Activity 4.1 - Research Internet Access Technologies

Objectives

Part 1: Investigate Broadband Distribution

Part 2: Research Broadband Access Options for Specific Scenarios

Background / Scenario

Although broadband internet access options have increased dramatically in recent years, broadband access varies greatly depending on location. In this lab, you will investigate current broadband distribution and research broadband access options for specific scenarios.

Required Resources

Device with internet access

Part 1: Investigate Broadband Distribution

In Part 1, you will research broadband distribution in a geographical location.

Step 1: Research broadband distribution.

Use the internet to research the following questions:

a. For the country in which you reside, what percentage of the population has broadband internet subscriptions?

According to Statista, 72.7% of the Philippine population has broadband internet subscriptions in 2020 and it was estimated that in 2023, there would be about 76% of the population using the internet.

Philippines: internet penetration rate 2017-2026 | Statista. (2017). Statista; Statista. https://www.statista.com/statistics/975072/internet-penetration-rate-in-the-philippines/

b. What percentage of the population is without broadband internet options?

According to the Inquirer article entitled “Mapping Digital Poverty in PH,” 83% of the Philippine population have broadband internet options which leads 17% of the population without broadband internet options.

Carrasco, B. (2021, February). Mapping digital poverty in PH. INQUIRER.net; INQUIRER.net. https://business.inquirer.net/318223/mapping-digital-poverty-in-ph

Step 2: Discover dedicated WAN technology service providers.

Using a search engine, research WAN technology offered by the local service providers. Complete the table below by identifying each service provider's WAN services, based on the information provided on the website. Note that some of these technologies are considered enterprise connection types and could be listed under separate web portal of the service provider

Internet Service Provider	Leased Line	MPLS	Ethernet Private Line (EPL)	VSAT	DSL	Cable Internet	Cellular Broadband	FTTH
PLDT / Smart	International Private Leased Circuit	Metro E-WAN	Metro E-Line	Gilat Satellite Networks	PLDT Home DSL (discontinued)	N/A	Smart Bro	fiber-powered fixed line
Globe	IPL Time Division Multiplexing (TDM)	International E-Line	E-Line	Gilat Satellite Networks	Globe At Home DSL	N/A	GFiber	Globe At Home internet
Sky Internet	N/A	N/A	N/A	(discontinued)	Sky Broadband	Sky Cable	N/A	Sky Fiber
Converge	N/A	Converge Connect	International Private Line	VSAT	N/A	N/A	N/A	FiberX
DITO Telecom	N/A	N/A	N/A	in the works	N/A	N/A	Dito Flash 5G Home	in the works

Part 2: Research Broadband Access Options for Specific Scenarios

In Part 2, you will research and detail broadband options for the following scenarios and select the best last-mile technology to meet the needs of the consumer. For each scenario, use the area of residence of one member of the group to serve as the hypothetical location in which the scenario will take place; and identify providers and services available in the area accordingly.

.

Scenario 1: You are moving to San Juan City, Metro Manila and are exploring home internet connections. Research and detail 3 internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed
Globe	*Fiber*	*Php 2,099*	*300 Mbps*
Converge	*Fiber*	*Php 2,000*	*300 Mbps*
PLDT	*Fiber*	*Php 2,799*	*300 Mbps*

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

From the list of local ISPs, I would choose PLDT. Even though it has the highest cost per month for the same download speed, it ranked the best overall in the Ookla Speedtest Awards for the third to fourth quarter of 2021. PLDT had the fastest speed among its competitors based on the actual data gathered by Speedtest.net and it is provided in at least 60% of Philippine towns and cities. Their installation and application process is smooth and easy while they provide various other options along with Smart. Despite the slightly higher cost per Mbps, I think it would be worth it with the speed and service that they provide.

Scenario 2: You are moving to Balayan, Batangas and your job requires you to have 24 hours anytime/anywhere access. Research and detail 3 internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed
Globe	*Cellular Broadband*	*Php 999*	*42 Mbps*
Converge	*Fiber*	*Php 1,500*	*100 Mbps*
Sky	*Cellular Broadband*	*Php 1,499*	*42 Mbps*

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

Considering that ISP connection is portable and is able to be accessed anytime. The best choice in this scenario is Globe's MyFi which is a pocket wifi. In terms of cost it is lower than Sky's SkyMobi (pocket wifi of Sky) and since Converge doesn't produce pocket wifi's Globe's MyFi is the ideal choice. Additionally, Globe's MyFi has packages that provide 100 GB worth of data access while Sky's SkyMobi only provides 10 GB.

Scenario 3: Your business in Taft Avenue, Manila is expanding to 25 employees and will need to upgrade your broadband access to include internet connection for onsite equipment and web hosting. Research and detail 3 internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed
PLDT	*Fiber*	*Php 2,490*	*100 mbps*
Globe	*Fiber*	*Php 2,499*	*200 mbps*
Converge	*Fiber*	*Php 1,500*	*100 mbps*

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

Similarly to the first example, from the list of local ISPs, I would choose PLDT. Even though it has the highest cost per month for the same download speed, it ranked the best overall in the Ookla Speedtest Awards for the third to fourth quarter of 2021. PLDT had the fastest speed among its competitors based on the actual data gathered by Speedtest.net and it is provided in at least 60% of Philippine towns and cities. Their installation and application process is smooth and easy while they provide various other options along with Smart. Despite the slightly higher cost per Mbps, I think it would be worth it with the speed and service that they provide. In Metro Manila, PLDT is established as the leader in telecommunications, so it would be a safe option to go with them.

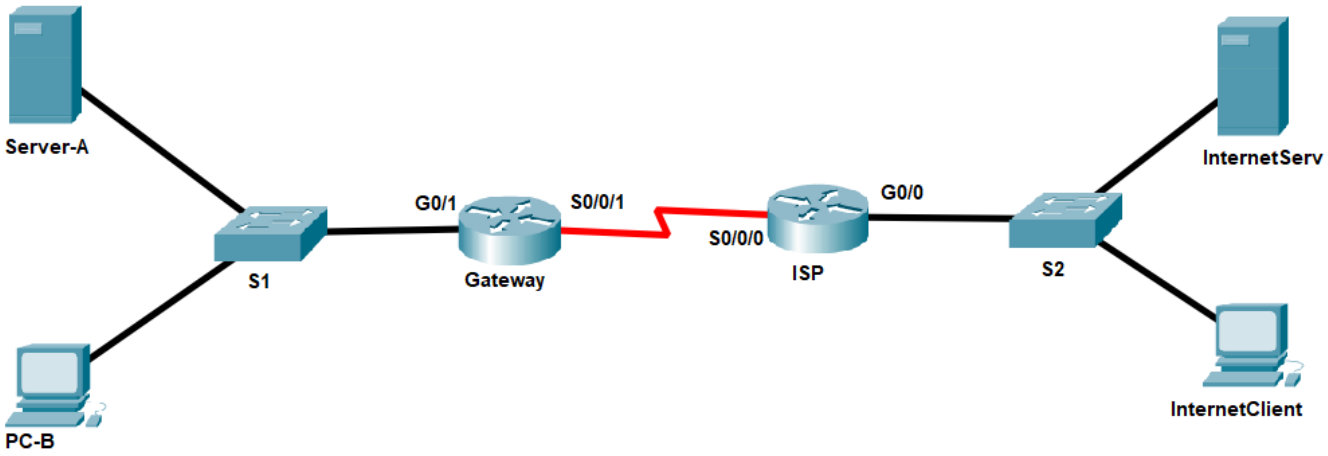
Reflection Question

Despite the high demand for Internet connectivity in the Philippines, Internet access in the country remains to be lacking in some locations, as well as slow and expensive in comparison to several of our Asian neighbors. What could be the reasons for these issues?

With the increasing demand for Internet connectivity in the Philippines, most especially for online work and education, our country has not been able to keep up or accommodate the need for it. One of the reasons for this issue is the high costs and expenses that are involved, whether personal or public. Some of these expensive costs include, but are not limited to, internet subscription, equipment, and infrastructure. With the high costs, it is just not affordable for the general public. Another possible reason is the lack of service providers in the country which leaves little to no competition between them. Since Filipinos would have no choice than to avail of the services provided by the limited providers, companies may not feel the need to improve their services because they are able to thrive despite the lack in their services and improvements. It is also possible that the difficult and various regulations needed for service providers to build the necessary infrastructure makes it nearly impossible for them to provide to further or harder to reach locations.

Lab 5.1 Static and Dynamic NAT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	G0/0	192.31.7.1	255.255.255.0	N/A
InternetSrv	NIC	192.31.7.100	255.255.255.0	192.31.7.1
InternetClient	NIC	192.31.7.2	255.255.255.0	192.31.7.1
Server-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

Background / Scenario

Network Address Translation (NAT) is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited.

In this lab, an ISP has allocated the public IP address space of 209.165.200.224/27 to a company. This provides the company with 30 public IP addresses. The addresses, 209.165.200.225 to 209.165.200.241, are for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. A static route is used from the ISP to the gateway router, and a default route is used from the gateway to the ISP router. The ISP connection to the Internet is simulated by a loopback address on the ISP router.

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure all device IP settings according to the given addressing table.

Step 3: Configure a VTY password on the ISP router

Enable telnet on the ISP router by configuring ‘cisco’ as the password on the VTY lines

Step 4: Configure static routing.

a. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 5: Save the running configuration to the startup configuration.

Step 6: Verify network connectivity.

a. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

b. From the Server-A and PC-B, ping the G0/1 interface on the Gateway router.

Were your pings successful?	Yes

Troubleshoot your settings if these don’t work

c. From the Server-A and PC-B, ping the ISP router.

Were your pings successful?	No

Were the results expected? Why or why not?

Yes, the results were expected because the Gateway router does not know the remote network of the ISP router.

Part 2: Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

Step 1: Configure a static mapping.

A static map is configured to tell the router to translate between the private inside server address 192.168.1.20 and the public address 209.165.200.225. This allows a user from the Internet to access Server-A. ServerA will serve as a device with a constant address that can be accessed from the Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Step 2: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 3: Test the configuration.

a. Display the static NAT table by issuing the **show ip nat translations** command.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

What public address is ServerA's IP address translated to?	209.165.200.225
Who assigned the inside global address in this scenario?	The administrator, me
Who assigned the inside local address in this scenario?	The administrator, me

b. From Server-A, ping the G0/0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table using the **show ip nat translations** command

How is the output different from what was shown in the previous step?

Compared to the previous step, this output contains more lines and the pings were now successful.

What protocol was used by the translated traffic from ServerA to the ISP? Hint: Check the first column of the NAT table	ICMP

c. From ServerA, telnet to the ISP G0/0 interface and display the NAT table.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Note: The NAT for the ICMP request may have timed out and been removed from the NAT table.

What was the protocol used in this translation?	TCP
What are the port numbers used?	1025 and 23
What is the inside local address?	192.168.1.20
What is the inside global address?	209.165.200.225
What is the outside global address?	192.31.7.1

d. Because static NAT was configured for ServerA, verify that pinging from the InternetClient to ServerA at the static NAT public address (209.165.200.225) is successful.

e. On the Gateway router, display the NAT table to verify the translation.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    192.31.7.2:12      192.31.7.2:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Notice that the Outside local and Outside global addresses are the same. This address is the InternetClient's address. For the ping from the Internet to succeed, the Inside global static NAT address 209.165.200.225 was translated to the Inside local address of ServerA (192.168.1.20).

f. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Part 3: Configure and Verify Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

Step 1: Clear NATs.

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Step 2: Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 3: Verify that the NAT interface configurations are still valid.

Issue the **show ip nat statistics** command on the Gateway router to verify the NAT configurations.

Step 4: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Step 5: Define the NAT from the inside source list to the outside pool.

Note: Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Step 6: Test the configuration.

a. From PC-B, ping the G0/0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

What is the translation of the Inside local host address for PC-B?

What is the translation of the Inside local host address for PC-B?	192.168.1.21
Who assigned the inside global address in this scenario?	The Gateway router from the NAT pool
Who assigned the inside local address in this scenario?	The administrator, me

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

b. From PC-B, open a browser and enter the IP address of the Internet Server

c. Display the NAT table (Your output may differ from the example below).

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.100:80    192.31.7.100:80
```

What protocol was used in this translation?	TCP
What is the port number was used by the inside addresses?	1025
What is the port number was used by the outside addresses?	80
What well-known application service was involved in the transaction?	HTTP

d. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Step 7: Remove the static NAT entry.

a. Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Clear the NATs and statistics.

Step 8: Recreate NAT address mappings.

a. Ping the ISP (192.31.7.1) from Server-A. Afterwards, ping the ISP from PC-B.

b. Display the NAT table again of the Gateway router.

What public address is ServerA's IP address translated to?	209.165.200.242
What public address is PC-B's IP address translated to?	209.165.200.243

Is the public address assigned to PC-B identical to the one assigned prior to clearing the NAT table?	No

Display the NAT table and statistics. **Note**:. Your output may not match exactly with the sample below.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Reflection

1. Will using static NAT result in conservation of public IP Addresses? Why or why not?

Static Network Address Translation (SNAT) will result in conservation of public IP Addresses because they are assigned in a first-come first-serve basis. Static NAT is used to conserve IP addresses by allowing private IP networks with unregistered IP addresses to connect to the Internet. SNAT maps unregistered IP addresses using 1-to-1 network address translation to match up with registered IP addresses.

No, as you're still using 1 public IP address permanently mapped to every single internal host that needs to access an external network.

2. If dynamic NAT is used, will inside hosts be consistently translated to the same global/public IP address? Why or why not?

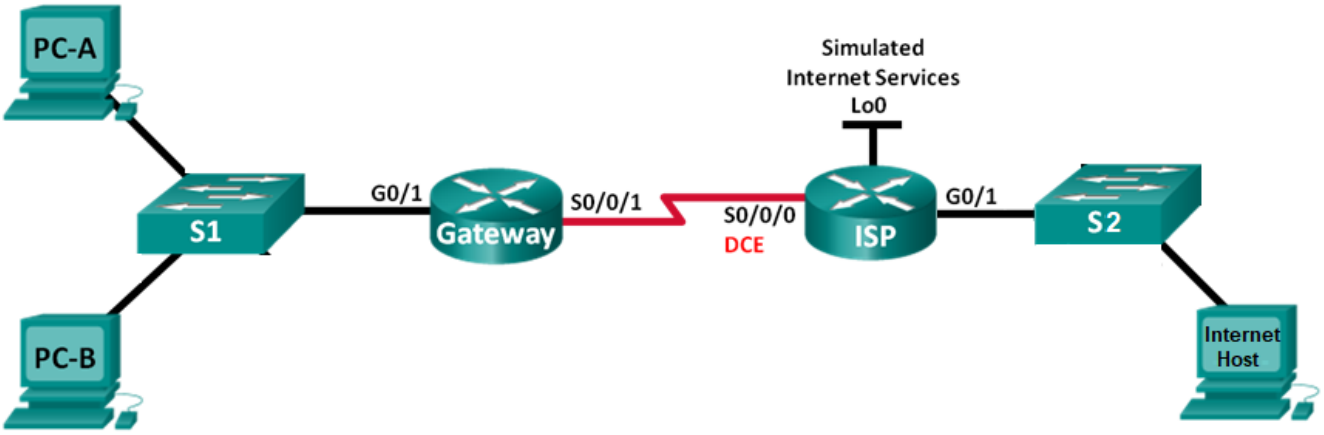
   If dynamic NAT is used, the inside hosts will not be consistently translated to the same global/public IP address because addresses are assigned in first-come first-serve basis. Dynamic NAT does the mapping of a local address to a global address happens dynamically. This means that the router dynamically picks an address from the global address pool that is not currently assigned. The dynamic entry stays in the NAT translations table as long as the traffic is exchanged. The entry times out after a period of inactivity and the global IP address can be used for new translations.

3. Compare static NAT vs dynamic NAT. Give at least 1 advantage that static NAT has over dynamic NAT, and at least 1 advantage that dynamic NAT has over static NAT.

   Static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not. On the other hand, dynamic NAT does not require an administrator to manually assign hosts to their public addresses.

Lab 5.2 PAT and Port Forwarding

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
	G0/1	100.100.100.1	255.255.255.0	N/A
S1	VLAN1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
Internet Client	NIC	100.100.100.100	255.255.255.0	100.100.100.1

Objectives

Part 1: Configure and Verify NAT Pool Overload

Part 2: Configure and Verify PAT

Part 3: Configure and Verify Port Forwarding

Background / Scenario

In the first part of the lab, your company is allocated the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of

IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns connections using the IP address plus a unique port number. After the maximum number of translations for a single IP address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool.

In Part 3, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the Internet connection from the company Gateway router to the ISP. You will use the PAT to convert multiple internal addresses into the one usable public address.

Finally in Part 4, you will use the port forwarding to allow external clients to access web and FTP services inside your network. Port forwarding allows the creation of static address translation maps using specific ports only. Doing so allows a network to host services for public access even when NAT overloading or PAT is used for internal hosts to access the Internet.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches.

Step 4: Configure basic settings for the S1 switch.

a. Configure IP addresses and default gateway as listed in the Addressing Table.

b. Configure device name as shown in the topology.

c. Enable Web access access on S1 to simulate a web server with local authentication for user admin.

```
S1(config)# ip http server
S1(config)# ip http authentication local
S1(config)# username admin privilege 15 secret class
```

Step 5: Configure basic settings for each router.

a. Configure IP addresses for the routers as listed in the Addressing Table.

b. Set the clock rate to **128000** for DCE serial interface.

c. Configure device name as shown in the topology.

d. Assign **cisco** as the console and vty passwords.

e. Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Configure static routing.

a. Create a static route from the ISP router to the Gateway router.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

b. Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 7: Verify network connectivity.

a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.

b. Verify that the static routes are configured correctly on both routers.

Part 2: Configure and Verify NAT Pool Overload

In Part 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

Step 1: Define an access control list that matches the LAN private IP addresses.

ACL 1 is used to allow the 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 2: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.225  209.165.200.230
netmask 255.255.255.248
```

Step 3: Define the NAT from the inside source list to the outside pool.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Step 4: Specify the inside interfaces.

In this topology, both G0/0 and G0/1 of the Gateway router are connected to networks with hosts that need to be translated; hence you will need to specify both as inside interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
```

Step 5: Specify the outside interface.

The S0/0/0 interface of the Gateway router is connected to the ISP; hence it will serve as the outside interface for NAT.

```
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 6: Verify the NAT pool overload configuration.

a. From each PC and switch host in the inside network, ping the 192.31.7.1 address on the ISP router

b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 4, occurred 00:00:25 ago
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  GigabitEthernet0/0
  GigabitEthernet0/1
Hits: 24  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
 pool public_access: netmask 255.255.255.248
        start 209.165.200.225 end 209.165.200.230
        type generic, total addresses 6, allocated 1 (16%), misses 0
```

c. Display NATs on the Gateway router.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1     192.31.7.1:1       192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.2:1      192.31.7.1:1       192.31.7.1:2
```

Note: Depending on how much time has elapsed since you performed the pings from each PC and S1r, you may not see all three translations. ICMP translations have a short timeout value.

How many Inside local IP addresses are listed in the sample output above?	3
How many Inside global IP addresses are listed?	1
How many port numbers are paired with the Inside global addresses?	3

What would be the result of pinging the Inside local address of PC-A from the Internet Server? Why?

The ping would not be successful because the router is aware of the location of the inside global address in its routing table but the inside local address is not advertised.

Part 3: Configure and Verify PAT

In Part 2, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all of the commands in Part 1 will be reused in Part 2.

Step 1: Clear NATs and statistics on the Gateway router.

Step 2: Verify the configuration for NAT.

a. Verify that statistics have been cleared.

b. Verify that the outside and inside interfaces are still configured for NATs.

c. Verify that the ACL is still configured for NATs.

What command did you use to confirm the results from steps a to c?

```
Gateway# show ip nat statistics
```

Step 3: Remove the pool of useable public IP addresses.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Step 4: Remove the NAT translation from inside source list to outside pool.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Step 5: Associate the source list with the outside interface.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Step 6: Test the PAT configuration.

a. From each PC and S1 of the internal network, ping the Internet Server.

b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 4, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  GigabitEthernet0/0
  GigabitEthernet0/1
Hits: 24  Misses: 0
Dynamic mappings:
```

c. Display NAT translations on Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.18:3  192.168.1.20:1     192.31.7.1:1       192.31.7.1:3
icmp 209.165.201.18:1  192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.201.18:4  192.168.1.2:1      192.31.7.1:1       192.31.7.1:4
```

Part 4: Configure and Verify Port Forwarding

In Part 4, you will configure port forwarding to S1 so that its HTTP service will be accessible to external hosts. This will be done by mapping address and TCP ports to the same public address configured on the Gateway.

Step 1: Map the web service ports of the global address to the Web Server.

a. To determine the correct mapping, you must be familiar with the port numbers used by well-known network services. Web services use the HTTP application layer protocols.

What transport layer protocol does HTTP use?	TCP

What well-known port number is associated with HTTP?	80

b. Configure the static mapping of the inside global address to the web service ports of the Web Server. The address of S0/0/0 will be used for this purpose.

```
Gateway(config)# ip nat inside source static tcp 192.168.1.2 80 209.165.201.18
                 80
```

Note: The **ip nat inside** and **ip nat outside** commands do not need to be repeated since these have been previously configured in Part 2.

Step 2: **Verify the port forwarding configuration.**

a. Display IP NAT statistics on the Gateway

```
Gateway# show ip nat statistics
Total active translations: 4 (4 static, 0 dynamic; 4 extended)
Peak translations: 4, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 15  Misses: 2
Expired translations: 0
Dynamic mappings:
```

b. Display the IP NAT table on the Gateway

```
Gateway# show ip nat translation
Pro     Inside global       Inside local     Outside local   Outside global
tcp     209.165.201.18:80    192.168.1.2:80      ---             ---
```

Step 3: **Test the PAT configuration.**

a. From the Internet PC, access the web service of S1 in the internal network by entering 'http://209.165.201.18' in a browser.

Did you get a response?	Yes

b. Display the NAT translation table on the Gateway router. Similar to static NAT, a new entry should have been automatically created for the web session.

To which host was the web connection request of the Internet PC sent?	Gateway router	S1

Reflection

1. What benefit does PAT/NAT overload have over static or dynamic NAT?

NAT translates the inside local addresses into inside global addresses; similarly, PAT translates the private unregistered IP addresses into public registered IP addresses. However, unlike NAT, PAT also uses source port numbers, allowing multiple hosts to share a single IP address while using different port numbers. Additionally, since there is only one public ip address that is assigned to a local network it won't be a hassle to configure each host with a public ip address like static NAT.

In summary, the primary advantage of PAT/NAT overload is that using the same public IP address, numerous devices from a single private network may access the internet or another remote network. In contrast to NAT, it also employs source port numbers, allowing numerous hosts with various port numbers to be allocated to the same IP address.

2. Why is port forwarding needed to host network services accessible to external hosts when the border router uses PAT/NAT overload?

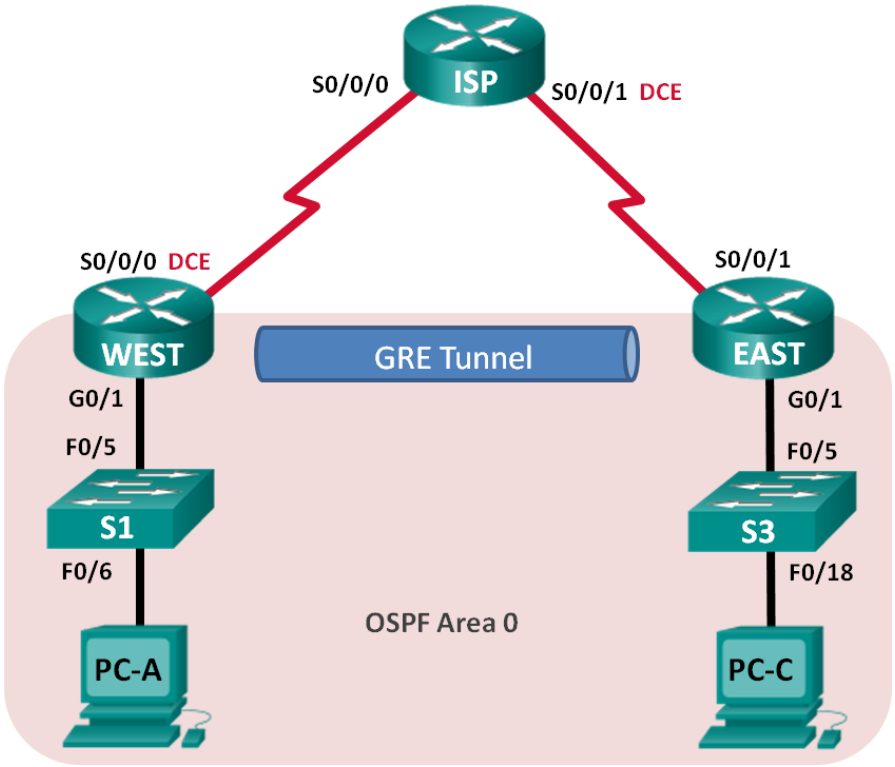
Port forwarding preserves public IP addresses. It can protect servers and clients from unwanted access, "hide" the services and servers available on a network and limit access to and from a network. It is used to keep unwanted traffic off networks. It also allows network administrators to use one IP address for all external communications on the Internet while dedicating multiple servers with different IPs and ports to the task internally. Port forwarding allows people on the internet to reach services on a private network that has a private addressing scheme.

Port forwarding is what allows outside hosts to access hosts within a private network that only have private IP addresses. For example, if a web server on my local network has a private address, users from outside my network would be unable to access it unless I enable port forwarding because private addresses are not routable on the internet. This is what we addressed in the last part of the activity, we enabled port forwarding so that external hosts could access the web server using https.

This is also doable using regular static NAT. Why is port forwarding necessary in particular when you're using PAT for your network?

Lab 6.1 Configuring a Point-to-Point GRE VPN Tunnel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	172.16.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
EAST	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure a GRE Tunnel

Part 3: Enable Routing over the GRE Tunnel

Background / Scenario

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of network layer protocols between two locations over a public network, such as the Internet.

GRE can be used with:

- Connecting IPv6 networks over IPv4 networks
- Multicast packets, such as OSPF, EIGRP, and streaming applications

In this lab, you will configure an unencrypted point-to-point GRE VPN tunnel and verify that network traffic is using the tunnel. You will also configure the OSPF routing protocol inside the GRE VPN tunnel. The GRE tunnel is between the WEST and EAST routers in OSPF area 0. The ISP has no knowledge of the GRE tunnel. Communication between the WEST and EAST routers and the ISP is accomplished using default static routes.

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses, routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings for each router.

a. Configure the device names.

b. Apply IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Do NOT configure the Tunnel0 interfaces at this time.

Step 3: Configure default routes to the ISP router.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Step 4: Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 5: Verify connectivity.

At this point, the PCs are unable to ping each other. Each PC should be able to ping its default gateway. The routers must be able to ping the serial interfaces of the other routers in the topology. If not, troubleshoot until you can verify connectivity.

Step 6: Save your running configuration.

Part 2: Configure a GRE Tunnel

In Part 2, you will configure a GRE tunnel between the WEST and EAST routers.

Step 1: Configure the GRE tunnel interface.

a. Configure the tunnel interface on the WEST router. Use S0/0/0 on WEST as the tunnel source interface and 10.2.2.1 as the tunnel destination on the EAST router.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

b. Configure the tunnel interface on the EAST router. Use S0/0/1 on EAST as the tunnel source interface and 10.1.1.1 as the tunnel destination on the WEST router.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source s0/0/1
EAST(config-if)# tunnel destination 10.1.1.1
```

Note: On real routers, either the interface name or the IP address can be used as the source for the **tunnel source** command,.

Step 2: Verify that the GRE tunnel is functional.

a. Verify the status of the tunnel interface on the WEST and EAST routers.

```
WEST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Tunnel0                    172.16.12.1     YES manual up                    up

EAST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
```

b. Issue the **show interfaces tunnel 0** command to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel.

What is the tunneling protocol used? What are the tunnel source and destination IP addresses associated with GRE tunnel on each router?

The tunneling protocol used is GRE. For the WEST router, the tunnel source is 10.1.1.1 (S0/0/0) while the destination IP address is 10.2.2.1. For the EAST router, the tunnel source is 10.2.2.1 (S0/0/1) while the destination IP address is 10.1.1.1.

c. Ping across the tunnel from the WEST router to the EAST router using the IP address of the tunnel interface.

```
WEST# ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

This should be successful. If not, troubleshoot your configuration.

d. Use the **traceroute** command on the WEST to determine the path to the tunnel interface on the EAST router. What is the path to the EAST router?

The path to the EAST router is 172.16.12.1 > 172.16.12.2

e. Ping and trace the route across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface.

What is the path to the WEST router from the EAST router? List the IP addresses appearing in the trace output.

The path to the WEST router from the EAST router is 172.16.12.2 > 172.16.12.1

With which interfaces are these IP addresses associated? Explain why these IP addresses are the ones that appear on the trace output instead of reflecting the actual path that packets take through the ISP.

The IP addresses are associated with the tunnel 0 interfaces on the WEST and EAST routers. These IP addresses are the ones that appear on the trace output instead of reflecting the actual path that packets take through the ISP because the traffic is using the tunnel.

f. The **ping** and **traceroute** commands should be successful. If not, troubleshoot before continuing to the next part.

Part 3: Enable Routing over the GRE Tunnel

In Part 3, you will configure OSPF routing so that the LANs on the WEST and EAST routers can communicate using the GRE tunnel.

After the GRE tunnel is set up, the routing protocol can be implemented. For GRE tunneling, a network statement will include the IP network of the tunnel, instead of the network associated with the serial interface. just like you would with other interfaces, such as Serial and Ethernet. Remember that the ISP router is not participating in this routing process.

Step 1: Configure OSPF routing for area 0 over the tunnel.

a. Configure OSPF process ID 1 using area 0 on the WEST router for the 172.16.1.0/24 and 172.16.12.0/24 networks.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Configure OSPF process ID 1 using area 0 on the EAST router for the 172.16.2.0/24 and 172.16.12.0/24 networks.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Step 2: Verify OSPF routing.

a. From the WEST router, issue the **show ip route** command to verify the route to 172.16.2.0/24 LAN on the EAST router.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

What is the exit interface and IP address to reach the 172.16.2.0/24 network?

> The exit interface and IP address to reach the 172.16.2.0/24 network is the tunnel 0 interface with IP address 172.16.12.2

b. From the EAST router issue the command to verify the route to 172.16.1.0/24 LAN on the WEST router.

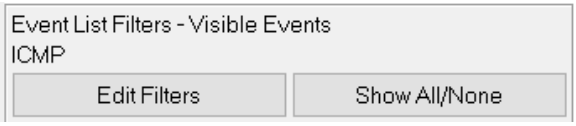
What is the exit interface and IP address to reach the 172.16.1.0/24 network?

> The exit interface and IP address to reach the 172.16.1.0/24 network is the tunnel 0 interface with IP address 172.16.12.1

Step 3: Observe the behavior of tunneled traffic.

a. Switch to Simulation mode on Packet Tracer.

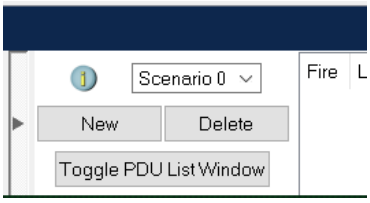
b. Set the event list filter to show only ICMP traffic.



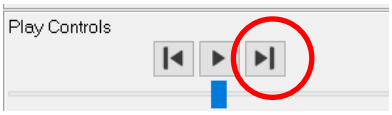
1) Click on the Show All/None button to clear all event types from the selection.
2) Click on Edit Filters
3) In the resulting pop up window, check ICMP and close the popup.

c. Observe an ICMP Packet as it traverses from the WEST to the EAST site.

1) Delete all packets that you may have created in your scenario list (click on 'Delete' button).



2) Perform a ping from PC-A to PC-C. Note that this will only show a packet representation of the ping message on the topology, but will not show any ping result yet because simulation mode gives you control over when packets move across network links.
3) Click on the play step button on your simulation controls. This will allow the packet to move to the next device in its path (S1).



4) Click on the play step button again for the packet to move from S1 to the WEST router.
5) Click on the currently stopped packet on the topology. A popup window will appear showing its contents. The 'In Layers' column shows how the packet looks like as it enters the current device; while the 'Out Layers' column shows how it looks like when it exits the device later on.

What is the source IP address of the ping as it ENTERS WEST?	172.16.1.3
What is the destination IP address of the ping as it ENTERS WEST?	172.16.2.3
What is the source IP address of the ping as it EXITS WEST?	10.1.1.1
What is the destination IP address of the ping as it EXITS WEST?	10.2.2.1

6) In the PDU pop up window, look at the contents of the 'Inbound PDU' and the Outbound PDU' tab which shows more details about packet contents and headers. Try to spot the differences in the way the incoming and outgoing packet is encapsulated.

What can you observe about the way the packet headers are structured?

The packet headers in Inbound PDU are EthernetII, IP, ICMP, and Variable Size PDU while the packet headers in Outbound PDU are HDLC, IP, GRE, IP, ICMP, and Variable Size PDU, which are more.

7) Click on play step button again until the ping packet reaches the EAST router.

8) Open the packet and check the contents.

What is the source IP address of the ping as it ENTERS EAST?	10.1.1.1
What is the destination IP address of the ping as it ENTERS EAST?	10.2.2.1
What is the source IP address of the ping as it EXITS EAST?	172.16.1.3
What is the destination IP address of the ping as it EXITS EAST?	172.16.2.3

9) Go back to Realtime mode.

d. Traceroute from PC-A to PC-C. What is the path from PC-A to PC-C?

The path from PC-A to PC-C is 172.16.1.1 > 172.16.12.2 > 172.16.2.3

Reflection

1. Is the data sent through the GRE tunnel considered secured? Why or why not?

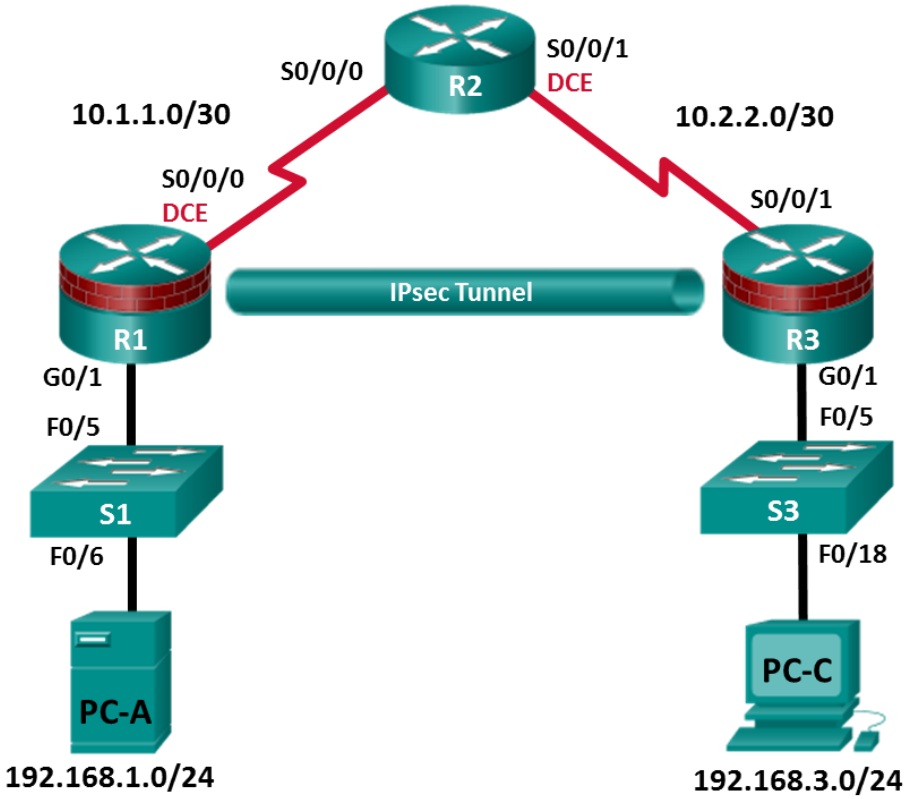
Generic Routing Encapsulation (GRE) is used when IP packets need to be sent from one network to another, without being parsed or treated like IP packets by any intervening routers. Even though GRE provides a stateless and private connection, data sent through the GRE tunnel is not considered secure because it does not use encryption or any other security mechanisms.

2. In this lab topology, would OSPF have worked between the 2 sites without the GRE tunnel? Why or why not?

OSPF would not have worked between the two sites without the GRE tunnel because OSPF was only configured on the tunnel. It was not configured on the ISP router so there is no path between the two sites that would allow for packets to pass through. However, if OSPF were to be configured on the ISP router, the two sites would be able to communicate with each other but security would be compromised.

Lab 6.2 Configuring a Secure Site-to-Site IPSec VPN

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

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure a Site-to-Site VPN Using IPSec

Part 3: Verify Secure Site-to-site VPN Operation

Background / Scenario

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation of VPN technology is remote access to a corporate office from a telecommuter location, such as a small office or home office.

In this lab, you will build and configure a multi-router network, configure a site-to-site IPsec VPN, and then test the VPN. 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 acts at the network layer and protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses and routing.

Step 1: Cable the network as shown in the topology.

Step 2: Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 3: Configure basic settings for each router.

a. Configure the device names.

b. Apply IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces.

Step 4: Configure OSPF routing.

Configure OSPF routing to achieve full connectivity among all hosts in the topology

Step 5: Verify connectivity.

At this point, all hosts must be able to ping each other. Test this to verify; and troubleshoot as necessary if any do not work

Step 6: Save your running configuration.

Part 2: Configure IPsec VPN Settings on R1 and R3.

IPsec is an open framework that allows for the exchange of security protocols as new technologies, and encryption algorithms as they are developed.

There are two central configuration elements in the implementation of an IPsec VPN:

- Implement Internet Key Exchange (IKE) parameters

- Implement IPsec parameters

In Part 2 of this lab, you will configure an IPsec VPN tunnel between R1 and R3 that passes through R2

Step 1: **Enable IKE policies on R1 and R3.**

a. Establish an ISAKMP policy and view the available options.

To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and the hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp policy number** global configuration mode command on R1 for policy 10.

```
R1(config)# crypto isakmp policy 10
```

b. View the various IKE parameters available using Cisco IOS help by typing a question mark (**?**).

```
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

c. Configure the IKE Phase 1 ISAKMP policy on R1 and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

1) Configure an ISAKMP policy with a priority of **10**. Use **pre-shared key** as the authentication type, **aes 256** for the encryption algorithm, **sha** as the hash algorithm, and the Diffie-Hellman group **14** key exchange. Give the policy a lifetime of **3600** seconds (one hour).

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
```

2) Configure the same policy on R3.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash sha
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 14
R3(config-isakmp)# lifetime 3600
```

```
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# end
```

d. Verify the IKE policy with the **show crypto isakmp policy** command.

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
```

Step 2: Configure pre-shared keys.

a. Because pre-shared keys are used as the authentication method in the IKE policy, a key must be configured on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration mode **crypto isakmp key <key-string> address <ip-address>** command is used to enter a pre-shared key.

Use the IP address of the remote peer, which is the remote interface that the peer would use to route traffic to the local router.

Which IP addresses should you use to configure the IKE peers, given the topology diagram and IP addressing table?

The IP addresses that should be used to configure IKE peers are 10.1.1.1 and 10.2.2.1

b. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of **cisco123** on router R1. Production networks should use a complex key. This command points to the remote peer R3 S0/0/1 IP address.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1
```

c. Configure the pre-shared key **cisco123** on router R3. The command for R3 points to the R1 S0/0/0 IP address.

```
R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```

Step 3: Configure the IPsec transform set and lifetime.

a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an IPsec transform set, use the **crypto ipsec transform-set <tag>** command. Use **?** to see which parameters are available.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-null      ESP transform w/o cipher
  esp-seal      ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac  ESP transform using HMAC-SHA auth
```

b. On R1 and R3, create a transform set with tag 50 and use an ESP transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)# exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

What is the function of the IPsec transform set?

> The function of the IPsec transform set defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, and authentication algorithms.

Step 4: Define interesting traffic.

To make use of the IPsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining IPsec traffic is encrypted if the IPsec session is configured correctly. A packet that is denied by one of these access lists is not dropped it is sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which means the default action is to not encrypt traffic. If there is no IPsec security association correctly configured, no traffic is encrypted and traffic is forwarded unencrypted.

In this scenario, from the perspective of R1, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN or vice versa from the perspective of R3. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

a. Configure the IPsec VPN interesting traffic ACL on R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

b. Using a similar technique, configure the IPsec VPN interesting traffic ACL on R3.

What ACL is needed on R3?

> R3(config)**# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**

Step 5: Create and apply a crypto map.

A crypto map associates traffic that matches an access list to a peer and various IKE and IPsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces that it is applied to should be the ones facing the IPsec peer.

To create a crypto map, use **crypto map <name> <sequence-num> <type>** command in global configuration mode to enter crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in ascending numerical order. Enter crypto map configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.

a. Create the crypto map on R1, name it **CMAP**, and use **10** as the sequence number. A message displays after the command is issued.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

b. Use the match **address <access-list>** command to specify which access list defines which traffic to encrypt.

```
R1(config-crypto-map)# match address 101
```

c. To view the list of possible **set** commands that you can do with a crypto map, use the help function.

```
R1(config-crypto-map)# set ?
  identity              Identity restriction.
  ip                    Interface Internet Protocol config commands
  isakmp-profile        Specify isakmp Profile
  nat                   Set NAT translation
  peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings
  reverse-route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in priority order
```

d. Setting a peer IP or hostname is required. Set it to R3's remote VPN endpoint interface using the following command.

```
R1(config-crypto-map)# set peer 10.2.2.1
```

e. Use the **set transform-set <tag>** command to hard code the transform set to be used with this peer..

```
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# exit
```

f. Create a mirrored matching crypto map on R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# exit
```

g. Apply the crypto map to interfaces.

Note: The SAs are not established until the crypto map has been activated by interesting traffic. The router generates a notification that crypto is now on.

Apply the crypto maps to the appropriate interfaces on R1 and R3.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end

R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```

Part 3: Verify the Site-to-Site IPsec VPN Configuration.

In Part 3 of this lab, you will now use show commands to verify the operation of the configures site-to-site VPN connection. This involves verifying IKE and IPSEC settings, as well as verifying that the corresponding security associations (SAs) are actually established between the peer routers.

Step 1: Verify the IPsec configuration on R1 and R3.

a. Previously, you used the **show crypto isakmp policy** command to display the configured ISAKMP policies on the router. The **show crypto ipsec transform-set** command displays the configured IPsec policies in the form of the transform sets.

```
R1# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

R3# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

b. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R1# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/0

R3# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
```

```
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/1
```

Note: The output of these **show** commands does not change if interesting traffic goes across the connection. You test various types of traffic in the next task.

Step 2: **Verify the IPsec VPN Operation.**

a. Display ISAKMP security associations.

The **show crypto isakmp sa** command reveals that no IKE SAs exist yet. When interesting traffic is sent, this command output will change.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

b. Display IPsec security associations.

The **show crypto ipsec sa** command shows the unused SA between R1 and R3.

Note: The number of packets sent across is zero, and there is a lack of any security associations listed toward the bottom of the output. The output for R1 is shown here.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:
```

Why haven't any SAs been negotiated?

> IPsec has not begun to negotiate an SA over which it will encrypt traffic because no interesting traffic has been identified.

Step 3: Generate some uninteresting test traffic and observe the results.

a. Ping from R1 to the R3 S0/0/1 interface IP address 10.2.2.1. These pings should be successful.

b. Issue the show crypto isakmp sa command.

c. Ping from R1 to the R3 G0/1 interface IP address 192.168.3.1. These pings should be successful.

d. Issue the show crypto isakmp sa command again.

Was an SA created for these pings? Explain.

> An SA was not created for these pings. The source address of both pings was 10.1.1.1 (R1). In the first case, the destination address was 10.2.2.1. In the second case, the destination address was 192.168.3.1. The ACL 101 that is associated with the crypto map for R1 defines interesting traffic as IP packets from the 192.168.1.0/24 network to the 192.168.3.0/24 network.

e. Issue the **debug ip ospf events command**. You should see OSPF hello packets passing between R1 and R3.

```
R1# debug ip ospf events
OSPF hello events debugging is on
R1#
*Apr  7 18:04:46.467: OSPF: Send hello to 224.0.0.5 area 0 on GigabitEthernet0/1 from
192.168.1.1
*Apr  7 18:04:50.055: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from
10.1.1.1
*Apr  7 18:04:52.463: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
*Apr  7 18:04:52.463: OSPF: End of hello processing
*Apr  7 18:04:55.675: OSPF: Send hello to 224.0.0.5 area 0 on GigabitEthernet0/1 from
192.168.1.1
*Apr  7 18:04:59.387: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from
10.1.1.1
*Apr  7 18:05:02.431: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
```

```
*Apr  7 18:05:02.431: OSPF: End of hello processing
```

f. Turn off debugging with the **no debug ip ospf events** or **undebug all** command.

g. Re-issue the **show crypto isakmp sa** command.

Was an SA created between R1 and R3? Explain.

An SA was not created between R1 and R3 because it is router-to-router routing protocol traffic. The source and destination of these packets does not initiate the SA and is not encrypted.

Step 4: Generate some interesting test traffic and observe the results.

a. Use an extended ping from R1 to the R3 G0/1 interface IP address **192.168.3.1**. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press **Enter** to accept the defaults, except where a specific response is indicated.

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1
..!!!
Success rate is 100 percent (3/5), round-trip min/avg/max = 92/92/92 ms
```

b. Re-issue the **show crypto isakmp sa** command.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.2.2.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Why was an SA created between R1 and R3 this time?

Yes, an SA was created between R1 and R3. The source was 192.168.1.1 and the destination was 192.168.3.1. This is interesting traffic based on the ACL 101 definition. An SA is established and packets travel through the tunnel as encrypted traffic.

What are the endpoints of the IPsec VPN tunnel?

The endpoints of the IPsec VPN tunnel are 10.1.1.1 and 10.2.2.1

c. Ping from PC-A to PC-C. If the pings were successful, issue the **show crypto ipsec sa** command.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC1DD058(203280472)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:6, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

```
outbound ah sas:

outbound pcp sas:
```

How many packets have been transformed between R1 and R3?

3 packets have been transformed between R1 and R3.

This example used pings to generate interesting traffic. What other types of traffic would result in an SA forming and tunnel establishment?

Other types of traffic that would result in an SA forming and tunnel establishment includes any traffic initiated from R1 with a source address in the 192.168.1.0/24 network and a destination address in the 192.168.3.0/24 network. On R3, interesting traffic is any traffic with a source address in the 192.168.3.0/24 network and a destination address in the 192.168.1.0/24 network. This includes FTP, HTTP, Telnet, and others.

Reflection

1. Would traffic on the Gigabit Ethernet link between PC-A and the R1 G0/0 interface be encrypted by the site-to-site IPsec VPN tunnel? Why or why not?

Traffic on the Gigabit Ethernet link between PC-A and the R1 G0/0 interface **will not be encrypted** by the site-to-site IPsec VPN tunnel. This is because it only encrypts from router R1 to R3. A sniffer could be used to see the traffic from PC-A to the R1 default gateway.

2. Assuming that R2 was an ISP router that was not configured with OSPF routing, how can OSPF routing be achieved between R1 and R3 while still maintaining secure communications between the 2 sites?

Assuming that R2 was an ISP router that was not configured with OSPF routing, it can still be achieved between R1 and R3 while maintaining secure communications between the 2 sites through the IPSec Protocol. To run OSPF over IPSec tunnels, a Layer 3 GRE tunnel is configured between two routers with GRE destination addresses as the inner address of the IPsec tunnel. OSPF is enabled on the Layer 3 GRE tunnel interface, and all of the OSPF control packets undergo GRE encapsulation before entering the IPsec tunnels.