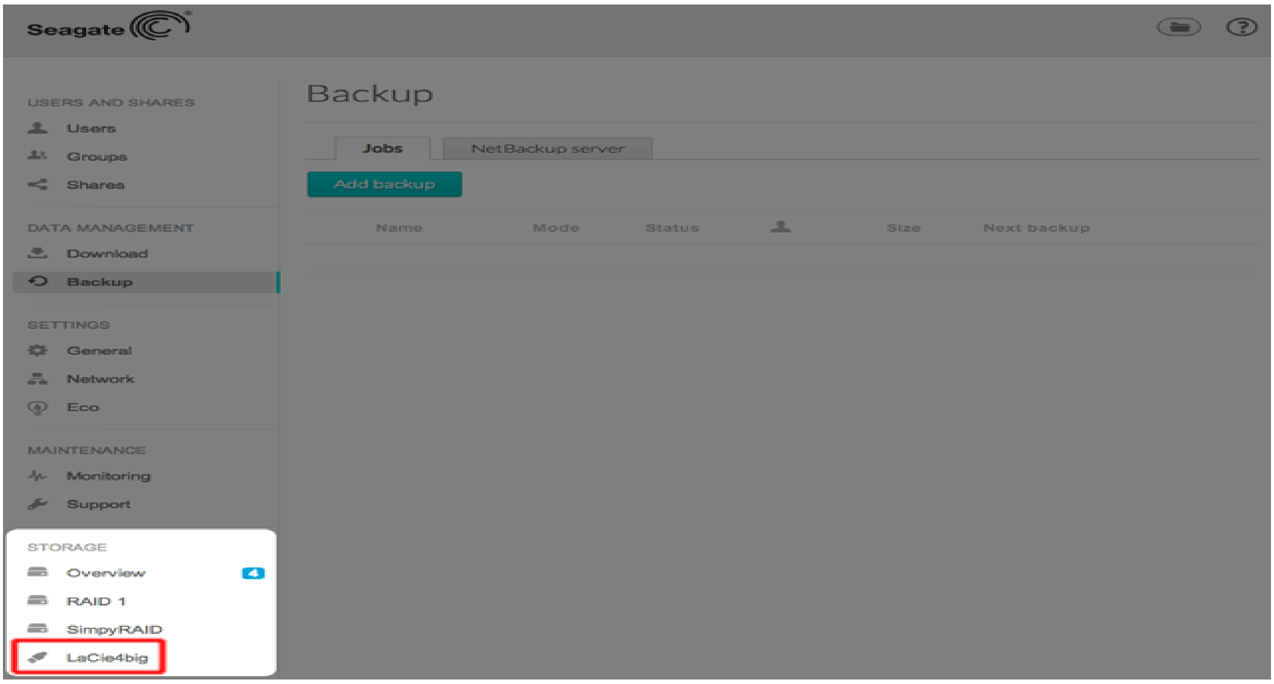
d. Switch to Simulation mode (Shift + S). Open the web browser on PC1 and enter www.web.pka as the URL. Click **Go**.

e. Click **Capture / Forward** to load the web page.
Compare the **tracert** results to the simulation results for the HTTP packets. Record your observations

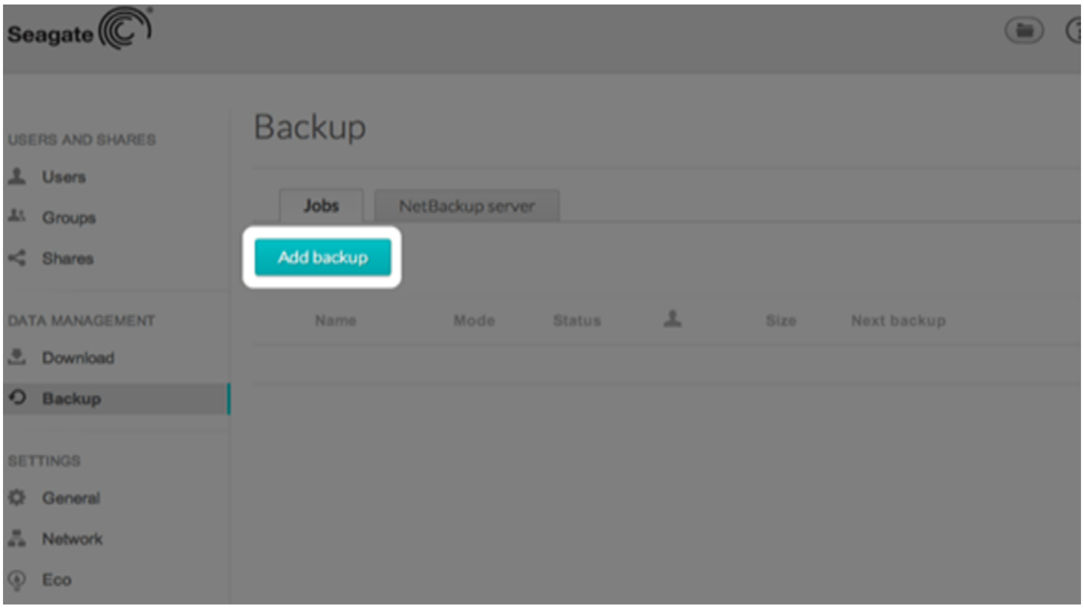
5. Configure BACK UP with

A. Create a local backup (DAS)

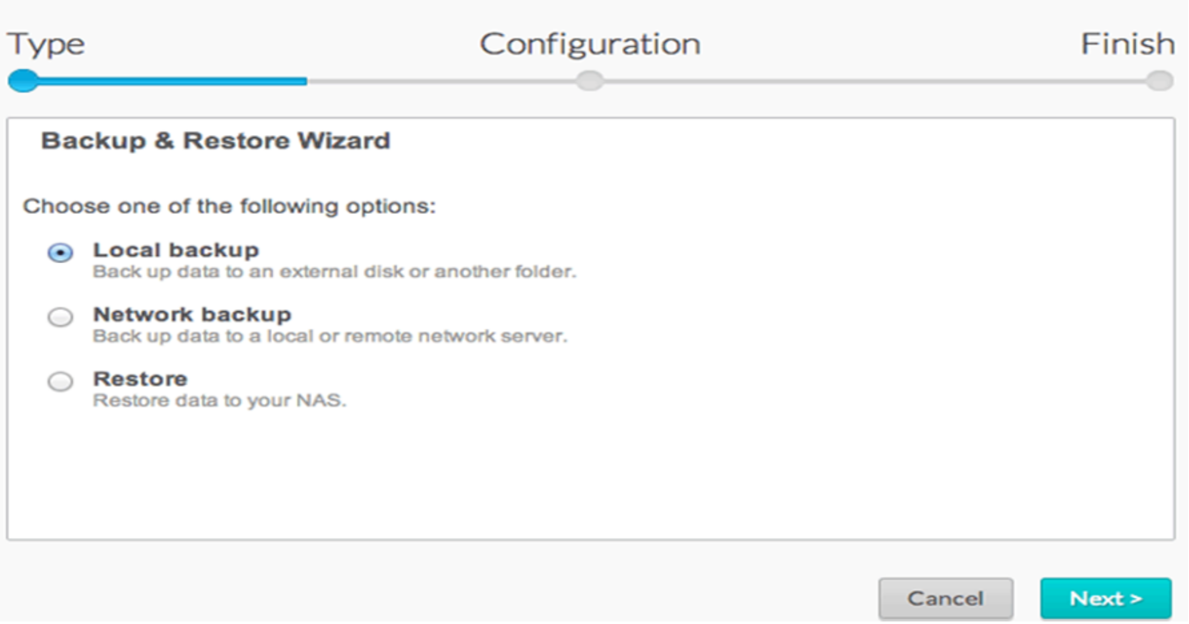
Connect an external hard drive (direct attached storage, or DAS) to one of the eSATA or USB ports on the NAS device, then follow the steps below. The DAS should appear as a volume in the NAS Ports and Direct Attached Storage section of the Storage page.



1. In an Internet browser, navigate to NAS OS, then select Backup.
   Select Add Backup



2. Select Local Backup, then click Next.



Backup & Restore Wizard

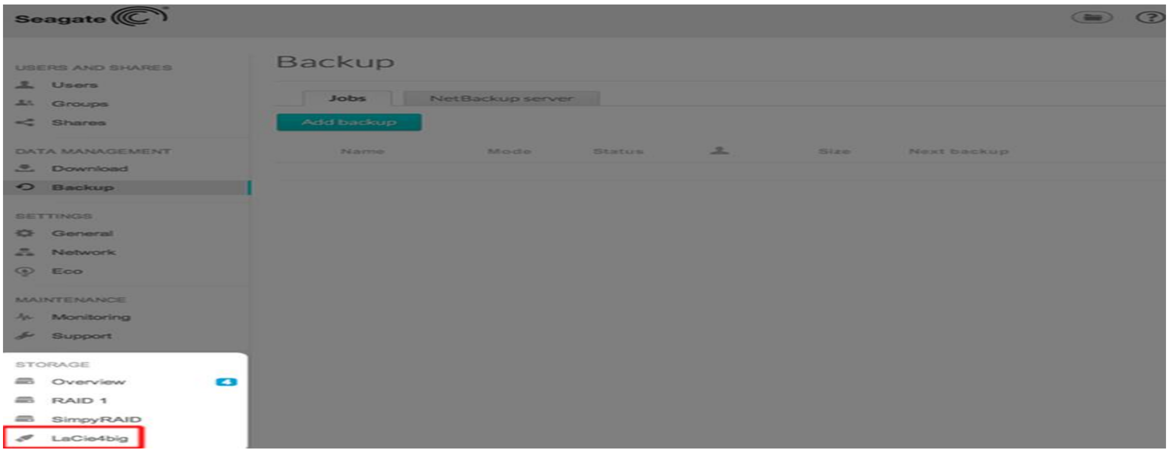
Choose one of the following options:

● Local backup
Back up data to an external disk or another folder.

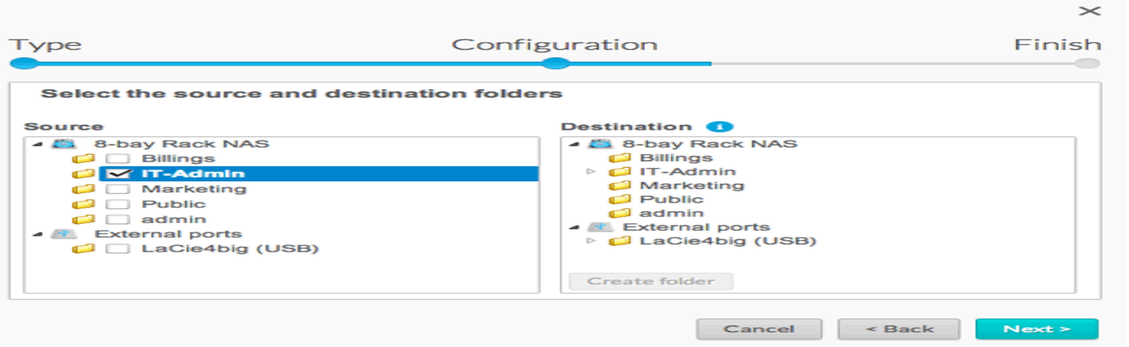
○ Network backup
Back up data to a local or remote network server.

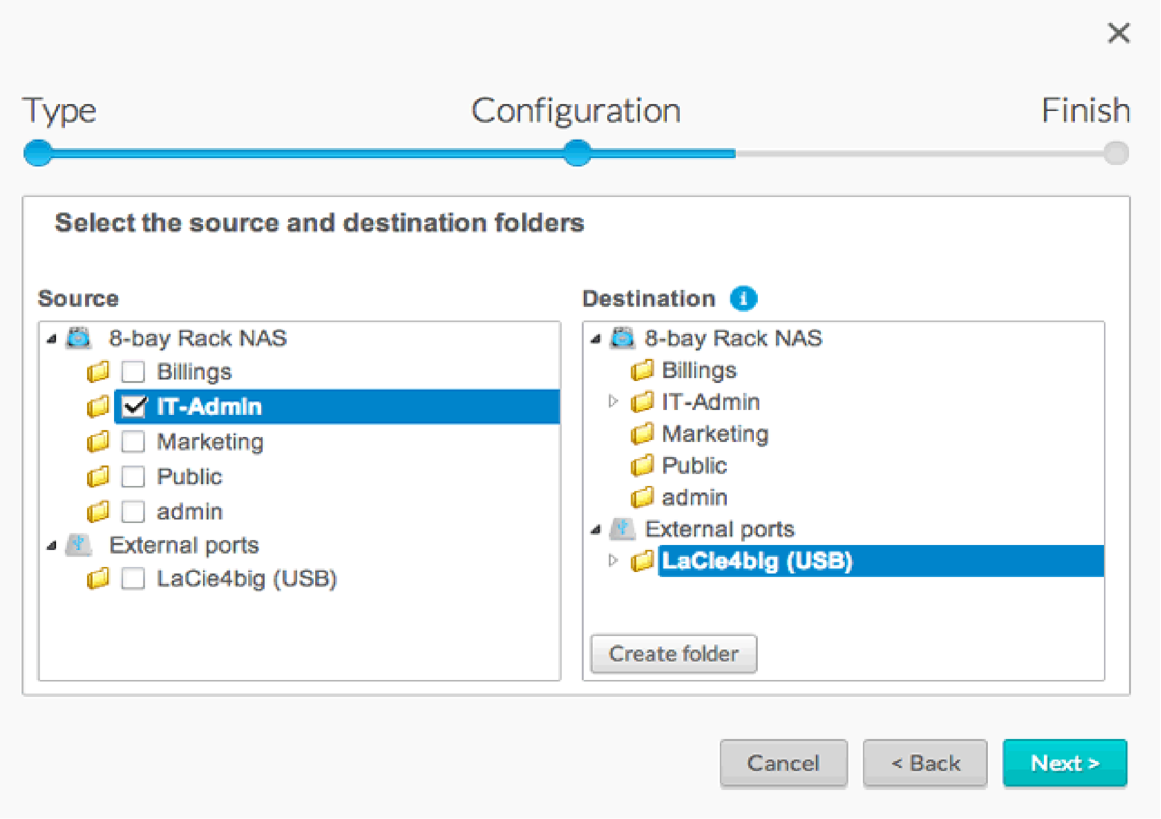
○ Restore
Restore data to your NAS.

3. Under Source on the left, select the NAS shares or DAS partitions to back up. Under Destination on the right, select the external or NAS share recipients of the backup task.

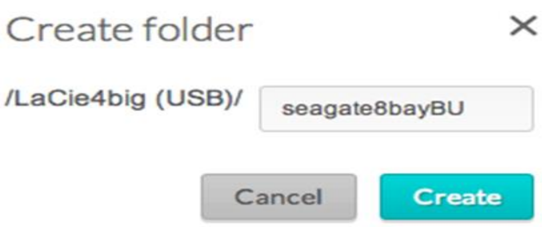


4. select the external ports or NAS share to receive the backup task.

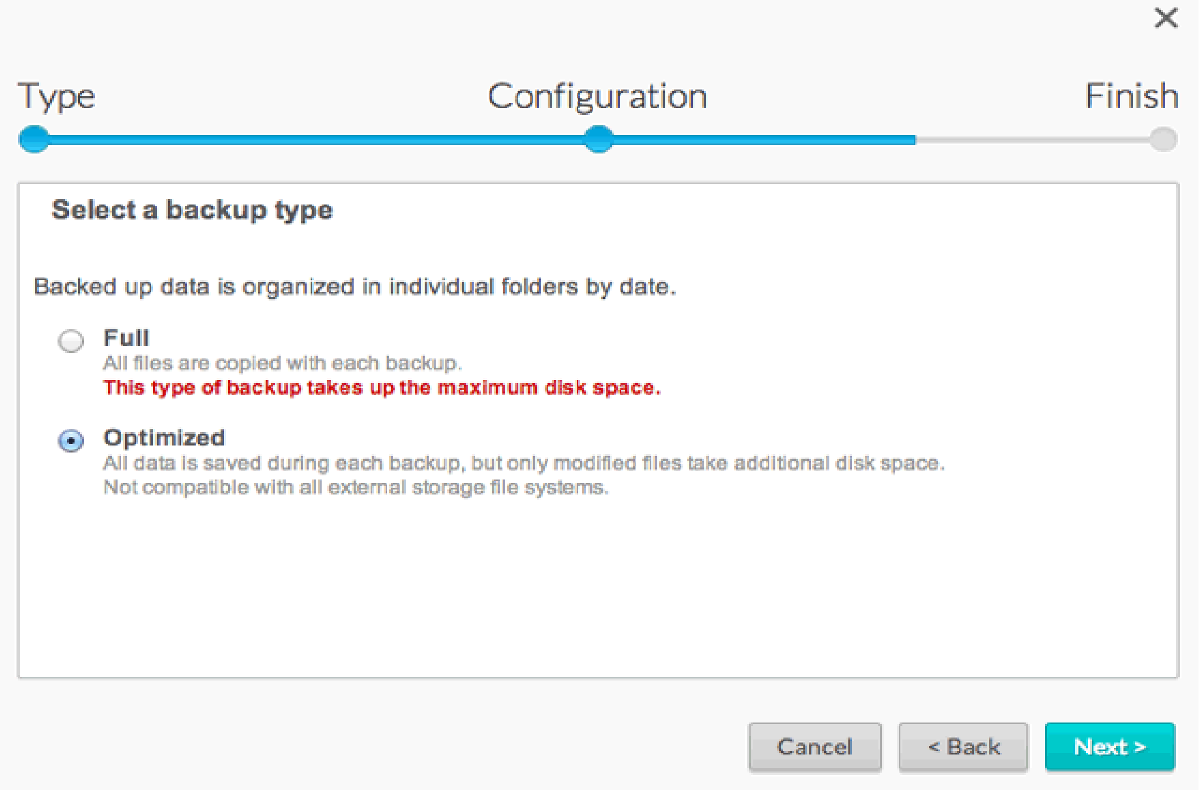




5. To better organize backup tasks, you can create a folder in the destination. Select Create folder, then enter its name when prompted. Click Create, then click Next.



6. Select a backup type:



Select a backup type

Backed up data is organized in individual folders by date.

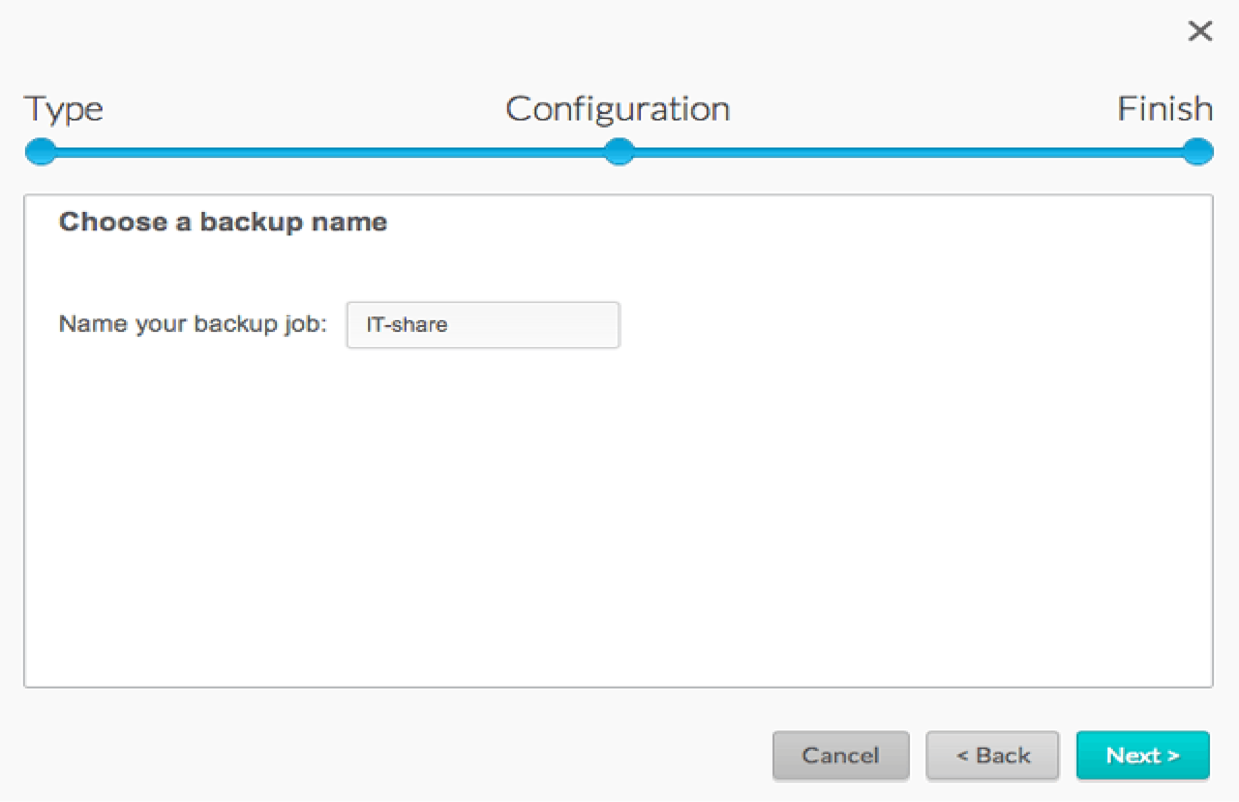
○ **Full**
All files are copied with each backup.
This type of backup takes up the maximum disk space.

● **Optimized**
All data is saved during each backup, but only modified files take additional disk space.
Not compatible with all external storage file systems.

Complete: all contents of the source folder will be saved each time the task is executed. This method offers more security, but it requires increased storage capacity at the destination.

Optimized: after the initial full backup, subsequent backups only concern modified files. This method makes it possible to efficiently use storage space at the destination. Important: Optimized backups are not available on all DAS file systems. See the table below for more information.

7. **Click Next.**
8. Select Manual, Scheduled, or Automatic, then click Next.
   - For a manual backup, follow the procedure described below.
   - Automatic backups start as soon as the DAS is connected to the NAS device. This feature is only available for backup jobs performed to or from a DAS.
9. (Skip this step if you selected Manual.) Specify the frequency and time to run your backup job. Click Next.
10. Enter a name for the backup, then click Next.



Choose a backup name

Name your backup job: IT-share

Review the backup settings on the Summary page. If you want to start the backup immediately, leave the checkbox below the summary unchecked and click Finish. The backup task will appear on the Backup page.

Background

In this activity, you will observe how an access control list (ACL) can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

Manual backups

The administrator must start the backup manually:

a. Go to NAS OS > Backup.
b. Identify the manual backup task you want to start, then position your mouse cursor to the far right of the line to display the gray arrow.
c. Click the gray arrow of the backup task to start the backup.

File systems compatible with optimized local backups

Operating systems	Hard disk file system	Optimized local backup (incremental)
Linux	EXT2, EXT3, EXT4 et XFS	yes
Mac	HFS+ not logged	yes

Mac	HFS+ not logged	Non
Windows/Mac	FAT32	Non
Windows	NTFS	Non

B. Restore A Local Backup

Restore jobs and remote backups: Remote backups cannot be restored using the Backup & Restore Wizard. You can retrieve backup files directly from the destination NAS's folder.

1. Go to NAS OS in an Internet browser and choose Backup.

2. Choose Add backup to launch the Backup & Restore Wizard.

3. Select Restore and choose Next.

4. Select a restore type, either from an existing backup job, or from a backup folder.

5. Backup job: select the backup job from the pull-down menu.

6. Backup folder: browse for the source folder that hosts your backup. Select the backup directory.

7. Choose Next.

8. Review the summary of the restore then choose Next.

9. Select the last backup or choose an earlier restore point. A restore point is the date for a backup. You can select an earlier restore point from the calendar and the time from the drop-down menu.

10. Choose Next.

11. Choose where to restore the backup.

12. Restore to the initial location of the data, which will save the data on the source folder. By default, the box Remove all files on the bottom of the window is checked. By keeping this box checked, all changes since the date of the backup will be lost. You can deselect the box to keep all data.

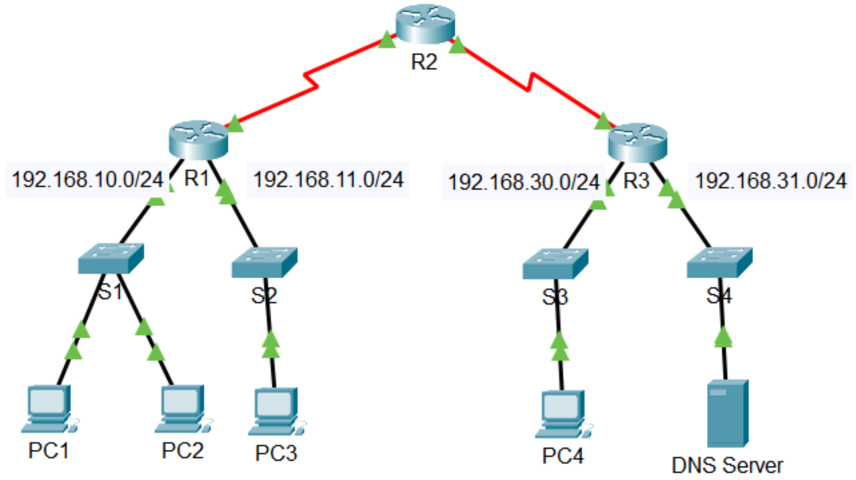
13. If you want to restore the backup to a specific folder, select Browse to choose another destination. You can create a folder in the new location. Choose Apply.

14. To free disk space, you can check the box to erase all data in the destination directory.

15. Name the restore job, then choose Next.

16. Review the summary for the restore job then choose Finish to add the job.

6. ACL Demonstration



Objectives

Part 1: Verify Local Connectivity and Test Access Control List

Part 2: Remove Access Control List and Repeat Test

Addressing Table

Device	Interface	IP Address / Prefix
R1	G0/0	192.168.10.1/24
R1	G0/1	192.168.11.1/24
R1	S0/0/0	10.1.1.1/30
R2	S0/0/0	10.10.1.2/30
R2	S0/0/1	10.10.1.5/30
R3	G0/0	192.168.30.1/24
R3	G0/1	192.168.31.1/24
R3	S0/0/1	10.10.1.6/24
PC1	NIC	192.168.10.10/24
PC2	NIC	192.168.10.11/24
PC3	NIC	192.168.11.10/24
PC4	NIC	192.168.30.12/24
DNS Server	NIC	192.168.31.12/24

Blank Line - no additional information

Instructions

Part 1: Verify Local Connectivity and Test Access Control List

Step 1: Ping devices on the local network to verify connectivity.

a. From the command prompt of **PC1**, ping **PC2**.

b. From the command prompt of **PC1**, ping **PC3**.

Why were the pings successful?

Step 2: Ping devices on remote networks to test ACL functionality.

a. From the command prompt of **PC1**, ping **PC4**.

b. From the command prompt of **PC1**, ping the **DNS Server**.

Why did the pings fail? (**Hint**: Use simulation mode or view the router configurations to investigate.)

Part 2: Remove the ACL and Repeat the Test

Step 1: Use show commands to investigate the ACL configuration.

a. Navigate to R1 CLI. Use the **show run** and **show access-lists** commands to view the currently configured ACLs. To quickly view the current ACLs, use **show access-lists**. Enter the **show access-lists** command, followed by a space and a question mark (?) to view the available options:

Open configuration window

```
R1# show access-lists ?
<1-199> ACL number
WORD ACL name
<cr>
```

If you know the ACL number or name, you can filter the **show** output further. However, **R1** only has one ACL; therefore, the **show access-lists** command will suffice.

```
R1#show access-lists
Standard IP access list 11
10 deny 192.168.10.0 0.0.0.255
20 permit any
```

The first line of the ACL blocks any packets that originate in the **192.168.10.0/24** network, which includes Internet Control Message Protocol (ICMP) echoes (ping requests). The second line of the ACL allows all other **ip** traffic from **any** source to transverse the router.

b. For an ACL to impact router operation, it must be applied to an interface in a specific direction. In this scenario, the ACL is used to filter traffic exiting an interface. Therefore, all traffic leaving the specified interface of R1 will be inspected against ACL 11.

Although you can view IP information with the **show ip interface** command, it may be more efficient in some situations to simply use the **show run** command. To obtain a complete list of interfaces that the ACL that may be applied to, and the list of all ACLs that are configured, use the following command:

```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface Serial0/0/0
ip access-group 11 out
interface Serial0/0/1
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
```

The second pipe symbol '|" creates an OR condition that matches 'interface' OR 'access'. It is important that no spaces are included in the OR condition. Use one or both of these commands to find information about the ACL.**Qestion:**

To which interface and in what direction is the ACL applied?

Step 2: Remove access list 11 from the configuration.

You can remove ACLs from the configuration by issuing the **no access list** [*number of the ACL*] command. The **no access-list** command when used without arguments deletes all ACLs configured on the router. The **no access-list** [*number of the ACL*] command removes only a specific ACL. Removing an ACL from a router does not remove the ACL from the interface. The command that applies the ACL to the interface must be removed separately.

a. Under the Serial0/0/0 interface, remove access-list 11, which was previously applied to the interface as an **outgoing** filter:

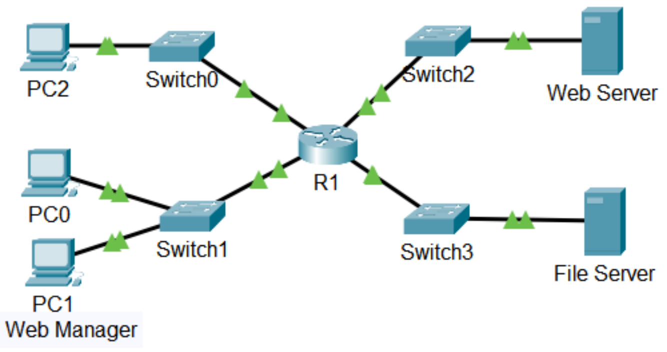
```
R1(config)# interface s0/0/0
R1(config-if)# no ip access-group 11 out
```

b. In global configuration mode, remove the ACL by entering the following command:

```
R1(config)# no access-list 11
```

c. Verify that **PC1** can now ping the **DNS Server** and **PC4**.

7. Configure Named Standard IPv4 ACLs



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
R1	F0/1	192.168.20.1	255.255.255.0	N/A
R1	E0/0/0	192.168.100.1	255.255.255.0	N/A
R1	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Blank Line - no additional information

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

Background / Scenario

The senior network administrator has asked you to create a standard named ACL to prevent access to a file server. The file server contains the data base for the web applications. Only the Web Manager workstation PC1 and the Web Server need to access the File Server. All other traffic to the File Server should be denied.

Instructions

Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.

Step 2: Configure a named standard ACL.

Open configuration window

a. Configure the following named ACL on **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
```

```
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# permit host 192.168.100.100
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive, and the statements must be in the same order as shown.

b. Use the **show access-lists** command to verify the contents of the access list before applying it to an interface. Make sure you have not mistyped any IP addresses and that the statements are in the correct order.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

Step 3: Apply the named ACL.

a. Apply the ACL outbound on the Fast Ethernet 0/1 interface.

Note: In an actual operational network, applying an access list to an active interface is not a good practice and should be avoided if possible.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. Save the configuration.

Close configuration window

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Open configuration window

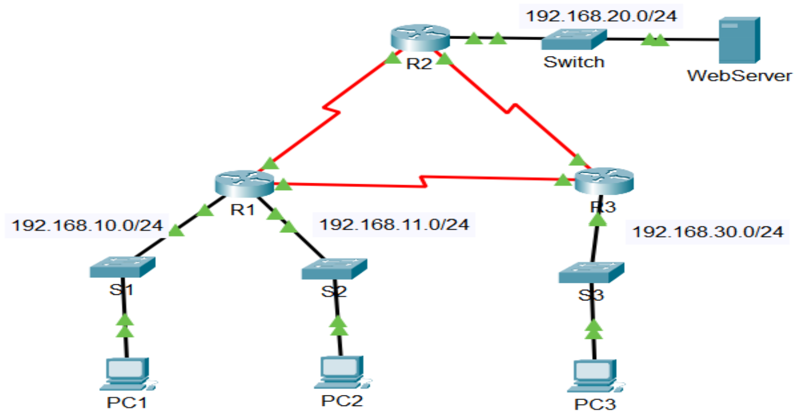
Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** and the **Web Server** should be able to ping the **File Server**. Repeat the **show access-lists** command to see the number of packets that matched each statement.

End of document
Close configuration window

8. Configure Numbered Standard IPv4 ACLs



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
R1	G0/1	192.168.11.1	255.255.255.0	N/A
R1	S0/0/0	10.1.1.1	255.255.255.252	N/A
R1	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
R3	S0/0/0	10.3.3.2	255.255.255.252	N/A
R3	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Blank Line - no additional information

Objectives

Part 1: Plan an ACL Implementation

Part 2: Configure, Apply, and Verify a Standard ACL

Background / Scenario

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Instructions

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

Step 2: Evaluate two network policies and plan ACL implementations.

a. The following network policies are implemented on **R2**:

- The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

b. The following network policies are implemented on **R3**:

- The 192.168.10.0/24 network is not allowed to communicate with the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

a. Create an ACL using the number **1** on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

Open configuration window

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. By default, an access list denies all traffic that does not match any rules. To permit all other traffic, configure the following statement:

```
R2(config)# access-list 1 permit any
```

c. Before applying an access list to an interface to filter traffic, it is a best practice to review the contents of the access list, in order to verify that it will filter traffic as expected.

```
R2# show access-lists
Standard IP access list 1
       10 deny 192.168.11.0 0.0.0.255
       20 permit any
```

d. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface. Note: In an actual operational network, it is not a good practice to apply an untested access list to an active interface.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Step 2: Configure and apply a numbered standard ACL on R3.

a. Create an ACL using the number **1** on **R3** with a statement that denies access to the 192.168.30.0/24 network from the **PC1** (192.168.10.0/24) network.

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. By default, an ACL denies all traffic that does not match any rules. To permit all other traffic, create a second rule for ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Verify that the access list is configured correctly.

```
R3# show access-lists
Standard IP access list 1
      10 deny 192.168.10.0 0.0.0.255
      20 permit any
```

d. Apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Step 3: Verify ACL configuration and functionality.

a. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.
- A ping from 192.168.11.10 to 192.168.20.254 fails.
- A ping from 192.168.10.10 to 192.168.30.10 fails.
- A ping from 192.168.11.10 to 192.168.30.10 succeeds.
- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

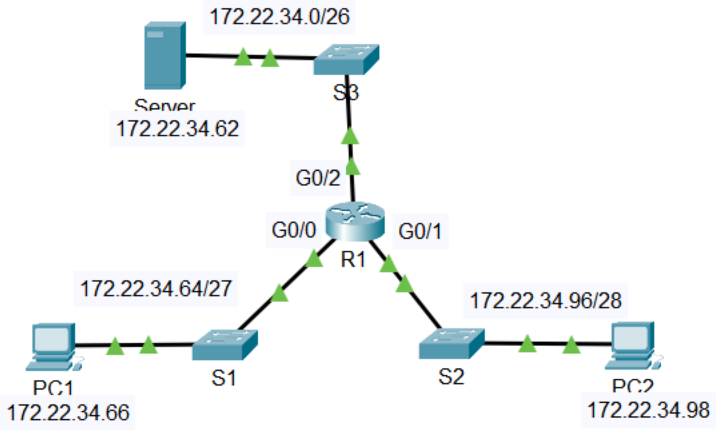
c. Issue the **show access-lists** command again on routers **R2** and **R3**. You should see output that indicates the number of packets that have matched each line of the access list. Note: The number of matches shown for your routers may be different, due to the number of pings that are sent and received.

```
R2# show access-lists
Standard IP access list 1
      10 deny 192.168.11.0 0.0.0.255 (4 match(es))
      20 permit any (8 match(es))

R3# show access-lists
Standard IP access list 1
      10 deny 192.168.10.0 0.0.0.255 (4 match(es))
      20 permit any (8 match(es))
```

Close configuration window
End of document

9. Configure Extended ACLs - Scenario 1



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
R1	G0/1	172.22.34.97	255.255.255.240	N/A
R1	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

Blank Line - no additional information

Objectives

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

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

Background / Scenario

Two employees need access to services provided by the server. **PC1** only needs FTP access while **PC2** only needs web access. Both computers need to be able to ping the server, but not each other.

Instructions

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

Step 1: Configure an ACL to permit FTP and ICMP from PC1 LAN.

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

Open configuration window

```
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 Specify packets to reject
permit 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. When configured and applied, this ACL should permit FTP and ICMP. ICMP is listed above, but FTP is not. This is because FTP is an application layer protocol that uses TCP at the transport layer. Enter TCP to further refine the ACL help.

```
R1(config)# access-list 100 permit tcp?
A.B.C.D Source address
any Any source host
host A single source host
```

e. The source address can represent a single device, such as PC1, by using the **host** keyword and then the IP address of PC1. Using the keyword **any** permits any host on any network. Filtering can also be done by a network address. In this case, it is any host that has an address belonging to the 172.22.34.64/27 network. Enter this 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 by determining the binary opposite of the /27 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
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
```

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 established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq 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 a specific type of ICMP traffic does not need 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.

l. Execute the **show access-list** command and verify that access list 100 contains the correct statements. Notice that the statement **deny any any** does not appear at the end of the access list. The default execution of an access list is that if a packet does not match a statement in the access list, it is not permitted through the interface.

```
R1#show access-lists
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

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 the Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

Note: On an actual operational network, it is not a good practice to apply an untested access list to an active interface.

```
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.

```
ftp> quit
```

close configuration window

d. Ping from PC1 to PC2. The destination host should be unreachable, because the ACL did not explicitly permit the traffic.

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

Step 1: Configure an ACL to permit HTTP access and ICMP from PC2 LAN.

a. Named ACLs start with the **ip** keyword. From global configuration mode of **R1**, enter the following command, followed by a question mark.

Open configuration window

```
R1(config)# ip access-list?
extended Extended Access List
standard Standard 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 and the access list statements must be the correct order.)

```
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 ?
A.B.C.D Source wildcard bits
```

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 extended named ACL configuration mode.

h. Execute the **show access-list** command and verify that access list **HTTP_ONLY** contains the correct statements.

```
R1# show access-lists
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

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 the Gigabit Ethernet 0/1 interface. Enter interface configuration mode and apply the ACL.

Note: On an actual operational network, it is not a good practice to apply an untested access list to an active interface. It should be avoided if possible.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Step 3: Verify the ACL implementation.

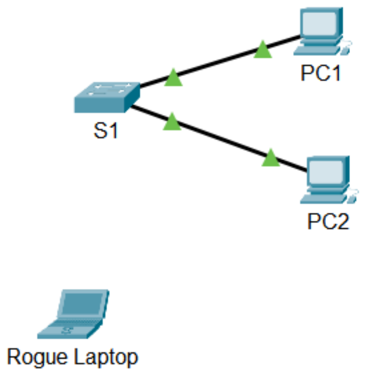
a. Ping from **PC2** to **Server**. If the ping is unsuccessful, verify the IP addresses before continuing.

b. From PC2 open a web browser and enter the IP address of the Server. The web page of the Server should be displayed.

c. FTP from **PC2** to **Server**. The connection should fail. If not, troubleshoot the access list statements and the access-group configurations on the interfaces.

Close configuration window
End of document
t

10. Implement Port Security



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Device	Interface	IP Address	Subnet Mask
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Blank Line - no additional information

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Part 1: Configure Port Security

a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

Open Configuration Window

```
S1(config)# interface range f0/1 - 2
S1(config-if-range)# switchport port-security
```

b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

```
S1(config-if-range)# switchport port-security maximum 1
```

c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

```
S1(config-if-range)# switchport port-security mac-address sticky
```

d. Set the violation mode so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

```
S1(config-if-range)# switchport port-security violation restrict
```

e. Disable all the remaining unused ports. Use the **range** keyword to apply this configuration to all the ports simultaneously.

```
S1(config-if-range)# interface range f0/3 - 24, g0/1 - 2
S1(config-if-range)# shutdown
```

Part 2: Verify Port Security

a. From **PC1**, ping **PC2**.

b. Verify that port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

```
S1# show run | begin interface
```

c. Use port-security show commands to display configuration information.

```
S1# show port-security
S1# show port-security address
```

d. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

e. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

f. Disconnect **PC2** and connect **Rogue Laptop** to F0/2, which is the port to which PC2 was originally connected. Verify that **Rogue Laptop** is unable to ping **PC1**.

g. Display the port security violations for the port to which **Rogue Laptop** is connected.

```
S1# show port-security interface f0/2
```

Close Configuration Window
Question

How many violations have occurred?

Type your answers here.

h. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.

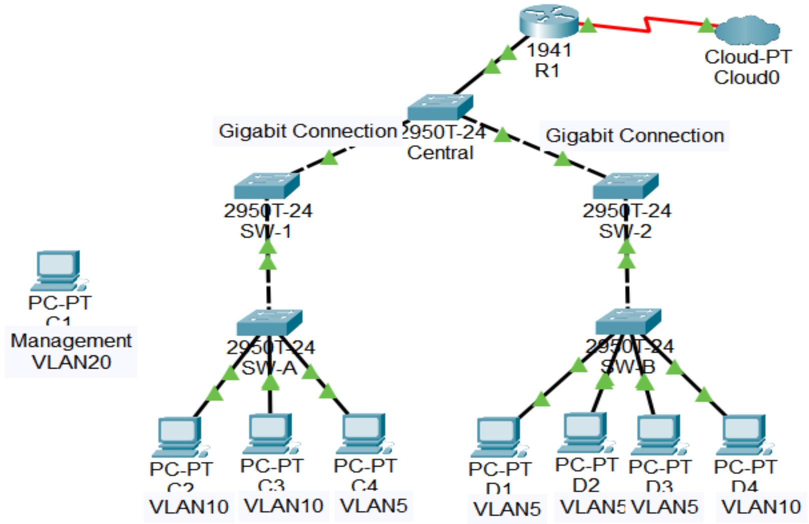
Question

Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?

Type your answers here.

End of Document

11. Layer 2 VLAN Security



Objectives

- Connect a new redundant link between switches.
- Enable trunking and configure security on the new trunk link between switches.
- Create a new management VLAN and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Background / Scenario

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to enable the management PC to connect to all switches and the router but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

All devices have been preconfigured with:

- Enable secret password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- SSH username and password: **SSHadmin** / **ciscosshpa55**

Instructions

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.

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**.

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

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**.

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

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.

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.

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

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.

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

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**.

Question: Were the pings successful? Explain.

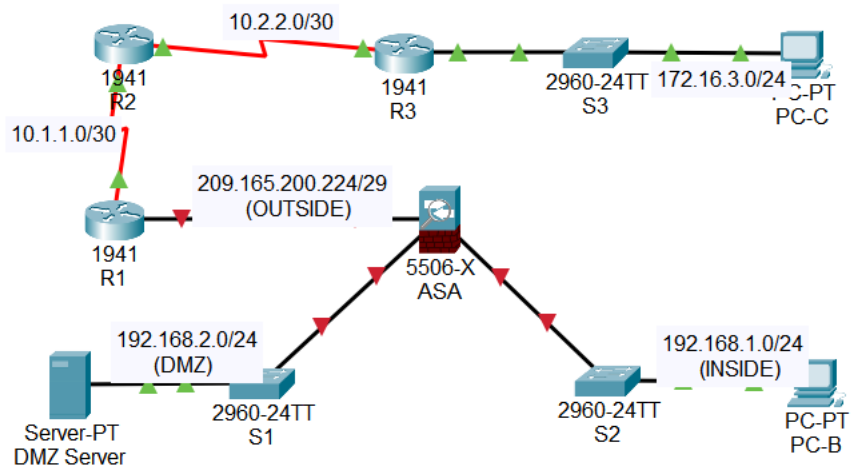
c. From **D1**, ping the management PC. Were the pings successful? Explain.

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.

12. Configure ASA Basic Settings and Firewall Using the CLI



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
R3	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	G1/1	209.165.200.226	255.255.255.248	NA
ASA	G1/2	192.168.1.1	255.255.255.0	NA
ASA	G1/3	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Blank Line, No additional information

Objectives

- Verify connectivity and explore the ASA
- Configure basic ASA settings and interface security levels using CLI
- Configure routing, address translation, and inspection policy using CLI
- Configure DHCP, AAA, and SSH
- Configure a DMZ, Static NAT, and ACLs

Scenario

Your company has one location connected to an ISP. R1 represents a CPE device managed by the ISP. R2 represents an intermediate Internet router. R3 represents an ISP that connects an administrator from a network management company, who has been hired to remotely manage your network. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network and by the remote administrator. The ISP assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

All router and switch devices have been preconfigured with the following:

- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- Admin username and password: **admin**/**adminpa55**

Note: This Packet Tracer activity is not a substitute for the ASA labs. This activity provides additional practice and simulates most of the ASA 5506-X configurations. When compared to a physical ASA 5506-X, there may be slight differences in command output or commands that are not yet supported in Packet Tracer.

Instructions

Part 1: Verify Connectivity and Explore the ASA

Step 1: Verify connectivity.

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface. PC-C is unable to ping the ASA, PC-B, or the DMZ server.

Step 2: Determine the ASA version, interfaces, and license.

Use the **show version** command to determine various aspects of this ASA device.

Step 3: Determine the file system and contents of flash memory.

a. Enter privileged EXEC mode. A password has not been set. Press **Enter** when prompted for a password.

b. Use the **show file system** command to display the ASA file system and determine which prefixes are supported.

c. Use the **show flash:** or **show disk0:** command to display the contents of flash memory.

Part 2: Configure ASA Settings and Interface Security Using the CLI

Tip: Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and submodes is essentially the same.

Step 1: Configure the hostname and domain name.

a. Configure the ASA hostname as **NETSEC-ASA**.

b. Configure the domain name as **netsec.com**.

Step 2: Configure the enable mode password.

Use the **enable password** command to change the privileged EXEC mode password to **ciscoenpa55**.

Step 3: Set the date and time.

Use the **clock set** command to manually set the date and time (this step is not scored).

Step 4: Configure the INSIDE and OUTSIDE interfaces.

You will only configure the G1/1 (OUTSIDE) and G1/2 (INSIDE) interfaces at this time. The G1/3 (DMZ) interface will be configured in Part 5 of the activity.

a. Create the G1/1 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and enable the interface.

```
NETSEC-ASA(config-if)# interface g1/1
NETSEC-ASA(config-if)# nameif OUTSIDE
NETSEC-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
NETSEC-ASA(config-if)# security-level 0
NETSEC-ASA(config-if)# no shutdown
```

b. Configure the G1/2 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100 and enable the interface.

```
NETSEC-ASA(config)# interface g1/2
NETSEC-ASA(config-if)# nameif INSIDE
NETSEC-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
NETSEC-ASA(config-if)# security-level 100
NETSEC-ASA(config-if)# no shutdown
```

c. Use the following verification commands to check your configurations:

1) Use the **show interface ip brief** command to display the status for all ASA interfaces.

Note: This command is different from the IOS command **show ip interface brief**. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

Tip: Most ASA **show** commands, including **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command.

2) Use the **show ip address** command to display the interface information.

Step 5: Test connectivity to the ASA.

a. You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary.

b. From PC-B, ping the G1/1 (OUTSIDE) interface at IP address 209.165.200.226. You should not be able to ping this address.

Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI

Step 1: Configure a static default route for the ASA.

Configure a default static route on the ASA OUTSIDE interface to enable the ASA to reach external networks.

a. Create a “quad zero” default route using the **route** command, associate it with the ASA OUTSIDE interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

```
NETSEC-ASA(config)# route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
```

b. Issue the **show route** command to verify the static default route is in the ASA routing table.

c. Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary.

Step 2: Configure address translation using PAT and network objects.

a. Create network object **INSIDE-NET** and assign attributes to it using the **subnet** and **nat** commands.

```
NETSEC-ASA(config)# object network INSIDE-NET
NETSEC-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
NETSEC-ASA(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
NETSEC-ASA(config-network-object)# exit
```

b. The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run** command.

c. From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.

d. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four were not. The outgoing pings (echos) were translated and sent to the destination. The returning echo replies were blocked by the firewall policy.

Part 4: Configure DHCP, AAA, and SSH

Step 1: Configure the ASA as a DHCP server.

a. Configure a DHCP address pool and enable it on the ASA INSIDE interface.

```
NETSEC-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 INSIDE
```

b. (Optional) Specify the IP address of the DNS server to be given to clients.

```
NETSEC-ASA(config)# dhcpd dns 209.165.201.2 interface INSIDE
```

c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (INSIDE).

```
NETSEC-ASA(config)# dhcpd enable INSIDE
```

d. Change PC-B from a static IP address to a DHCP client and verify that it receives IP addressing information. Troubleshoot, as necessary to resolve any problems.

Step 2: Configure AAA to use the local database for authentication.

a. Define a local user named **admin** by entering the **username** command. Specify a password of **adminpa55**.

```
NETSEC-ASA(config)# username admin password adminpa55
```

b. Configure AAA to use the local ASA database for SSH user authentication.

```
NETSEC-ASA(config)# aaa authentication ssh console LOCAL
```

Step 3: Configure remote access to the ASA.

The ASA can be configured to accept connections from a single host or a range of hosts on the INSIDE or OUTSIDE network. In this step, hosts from the OUTSIDE network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network.

a. Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter **no** when prompted to replace them.

```
NETSEC-ASA(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.


Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

b. Configure the ASA to allow SSH connections from any host on the INSIDE network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the OUTSIDE network. Set the SSH timeout to 10 minutes (the default is 5 minutes).

```
NETSEC-ASA(config)# ssh 192.168.1.0 255.255.255.0 INSIDE
NETSEC-ASA(config)# ssh 172.16.3.3 255.255.255.255 OUTSIDE
NETSEC-ASA(config)# ssh timeout 10
```

c. Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful.

```
C:\> ssh -l admin 209.165.200.226
```

d. Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

```
C:\> ssh -l admin 192.168.1.1
```

Part 5: Configure a DMZ, Static NAT, and ACLs

R1 G0/0 and the ASA OUTSIDE interface already use 209.165.200.225 and .226, respectively. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

Step 1: Configure the DMZ interface VLAN 3 on the ASA.

a. Configure DMZ VLAN 3, which is where the public access web server will reside. Assign it IP address 192.168.2.1/24, name it **DMZ**, and assign it a security level of 70. Because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

```
NETSEC-ASA(config)# interface g1/3
NETSEC-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
NETSEC-ASA(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
NETSEC-ASA(config-if)# security-level 70
NETSEC-ASA(config-if)# no shutdown
```

b. Use the following verification commands to check your configurations:

Use the **show interface ip brief** command to display the status for the ASA interfaces.

Use the **show ip address** command to display the information for the ASA interfaces.

Step 2: Configure static NAT to the DMZ server using a network object.

Configure a network object named **DMZ-SERVER** and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an OUTSIDE address using static NAT, and specify a public translated address of 209.165.200.227.

```
NETSEC-ASA(config)# object network DMZ-SERVER
NETSEC-ASA(config-network-object)# host 192.168.2.3
NETSEC-ASA(config-network-object)# nat (DMZ,OUTSIDE) static
209.165.200.227
NETSEC-ASA(config-network-object)# exit
```

Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

Configure a named access list **OUTSIDE-DMZ** that permits the TCP protocol on port 80 from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA OUTSIDE interface in the “IN” direction.

```
NETSEC-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host
192.168.2.3
NETSEC-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host
192.168.2.3 eq 80
NETSEC-ASA(config)# access-group OUTSIDE-DMZ in interface OUTSIDE
```

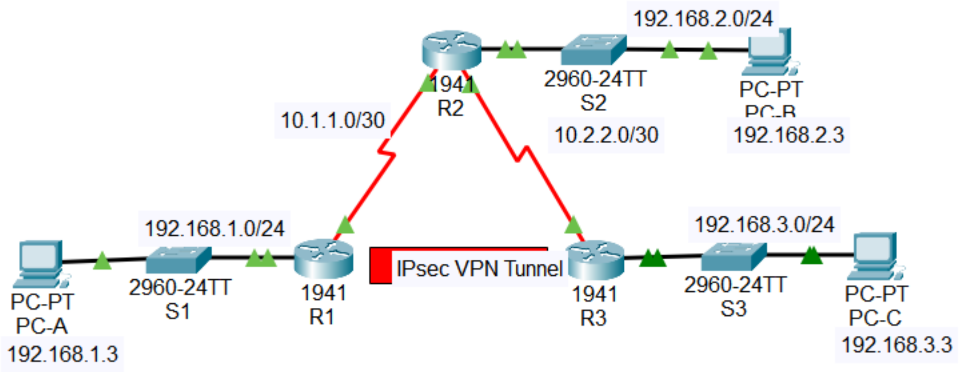
Note: Unlike IOS ACLs, the ASA ACL permit statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.

Step 4: Test access to the DMZ server.

From a web browser on PC-C, navigate to the DMZ server (209.165.200.227). Troubleshoot if it is not successful.

End of document

13. Configure and Verify a Site-to-Site IPsec VPN



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
R1	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
R2	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
R3	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
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

Blank Line, No additional information

Objectives

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.

Background / Scenario

The network topology shows three routers. Your task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	DES, 3DES, or **AES**	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication Method	**Pre-shared keys** or RSA	pre-share	pre-share
Key Exchange	DH Group 1, 2, or **5**	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		vpnpa55	vpnpa55

Blank Line, No additional information

Note: Bolded parameters are defaults. Only unbolded parameters have to be explicitly configured.

IPsec Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Blank Line, No additional information

The routers have been pre-configured with the following:

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin** / **ciscosshpa55**
- OSPF 101

Instructions

Part 1: Configure IPsec Parameters on R1

Step 1: Test connectivity.

Ping from PC-A to PC-C. The devices are all configured with routing. Therefore, the ping should succeed.

Step 2: Enable the Security Technology package.

a. On **R1**, issue the **show version** command to view the Security 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. Use the **show version** command again to verify that the **securityk9** is listed under current Technology packages.

Step 3: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on **R1** to the LAN on **R3** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the **R1** to **R3** LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit **deny all**, there is no need to configure a **deny ip any any** statement.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.

Configure the **crypto ISAKMP policy 10** properties on **R1** along with the shared crypto key **vpnpa55**. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

Note: The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 24.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

a. Create the transform-set VPN-SET to use **esp-aes and esp-sha-hmac**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Step 6: Configure the crypto map on the outgoing interface.

Bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface.

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

Part 2: Configure IPsec Parameters on R3

Step 1: Enable the Security Technology package.

a. On **R3**, issue the **show version** command to verify that the Security Technology package license information has been enabled.

b. If the Security Technology package has not been enabled, enable the package and reload **R3**.

Step 2: Configure router R3 to support a site-to-site VPN with R1.

Configure reciprocating parameters on **R3**. Configure ACL 110 identifying the traffic from the LAN on **R3** to the LAN on **R1** as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.

Configure the crypto ISAKMP policy 10 properties on **R3** along with the shared crypto key vpnpa55.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Step 4: Configure the IKE Phase 2 IPsec policy on R3.

a. Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Step 5: Configure the crypto map on the outgoing interface.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface. **Note**: This is not graded.

```
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
```

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on **R1**. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.

Step 2: Create interesting traffic.

Ping PC-C from PC-A.

Step 3: Verify the tunnel after interesting traffic.

On **R1**, re-issue the **show crypto ipsec sa** command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

Step 4: Create uninteresting traffic.

Ping **PC-B** from **PC-A**. **Note**: Issuing a ping from router **R1** to **PC-C** or **R3** to **PC-A** is not interesting traffic.

Step 5: Verify the tunnel.

On **R1**, re-issue the **show crypto ipsec sa** command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

Step 6: Check results.

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

end of document