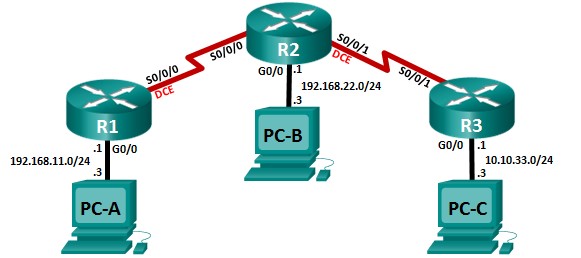
**CCNA: Connecting Networks**

# Skills Assessment – Student Training Exam

## Topology



## Assessment Objectives



**Part 1: Initialize Devices** (2 points, 5 minutes)

**Part 2: Configure Device Basic Settings** (18 points, 20 minutes)

**Part 3: Configure PPP Connections** (17 points, 20 minutes)

**Part 4: Configure NAT** (14 points, 15 minutes)

**Part 5: Monitor the Network** (16 points, 15 minutes)

**Part 6: Configure Frame Relay** (17 points, 20 minutes)

**Part 7: Configure a GRE VPN Tunnel** (16 points, 20 minutes)

## Scenario

In this Skills Assessment (SA) you will create a small network. You must connect the network devices and configure those devices to support various WAN protocols. This will require that you reload the routers before starting your configuration of the next WAN protocol. The assessment has you save your basic device configurations to flash prior to implementing a WAN protocol to allow you to restore these basic configurations after each reload.

The first WAN protocol you will configure is Point-to-Point Protocol (PPP) with CHAP authentication. You will also configure Network Address Translation (NAT), and network monitoring protocols during this phase of the assessment. After your instructor has signed off on this phase, you will reload the routers and configure Frame Relay. After the Frame Relay part is complete, and has been signed off by your instructor, you will reload the routers and configure a GRE VPN tunnel. Network configurations and connectivity will be verified throughout the assessment by using common CLI commands.

## Required Resources

* 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)  3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term.
* Console cable to configure the Cisco IOS devices via the console ports
* Ethernet and Serial cables as shown in the topology

## Part 1: Initialize Devices

**Total points: 2**

**Time: 5 minutes**

**Step 1: Initialize and reload routers.**

Erase the startup configurations and reload the devices.

|  |  |  |
| --- | --- | --- |
| **Task** | **IOS Command** | **Points** |
| Erase the startup-config file on all routers. |  | (1 point) |
| Reload all routers. |  | (1 point) |

**Note**: Before proceeding, have your instructor verify device initializations.

**Instructor Sign-off Part 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_\_ of 2**

## Part 2: Configure Device Basic Settings

**Total points: 18**

**Time: 20 minutes**

**Step 1: Configure PCs.**

Assign static IPv4 address information (IP address, subnet mask, default gateway) to the three PCs in the topology. Refer to the Topology diagram to obtain the IP address information.

|  |  |  |
| --- | --- | --- |
| **Configuration Item or Task** | **Specification** | **Points** |
| Configure static IPv4 address information on PC-A. |  | (1 point) |
| Configure static IPv4 address information on PC-B. |  | (1 point) |
| Configure static IPv4 address information on PC-C. |  | (1 point) |

**Step 2: Configure R1.**

Configuration tasks for R1 include the following:

|  |  |  |
| --- | --- | --- |
| **Configuration Item or Task** | **Specification** | **Points** |
| Disable DNS lookup |  | (1/2 point) |
| Router name | R1 | (1/2 point) |
| Encrypted privileged EXEC password | class | (1/2 point) |
| Console access password | cisco | (1/2 point) |
| Telnet access password | cisco | (1/2 point) |
| Encrypt the plain text passwords |  | (1/2 point) |
| MOTD banner | Unauthorized Access is Prohibited! | (1/2 point) |
| Configure G0/0 | Set the description.  Set the Layer 3 IPv4 address. Use the IP address information listed in the Topology.  Activate the interface. | (1 1/2 point) |

**Step 3: Configure R2.**

Configuration tasks for R2 include the following:

|  |  |  |
| --- | --- | --- |
| **Configuration Item or Task** | **Specification** | **Points** |
| Disable DNS lookup |  | (1/2 point) |
| Router name | R2 | (1/2 point) |
| Encrypted privileged EXEC password | class | (1/2 point) |
| Console access password | cisco | (1/2 point) |
| Telnet access password | cisco | (1/2 point) |
| Encrypt the plain text passwords |  | (1/2 point) |
| MOTD banner | Unauthorized Access is Prohibited! | (1/2 point) |
| Configure G0/0 | Set the description.  Set the Layer 3 IPv4 address. Use the IP address information listed in the Topology.  Activate the interface. | (1 1/2 point) |

**Step 4: Configure R3.**

Configuration tasks for R3 include the following:

|  |  |  |
| --- | --- | --- |
| **Configuration Item or Task** | **Specification** | **Points** |
| Disable DNS lookup |  | (1/2 point) |
| Router name | R3 | (1/2 point) |
| Encrypted privileged EXEC password | class | (1/2 point) |
| Console access password | cisco | (1/2 point) |
| Telnet access password | cisco | (1/2 point) |
| Encrypt the plain text passwords |  | (1/2 point) |
| MOTD banner | Unauthorized Access is Prohibited! | (1/2 point) |
| Configure G0/0 | Set the description.  Set the Layer 3 IPv4 address. Use the IP address information listed in the Topology.  Activate the interface. | (1 1/2 point) |

**Step 5: Save device configurations to Flash.**

Use the **copy running-config BasicConfig** command to save the running configuration to flash on each router. You will need this configuration file later in the assessment to restore the routers back to their basic configuration.

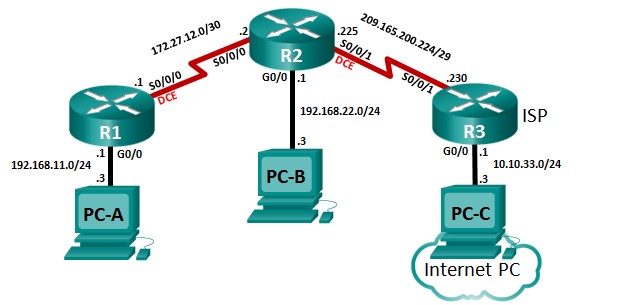
|  |  |  |
| --- | --- | --- |
| **Configuration Item or Task** | **Specification** | **Points** |
| Copy the running-config on R1 to flash. Name the file **BasicConfig**. |  | (1/2 point) |
| Copy the running-config on R2 to flash. Name the file **BasicConfig**. |  | (1/2 point) |
| Copy the running-config on R3 to flash. Name the file **BasicConfig**. |  | (1/2 point) |

**Instructor Sign-off Part 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Points: \_\_\_\_\_\_\_\_\_ of 18**

## Part 3: Configure PPP Connections

**Total points: 17**

**Time: 20 minutes**



### Figure 1: PPP Topology

Use **Figure 1** to obtain the IP information needed for this part of the student assessment.

**Step 1: Configure R1.**

Configuration tasks for R1 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/0. | Int s0/0/0  Description PPP Connection to R2  Ip address 172.27.12.1 255.255.255.252  Encapsulation ppp  Clock rate 128000  No shut | (2 points) |
| Configure CHAP authentication on S0/0/0. | ppp authentication chap  exit | (1 point) |
| Create a local database entry for CHAP authentication. | Username R2 password cisco | (1 point) |
| Set a static default route out S0/0/0. | Ip route 0.0.0.0.0 0.0.0.0.0 s0/0/0 | (1/2 point) |

**Step 2: Configure R2.**

Configuration tasks for R2 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/0. | Description PPP Connection to R!  Ip address 172.27.12.2 255.255.255.252  No shut  Encapsulation ppp | (2 point) |
| Configure CHAP authentication on S0/0/0. | ppp authentication chap | (1 point) |
| Create a local database entry for CHAP authentication. | Username R1 password cisco | (1 point) |
| Configure S0/0/1. | S0/3/1  Description PPP Connection to ISP  Ip address 209.165.200.225 255.255.255.248  Clock rate 128000  No shut  Encapsulation ppp  Exit | (2 points) |
| Set a static default route out S0/0/1. | Ip route 0.0.0.0.0 0.0.0.0.0 s0/3/1 | (1/2 point) |
| Set a static route for R1 LAN traffic out S0/0/0. | Ip route 192.168.11.0 255.255.255.0 s0/3/0 | (1 point) |

**Step 3: Configure R3.**

Configuration tasks for R3 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/1. | Int s0/3/1  Description PPP Connection to R2  Ip address 209.165.200.230 255.255.255.248  No shut  Encapsulation ppp | (2 points) |

**Step 4: Verify network connectivity.**

Verify connectivity using the **ping** command.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **Command** | **To** | **Expected Results** | **Points** |
| PC-A | ping | PC-B | Ping should be successful. | (1/2 point) |
| PC-C | ping | R3 G0/1 | Ping should be successful. | (1/2 point) |
| PC-C | ping | R2 S0/0/1 | Ping should be successful. | (1/2 point) |
| PC-A | ping | PC-C | Ping should **not** be successful. | (1/2 point) |
| PC-B | ping | PC-C | Ping should **not** be successful. | (1/2 point) |
| PC-C | ping | PC-B | Ping should **no**t be successful. | (1/2 point) |

**Note**: It may be necessary to disable the PC firewall for pings to be successful.

**Instructor Sign-off Part 3: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Points: \_\_\_\_\_\_\_\_\_ of 17**

## Part 4: Configure NAT

**Total points: 14**

**Time: 15 minutes**

**Step 1: Configure R2.**

Configuration tasks for R2 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Assign a static NAT to map the inside local IP address for PC-B to a Inside Global address. | Ip nat inside source static 192.168.22.3 **209.165.200.226** | (1 point) |
| Define an access control list to permit the R1 LAN for dynamic NAT. | Access-list 1 permit 192.168.11.0 0.0.0.255 | (1 point) |
| Define the dynamic NAT pool for the R1 LAN. | Ip nat pool R1-LAN **209.165.200.227 209.165.200.227 netmask 255.255.255.248** | (1 point) |
| Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address. | Ip nat inside source list 1 pool R1-LAN overload  [ Ip nat pool R1-LAN **209.165.200.227 209.165.200.227 netmask 255.255.255.248]???** | (1 point) |
| Define an access control list to permit the R2 LAN for dynamic NAT. | Access-list 2 permit 192.168.22.0 0.0.0.255 | (1 point) |
| Define the dynamic NAT pool for the R2 LAN. | Ip nat pool R2-LAN **209.165.200.228 209.165.200.228 netmask 255.255.255.248** | (1 point) |
| Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address. | Ip nat inside source list 2 pool R2-LAN overload | (1 point) |
| Assign the outside NAT interface. | Int s0/3/1  Ip nat outside | (1 point) |
| Assign the inside NAT interface for the R1 LAN. | Int s0/3/0  Ip nat inside | (1 point) |
| Assign the inside NAT interface for the R2 LAN. | Int f0/0  Ip nat inside | (1 point) |

**Step 2: Verify network connectivity.**

Verify connectivity using the **ping** command.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **Command** | **To** | **Expected Results** | **Points** |
| PC-A | ping | PC-C | Ping should be successful. | (1/2 point) |
| PC-C | ping | Inside Global address for PC-B (209.165.200.226). | Ping should be successful. | (1/2 point) |

**Note**: It may be necessary to disable the PC firewall for pings to be successful.

**Step 3: Verify NAT Configuration on R2.**

Enter the appropriate CLI command needed to display the following:

|  |  |  |
| --- | --- | --- |
| **Command Description** | **Student Input (command)** | **Points** |
| Display configured access lists. | Show access-lists | (1 point) |
| Display the current active NAT translations. | Show ip nat translations | (1 point) |
| Display detailed information about NAT including interface, access list, and pool assignments. | Show ip nat statistics | (1 point) |

**Instructor Sign-off Part 4: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Points: \_\_\_\_\_\_\_\_\_ of 14**

## Part 5: Monitor the Network

**Total points: 16**

**Time: 15 minutes**

**Step 1: Configure NTP.**

Configuration tasks include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Set the clock on R2 to a date and time specified for NTP testing. | R# clock set 9:00:00 3 April 2017 | (1 point) |
| Configure R2 as the NTP Master. | Ntp master 5 | (1 point) |
| Configure R1 so that it uses R2 as its NTP Server. | R1#conf t  Ntp server 172.27.12.2 | (1 point) |

**Step 2: Configure Syslog messaging.**

Configuration tasks include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Enable the timestamp service on R1 and R2 for system logging purposes. | Service timestamp log datatime msec | (1 points) |
| Enable logging of messages on R1 and R2. | Logging host 192.168.11.3 | (1 points) |
| Change message trapping level on R1 and R2. | Logging trap debugging | (1 points) |

**Step 3: Configure SNMP on R1.**

Configuration tasks include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Create a standard access list to permit the SNMP management station (PC-A) to retrieve SNMP information from R1. | Ip access-list standart SNMP-ACCESS  Permit 192.168.11.3 | (1 points) |
| Enable SNMP community access to the SNMP-ACCESS access list. | Snmp-server community SA-LAB to ro?? SNMP-ACCESS | (1 points) |
| Set the SNMP notification host. | Snmp-server host 192.168.11.3 version 2c SA-LAB | (1 points) |
| Enable all SNMP traps. | Snmp-server enable traps | (1 points) |

**Step 4: Collect NetFlow data on R2.**

Configuration tasks include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure NetFlow data capture on both serial interfaces. Capture ingress and egress data packets. | Int s0/3/0  Ip flow ingress  Ip flow egress  Int s0/3/1  Ip flow ingress  Ip flow egress  exit | (1 points) |
| Configure NetFlow data export. | Ip flow-export destination 192.168.22.3 9996 | (1 points) |
| Configure the NetFlow export version. | Ip flow-export version **9** | (1 points) |

|  |  |  |
| --- | --- | --- |
| **Command Description** | **Student Input (command)** | **Points** |
| Display the date and time. | R# show clock | (1/2 point) |
| Display the contents of logging buffers. | Show logging | (1 point) |
| Display information about the SNMP communities. | Show snmp-community? | (1/2 point) |
| Display the protocol using the highest volume of traffic. | Show ip cache flow | (1 point) |

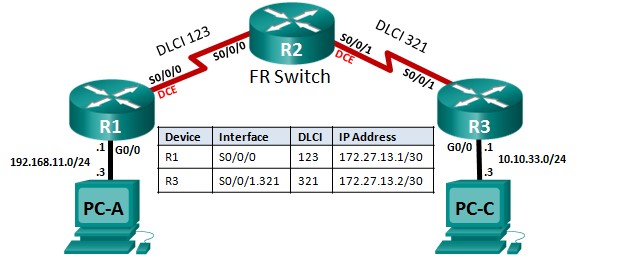
**Instructor Sign-off Part 5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Points: \_\_\_\_\_\_\_\_\_ of 16**

## Part 6: Configure Frame Relay

**NOTE: DO NOT PROCEED WITH THE ASSESSMENT UNTIL YOUR INSTRUCTOR HAS SIGNED OFF ON THE PREVIOUS PARTS.**

**Total points: 17**

**Time: 20 minutes**



### Figure 2: Frame Relay Topology

Use **Figure 2** to obtain the IP information needed for this part of the student assessment.

**Step 1: Reload routers and restore the BasicConfig to memory.**

1. Erase the startup configurations and reload the devices.
2. For each router, issue the **copy flash:BasicConfig running-config** command to reload the basic configuration that you saved at the end of Part 2.
3. Issue the **no shutdown** command for the G0/0 interface on R1 and R3.

**Step 2: Configure R2 as a Frame Relay Switch.**

Copy and paste the following configuration lines into R2. This will configure R2 as a Frame Relay switch and allow you to complete Part 6.

**frame-relay switching int s0/0/0 encapsulation frame-relay frame-relay intf-type dce frame-relay route 123 interface s0/0/1 321 frame-relay lmi-type ansi no shutdown int s0/0/1 clock rate 128000 encapsulation frame-relay ietf frame-relay intf-type dce frame-relay route 321 interface s0/0/0 123 no shutdown**

**Step 3: Configure R1.**

Configure Frame Relay on S0/0/0 on R1. Configuration tasks for R1 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/0. | Int s0/3/0  Desc Frame-Relay Connection tp R3  Ip address 172.29.13.1 255.255.255.252  Encapsulation frame-relay  Clock rate 128000  No shut | (2 points) |
| Disable Inverse ARP on S0/0/0. | no frame-relay inverse-arp | (1/2 point) |
| Map the IP local address to the DLCI. | Frame-relay map ip 172.27.13.1 123 | (1 point) |
| Map the remote IP address to the DLCI. Allow for multicast or broadcast traffic. | Frame-relay map ip 172.27.13.2 123 broadcast | (1 point) |
| Change the LMI type to the ANSI standard. | Frame-relay lmi-type ansi | (1 point) |
| Activate the interface. | No shut | (1/2 point) |
| Create a default route to the IP address on the other side of the Frame Relay link. | Exit  Ip route 0.0.0.0 0.0.0.0 172.27.13.2 | (1/2 point) |

**Step 4: Configure R3.**

Configure Frame Relay on a subinterface of S0/0/1 on R3. Configuration tasks for R3 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/1. | Int s0/3/1  Desc Frame Relay Connection to R1  encapsulation frame-relay ietf  no shut | (1 point) |
| Create a point-to-point subinterface on S0/0/1. | Int s0/3/1 321 point-to-point  Desc Frame Relay Connection to R1 | (1 point) |
| Set the Layer 3 IPv4 address on the subinterface. | Ip addess 172.27.13.2 255.255.255.252 | (1 point) |
| Disable Inverse ARP on the subinterface. | No frame-relay inverse-arp | (1/2 point) |
| Map the subinterface to the DLCI. | Frame-relay interface-dlci 321  exit | (1 point) |
| Create a default route to the IP address on the other side of the Frame Relay link. | Ip route 0.0.0.0.0 0.0.0.0 172.27.13.1 | (1/2 point) |

**Step 5: Verify network connectivity.**

Verify connectivity using the **ping** command.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **Command** | **To** | **Expected Results** | **Points** |
| PC-A | ping | Default gateway | Ping should be successful. | (1/2 point) |
| PC-C | ping | Default gateway | Ping should be successful. | (1/2 point) |
| PC-A | ping | 172.27.13.2 | Ping should be successful. | (1/2 point) |
| PC-C | ping | 172.27.13.1 | Ping should be successful. | (1/2 point) |
| PC-A | ping | PC-C | Ping should be successful. | (1/2 point) |

**Note**: It may be necessary to disable the PC firewall for pings to be successful.

**Step 6: Verify Frame Relay configuration.**

Enter the appropriate CLI command needed to display the following:

|  |  |  |
| --- | --- | --- |
| **Command Description** | **Student Input (command)** | **Points** |
| Display Frame Relay LMI statistics. | Show frame-relay lmi | (1 point) |
| Display the input and output packet count totals on a Frame Relay permanent virtual circuit (PVC). | Show frame-relay pvc | (1 point) |
| Display the Frame Relay maps between DLCIs and IP addresses. | Show frame-relay map | (1 point) |

**Instructor Sign-off Part 6: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

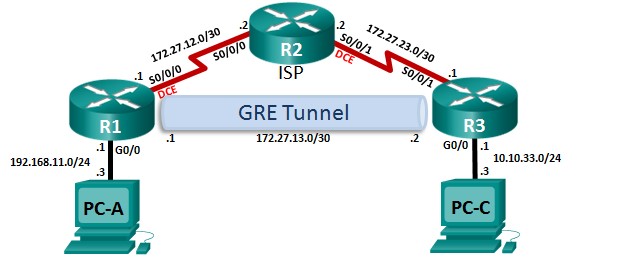
**Points: \_\_\_\_\_\_\_\_\_ of 17**

## Part 7: Configure a GRE VPN Tunnel

**NOTE: DO NOT PROCEED WITH THE ASSESSMENT UNTIL YOUR INSTRUCTOR HAS SIGNED OFF ON THE PREVIOUS PART.**

**Total points: 16**

**Time: 20 minutes**



### Figure 3: GRE VPN Topology

Use **Figure 3** to obtain the IP information needed for this part of the student assessment.

**Step 1: Reload routers and restore the BasicConfig to memory.**

1. Erase the startup configurations and reload the devices.
2. For each router, issue the **copy flash:BasicConfig running-config** command to reload the basic configuration that you saved at the end of Part 2.
3. Issue the **no shutdown** command for the G0/0 interface on R1 and R3.

**Step 2: Configure Serial Interfaces.**

1. Configuration tasks for R1 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/0. | S0/3/0  Desc HDLC Connection to ISP  Ip address 172.27.12.1 255.255.255.252  Encapsulation hdlc  Clock rate 128000  No shut | (1 point) |

1. Configuration tasks for R2 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/0. | S0/3/0  Desc HDLC Connection to R1  Ip address 172.27.12.2 255.255.255.252  Encapsulation hdlc  No shut | (1 point) |
| Configure S0/0/1. | S0/3/1  Desc HDLC Connection to ISP  Ip address 172.27.23.2 255.255.255.252  Encapsulation hdlc  Clock rate 128000  No shut | (1 point) |

1. Configuration tasks for R3 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Configure S0/0/1. | S0/3/1  Desc HDLC Connection to ISP  Ip address 172.27.23.1 255.255.255.252  Encapsulation hdlc  No shut | (1 point) |

**Step 3: Configure the GRE VPN tunnel and EIGRP on R1.**

Configuration tasks for R1 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Create a GRE tunnel interface. | Int tunnel 0  Desc GRE VPN Tunnel to R3  Ip address 172.27.23.1 255.255.255.252 | (2 points) |
| Use S0/0/0 as the tunnel source. | Tunnel source s0/3/0 | (1/2 point) |
| Set the tunnel destination with the IP address of the R3 S0/0/1 interface. | Tunnel destination 172.27.23.1  exit | (1/2 point) |
| Create a default route out S0/0/0. | Ip route 0.0.0.0 0.0.0.0 s0/3/0 | (1/2 point) |
| Configure EIGRP on R1 | Router eigrp 1 | (1/2 point) |
| Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive. | Do show ip route connected  Network 172.27.13.0 0.0.0.3  Network 192.168.11.0 0.0.0.255  Passive-interface f0/0 | (1/2 point) |

**Step 4: Configure the GRE VPN tunnel and EIGRP on R3.**

Configuration tasks for R3 include the following:

|  |  |  |
| --- | --- | --- |
| **Task** | **Specification** | **Points** |
| Create a GRE tunnel interface. | Int tunnel 0  Desc GRE VPN Tunnel to R1  Ip address 172.27.13.2 255.255.255.252 | (2 points) |
| Use S0/0/1 as the tunnel source. | Tunnel source s0/3/1 | (1/2 point) |
| Set the tunnel destination with the IP address of the R1 S0/0/0 interface. | Tunnel destination 172.27.12.1  exit | (1/2 point) |
| Create a default route out S0/0/1. | Ip route 0.0.0.0 0.0.0.0 s0/3/1 | (1/2 point) |
| Configure EIGRP on R3 | Router eigrp 1  \*Do show ip route connected\* | (1/2 point) |
| Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive. | Network 10.10.33.0 0.0.0.255  Network 172.27.13.0 0.0.0.3  Passive-interface f0/0 | (1/2 point) |

**Step 5: Verify network connectivity.**

Verify connectivity using the following commands.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **Command** | **To** | **Expected Results** | **Points** |
| PC-A | ping | Default gateway | Ping should be successful. | (1/2 point) |
| PC-C | ping | Default gateway | Ping should be successful. | (1/2 point) |
| PC-A | ping | PC-C | Ping should be successful. | (1/2 point) |
| R1 | traceroute | 172.27.23.1 | R2 should show up in the traceroute. | (1/2 point) |
| R1 | traceroute | 172.27.13.2 | R2 should be absent from traceroute. | (1/2 point) |

**Note**: It may be necessary to disable the PC firewall for pings to be successful.

**Step 6: Verify GRE VPN configuration.**

Enter the appropriate CLI command needed to display the following:

|  |  |  |
| --- | --- | --- |
| **Command Description** | **Student Input (command)** | **Points** |
| Display detail information about the GRE tunnel interface. | Show ip route | (1/2 point) |

**Instructor Sign-off Part 7: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 16**

## Part 8: Cleanup

**NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.**

Before turning off power to the routers:

* Remove the NVRAM configuration files (if saved) from all devices.
* Remove the **BasicConfig** file from flash using the **delete flash:BasicConfig** command.

### Router Interface Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Router Interface Summary** | | | | |
| **Router Model** | **Ethernet Interface #1** | **Ethernet Interface #2** | **Serial Interface #1** | **Serial Interface #2** |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |