Ütemterv

Számítógép hálózat üzemeltetési alapismeretek II.

Tárgy kódja: GEIAL30HB
Szak: mérnök informatikus alapszak, villamosmérnök alapszak.
Típusa: szakirányban választható
Oktató, előadó: dr. Kovács Szilveszter
Tárgyfelelős: dr. Kovács Szilveszter
Félév: 2019/2020 ősz

Hét	Elmélet	Gyakorlat
1.	Bevezetés. LAN redundancia.	Labor ismertetés.
2.	Link Aggregáció. Vezeték nélküli LAN	Packet Tracer szimulacios gyakorlatok
3.	Egyterületű OSPF.	Packet Tracer szimulacios gyakorlatok
4.	Többterületű OSPF.	Packet Tracer szimulacios gyakorlatok
5.	EIGRP konfiguráció és hibaelhárítás.	Packet Tracer szimulacios gyakorlatok
6.	Cisco IOS image és licenszálás.	Packet Tracer szimulacios gyakorlatok
7.	Évközi zárthelyi dolgozat.	Évközi gyakorlati feladat.
8.	Hierarchikus hálózattervezés.	Packet Tracer szimulacios gyakorlatok
9.	WAN kapcsolódás. Pont-pont kapcsolatok.	Packet Tracer szimulacios gyakorlatok
10.	Frame Relay konfiguráció.	Packet Tracer szimulacios gyakorlatok
11.	IPv4 Network Address Translation.	Packet Tracer szimulacios gyakorlatok
12.	Biztonságos távoli telephelyek kapcsolatok kialakítása.	Packet Tracer szimulacios gyakorlatok
13.	A hálózat monitorozása és hibaelhárítása.	Packet Tracer szimulacios gyakorlatok
14.	Évközi zárthelyi dolgozat.	Évközi gyakorlati feladat

Kötelező irodalom

- Kovács Szilveszter honlapján található előadásjegyzet (www.iit.uni-miskolc.hu/~szkovacs)

Ajánlott irodalom

- Tanenbaum, A.S.: Számítógép-hálózatok, Panem, 2003, ISBN 963 545 384 1

- Cisco Certified Networking Associate (CCNA) Routing and Switching, “Scaling Networks” és “Connecting Networks” tananyaga (angol nyelvű).

A tárgy lezárásának módja:

- aláírás, gyakorlati jegy

Évközi számonkérés:

- témaköröket záró rövid teszt feladatok
- két évközi zárthelyi dolgozat, amely a nagyobb tananyagegységek zárásaként íródik.

Az aláírás megszerzésének feltételei:

- Az ME SzMSz III. kötet 38§ (6) pontja alapján, ha a hallgató nem igazolt hiányzása a gyakorlatokon eléri a gyakorlatok darabszámának 50%-át, a tantárgy aláírása nem szerezhető meg.
- Az aláírás megszerzésének további feltétele a témaköröket záró rövid teszt és gyakorlati feladatok sikeres teljesítése.

Az gyakorlati jegy megszerzésének feltételei:

- Az aláírás megszerzése és a zárthelyi dolgozatok legalább elégséges szintű megírása.

Pótlási lehetőségek:

A gyakorlatok, egyéni feladatok és a zárhelyi dolgozatok egyszer pótolhatók, melyek egyenkénti (vagy összevont) pótlásra az ME SzMSz III. kötet 38§ (5) pontja alapján legkésőbb a szorgalmi időszak utolsó hetében kerülhet sor. A feladatok pótvédése határidő mulasztással jár, ezért különeljárási díjat kell fizetni.

Általános rendelkezések:

Az ME SzMSz III. kötet 96§ alapján a tárgyakhoz kapcsolódó valamennyi számonkérési alkalomnál a nem engedélyezett segédeszközök használata (puskázás) vagy más munkájának sajátként történő feltüntetése (plagizálás) fegyelmi vétségnek minősül, mely tanulmányi szankciókat vagy fegyelmi eljárást von maga után.

Tanulmányi szankció az évközi számonkéréseknél a számonkérés sikertelen minősítése. A számonkérés ilyen esetekben nem pótolható.

Tanulmányi szankció a vizsgaidőszakban a vizsga elégtelen minősítése, és hogy ismételt vizsgát a hallgató a tanszék által kijelölt időpontban, kijelölt vizsgabizottság előtt, szóbeli vizsga formájában tehet.

A puskázás és/vagy plagizálás tényét a tanszék a hallgató tanulmányi ideje alatt nyilvántartja, és ismételt előfordulás esetén a ME SzMSz III. kötet 96§ által előírt fegyelmi eljárást kezdeményez.

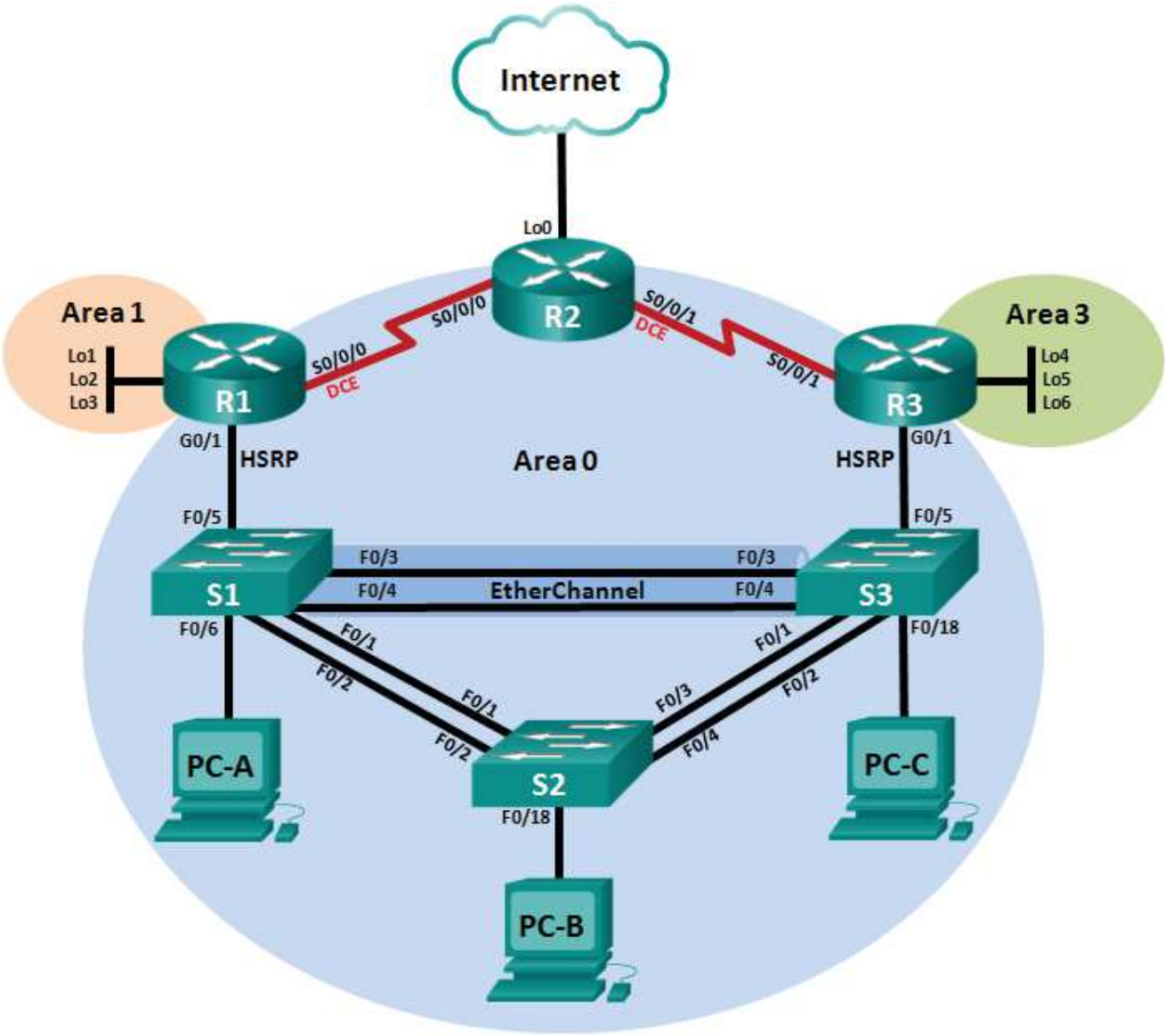
Miskolc, 2019. szeptember.

Dr. Kovács Szilveszter

CCNA: Scaling Networks

Skills Assessment (OSPF) – Student Training Exam

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.27.0.1	255.255.255.0	N/A
	S0/0/0	172.27.123.1	255.255.255.252	N/A
	Lo1	172.27.1.1	255.255.255.0	N/A
	Lo2	172.27.2.1	255.255.255.0	N/A
	Lo3	172.27.3.1	255.255.255.0	N/A
R2	S0/0/0	172.27.123.2	255.255.255.252	N/A
	S0/0/1	172.27.123.5	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.248	N/A
R3	G0/1	172.27.0.3	255.255.255.0	N/A
	S0/0/1	172.27.123.6	255.255.255.252	N/A
	Lo4	172.27.4.1	255.255.255.0	N/A
	Lo5	172.27.5.1	255.255.255.0	N/A
	Lo6	172.27.6.1	255.255.255.0	N/A
S1	VLAN 1	172.27.0.11	255.255.255.0	172.27.0.2
S2	VLAN 1	172.27.0.12	255.255.255.0	172.27.0.2
S3	VLAN 1	172.27.0.13	255.255.255.0	172.27.0.2
PC-A	NIC	172.27.0.21	255.255.255.0	172.27.0.2
PC-B	NIC	172.27.0.22	255.255.255.0	172.27.0.2
PC-C	NIC	172.27.0.23	255.255.255.0	172.27.0.2

Assessment Objectives

Part 1: Initialize Devices (10 points, 5 minutes)

Part 2: Configure Device Basic Settings (45 points, 30 minutes)

Part 3: Configure LAN Redundancy and Link Aggregation (28 points, 25 minutes)

Part 4: Configure OSPFv2 Dynamic Routing Protocol (51 points, 30 minutes)

Part 5: Verify Network Connectivity and HSRP Configuration (10 points, 15 minutes)

Part 6: Display IOS Image and License Information (6 points, 5 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 IPv4 connectivity, LAN redundancy, and link aggregation. You will then configure OSPFv2 and HSRP on the network and verify connectivity. Finally, you will demonstrate your knowledge of IOS images and licensing.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 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 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: 10

Time: 5 minutes

Step 1: Initialize and reload the routers and switches.

Erase the startup configurations and reload the devices.

Before proceeding, have your instructor verify device initializations.

Task	IOS Command	Points
Erase the startup-config file on all routers.		(2 points)
Reload all routers.		(2 points)
Erase the startup-config file on all switches and remove the old VLAN database.		(2 points)
Reload all switches.		(2 points)
Verify VLAN database is absent from flash on all switches.		(2 points)

Instructor Sign-off Part 1: _____

Points: _____ of 10

Part 2: Configure Device Basic Settings

Total points: 45

Time: 30 minutes

Step 1: 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)
Interface G0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Set a clocking rate of 128000. Activate Interface	(1 points)
Interface Loopback 1 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 2 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 3 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)

Step 2: 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)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Set a clocking rate of 128000. Activate Interface	(1 point)
Interface Loopback 0 (Simulated Internet connection)	Set the description. Set the Layer 3 IPv4 address to 209.165.200.225/29.	(1 point)
Default route	Configure a default route out Lo0.	(1/2 point)

Step 3: 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)
Interface G0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface Loopback 4 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 5 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 6 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)

Step 4: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S1	(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)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S2 and S3.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Step 5: Configure S2.

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S2	(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 clear text passwords.		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S1 and S3.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Step 6: Configure S3

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S3	(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)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S1 and S2.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Step 7: Configure IPv4 addresses on PCs.

Configuration Item or Task	Specification	Points
Configure static IPv4 address information on PC-A	Refer to Addressing Table for IPv4 address information.	(1/2 point)
Configure static IPv4 address information on PC-B	Refer to Addressing Table for IPv4 address information.	(1/2 point)
Configure static IPv4 address information on PC-C	Refer to Addressing Table for IPv4 address information.	(1/2 point)

Instructor Sign-off Part 2: _____

Points: _____ of 45

Part 3: Configure LAN Redundancy and Link Aggregation

Total points: 28

Time: 25 minutes

Step 1: Configure Spanning Tree on S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure as primary root bridge for VLAN 1.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-A.		(2 points)

Step 2: Configure Spanning Tree on S2.

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-B.		(2 points)

Step 3: Configure Spanning Tree on S3.

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure as secondary root bridge for VLAN 1.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-C.		(2 points)

Step 4: Configure HSRP on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
Configure the HSRP virtual IP address on interface G0/1.	Group: 1 Virtual IP address: 172.27.0.2	(2 points)
Make this the primary HSRP router.		(2 points)
Configure so this router becomes the primary HSRP router on a reboot.		(2 points)

Step 5: Configure HSRP on R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification	Points
Configure the HSRP virtual IP address on interface G0/1.	Group: 1 Virtual IP address: 172.27.0.2	(2 points)

Step 6: Configure an LACP EtherChannel between S1 and S3.

Configuration tasks include the following:

Configuration Item or Task	Specification	Points
On S1, configure an LACP EtherChannel on interfaces connected to S3.	Use group 1 and enable LACP unconditionally.	(2 points)
On S3, configure an LACP EtherChannel on interfaces connected to S1.	Use group 1 and enable LACP only if a LACP device is detected.	(2 points)

Instructor Sign-off Part 3: _____

Points: _____ of 28

Part 4: Configure OSPFv2 Dynamic Routing Protocol

Total points: 51

Time: 30 minutes

Step 1: Configure OSPFv2 on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	1.1.1.1	(1 point)
Advertise directly connected networks.	Use classless network addresses. Assign S0/0/0 and G0/1 interfaces to Area 0. Assign Loopback interfaces to Area 1.	(2 points)
Set all LAN interfaces as passive.		(2 points)
Configure an inter-area summary route for the networks in area 1.		(2 points)
Change the default cost reference bandwidth to support Gigabit interface calculations.	1000	(2 points)
Set the bandwidth on S0/0/0.	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0.	Cost: 7500	(1 point)
Create an OSPF MD5 key on S0/0/0.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication to S0/0/0.		(2 points)

Step 2: Configure OSPFv2 on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	2.2.2.2	(1 point)
Advertise directly connected networks.	Use classless network addresses. All connected networks should be assigned to Area 0 except the Lo0 network.	(2 points)
Propagate the default route to all other OSPF routers.		(2 points)
Change the default cost reference bandwidth to allow for Gigabit interfaces.	1000	(2 points)
Set the bandwidth on all serial interfaces.	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0.	Cost: 7500	(1 point)
Create an OSPF MD5 key on the serial interfaces.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication on the serial interfaces.		(2 points)

Step 3: Configure OSPFv2 on R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	3.3.3.3	(1 point)
Advertise directly connected networks.	Use classless network addresses Assign S0/0/1 and G0/1 interfaces to Area 0 Assign Loopback interfaces to Area 3	(2 points)
Set all LAN interfaces as passive.		(2 points)
Configure an inter-area summary route for the networks in area 3.		(2 points)
Change the default cost reference bandwidth to support Gigabit interface calculations.	1000	(2 points)
Set the serial interface bandwidth.	128 Kb/s	(1 point)
Create an OSPF MD5 key on S0/0/1.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication to S0/0/1.		(2 points)

Step 4: Verify network connectivity.

Verify that OSPF is functioning as expected. Enter the appropriate CLI command to discover the following information:

Question	Response	Points
What command will display all connected OSPFv2 routers?		(1 point)
What command displays a summary list of OSPF interfaces that includes a column for the cost of each interface?		(1 point)
What command displays the OSPF Process ID, Router ID, Address summarizations, Routing Networks, and Passive Interfaces configured on a router?		(1 point)
What command displays only OSPF routes?		(1 point)
What command displays detailed information about the OSPF interfaces, including the authentication method?		(1 point)
What command displays the OSPF section of the running-configuration?		(1 point)

Instructor Sign-off Part 4: _____

Points: _____ of 51

Part 5: Verify Network Connectivity and HSRP Configuration

Total points: 10

Time: 15 minutes

Use the listed command to verify that network is working as expected.

Step 1: Verify end-to-end connectivity.

Take corrective action if results are other than expected.

From	Command	To	Expected Results	Points
PC-A	ping	PC-C	Ping should be successful.	(1 point)
PC-B	ping	PC-A	Ping should be successful.	(1 point)
PC-B	ping	PC-C	Ping should be successful.	(1 point)
PC-B	ping	Default Gateway	Ping should be successful.	(1 point)
PC-B	ping	209.165.200.225	Ping should be successful.	(1 point)
PC-B	tracert	209.165.200.225	Trace should route through R1.	(1 point)

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

Step 2: Verify HSRP is working as expected.

Issue the **shutdown** command on R1 G0/1, and then re-issue the following commands to verify that HSRP is working as expected:

From	Command	To	Expected Results	Points
PC-B	ping	172.27.0.1	Ping should **not** be successful.	(1 point)
PC-B	ping	Default Gateway	Ping should be successful.	(1 point)
PC-B	ping	209.165.200.225	Ping should be successful.	(1 point)
PC-B	tracert	209.165.200.225	Trace should route through R3.	(1 point)

Note: Wait a few seconds before testing after shutting down the interface on R1.

Instructor Sign-off Part 5: _____

Points: _____ of 10

Part 6: Display IOS Image and License Information

Total points: 6

Time: 5 minutes

Enter the appropriate CLI command to discover the following information:

Question	Response	Points
What command displays the IOS image that is currently being used by the network device?		(1 point)
What command displays the size of an IOS image loaded on a network device?		(1 point)
What command displays a summary list of the Technology Package licenses on an ISR-G2 device that includes the current the state of each of those licenses?		(1 point)
What command displays the amount of space available to install an additional IOS image to a network device?		(1 point)
What command displays a list of all the licenses on an ISR-G2 device?		(1 point)
What command would you use to accept the end user license agreement?		(1 point)

Instructor Sign-off Part 6: _____

Points: _____ of 6

Part 7: 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.

Disconnect and neatly put away all cables that were used in the SA exam.

Router Interface Summary Table

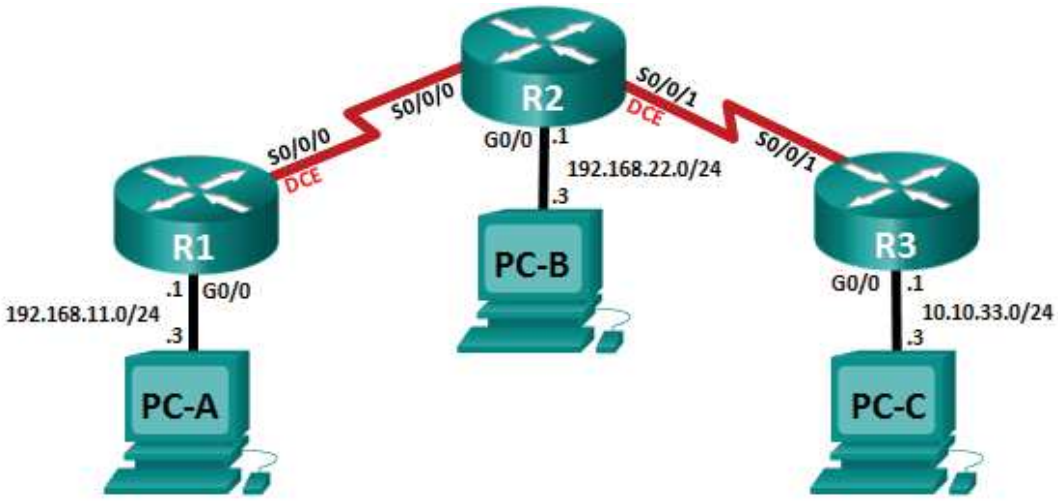
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)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

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

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

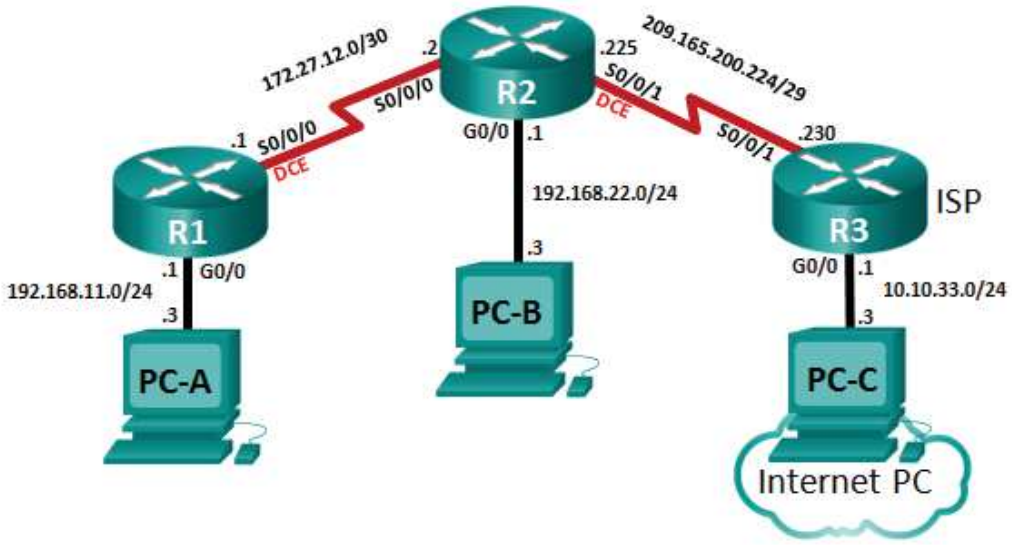


Figure 1: PPP Topology

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.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set encapsulation to **PPP**. Set the clocking rate to **128000**. Activate the interface.	(2 points)
Configure CHAP authentication on S0/0/0.		(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.		(1/2 point)

Step 2: Configure R2.

Configuration tasks for R2 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Activate the interface.	(2 point)
Configure CHAP authentication on S0/0/0.		(1 point)
Create a local database entry for CHAP authentication.	Username: **R1** Password: **cisco**	(1 point)
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Set the clocking rate to **128000**. Activate the interface.	(2 points)
Set a static default route out S0/0/1.		(1/2 point)
Set a static route for R1 LAN traffic out S0/0/0.		(1 point)

Step 3: Configure R3.

Configuration tasks for R3 include the following:

Task	Specification	Points
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Activate the interface.	(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.	Inside Global: **209.165.200.226**	(1 point)
Define an access control list to permit the R1 LAN for dynamic NAT.	Access List: **1**	(1 point)
Define the dynamic NAT pool for the R1 LAN.	Pool: **R1-LAN** Inside Global: **209.165.200.227**	(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.	Inside source: **Access list 1** Outside pool: **R1-LAN**	(1 point)
Define an access control list to permit the R2 LAN for dynamic NAT.	Access List: **2**	(1 point)
Define the dynamic NAT pool for the R2 LAN.	Pool: **R2-LAN** Inside Global: **209.165.200.228**	(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.	Inside source: **Access list 2** Outside pool: **R2-LAN**	(1 point)
Assign the outside NAT interface.		(1 point)
Assign the inside NAT interface for the R1 LAN.		(1 point)
Assign the inside NAT interface for the R2 LAN.		(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.		(1 point)
Display the current active NAT translations.		(1 point)
Display detailed information about NAT including interface, access list, and pool assignments.		(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.	Date: **August 25, 2013** Time: **9 am**	(1 point)
Configure R2 as the NTP Master.	Stratum Number: **5**	(1 point)
Configure R1 so that it uses R2 as its NTP Server.		(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.	Include milliseconds in the timestamp.	(1 points)
Enable logging of messages on R1 and R2.	Syslog server: **192.168.11.3**	(1 points)
Change message trapping level on R1 and R2.	Level: **debugging** (severity 7)	(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.	Access List: **SNMP-ACCESS**	(1 points)
Enable SNMP community access to the SNMP-ACCESS access list.	Community: **SA-LAB** Access level: **Read-only**	(1 points)
Set the SNMP notification host.	Host: **192.168.11.3** Version: **2c** Community: **SA-LAB**	(1 points)
Enable all SNMP 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.		(1 points)
Configure NetFlow data export.	Destination: **PC-B IP address** UDP Port: **9996**	(1 points)
Configure the NetFlow export version.	Version: **9**	(1 points)

Step 5: Verify monitoring configurations.

Enter the appropriate CLI command needed to display the following:

Command Description	Student Input (command)	Points
Display the date and time.		(1/2 point)
Display the contents of logging buffers.		(1 point)
Display information about the SNMP communities.		(1/2 point)
Display the protocol using the highest volume of traffic.		(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

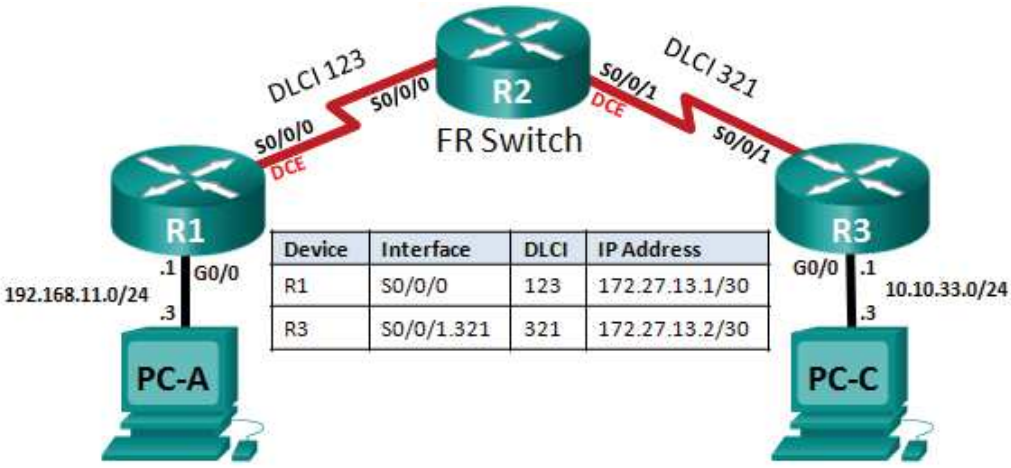


Figure 2: Frame Relay Topology

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.

a. Erase the startup configurations and reload the devices.

b. 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.

c. 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.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 2 at the top of Part 6 for IP address information. Set encapsulation to **frame-relay** Set the clocking rate to 128000	(2 points)
Disable Inverse ARP on S0/0/0.		(1/2 point)
Map the IP local address to the DLCI.	Refer to Figure 2 for DLCI information.	(1 point)
Map the remote IP address to the DLCI. Allow for multicast or broadcast traffic.	Refer to Figure 2 for IP address and DLCI information.	(1 point)
Change the LMI type to the ANSI standard.		(1 point)
Activate the interface.		(1/2 point)
Create a default route to the IP address on the other side of the Frame Relay link.	Refer to Figure 2 for the IP address.	(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.	Configure Frame Relay Encapsulation. Set encapsulation to **frame-relay** (use the IETF standard). Activate the interface.	(1 point)
Create a point-to-point subinterface on S0/0/1.	Subinterface #: **321** Set the description.	(1 point)
Set the Layer 3 IPv4 address on the subinterface.	Refer to Figure 2 at the top of Part 6 for IP address information.	(1 point)
Disable Inverse ARP on the subinterface.		(1/2 point)
Map the subinterface to the DLCI.	Refer to Figure 2 for DLCI information.	(1 point)
Create a default route to the IP address on the other side of the Frame Relay link.	Refer to Figure 2 for IP address.	(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.		(1 point)
Display the input and output packet count totals on a Frame Relay permanent virtual circuit (PVC).		(1 point)
Display the Frame Relay maps between DLCIs and IP addresses.		(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

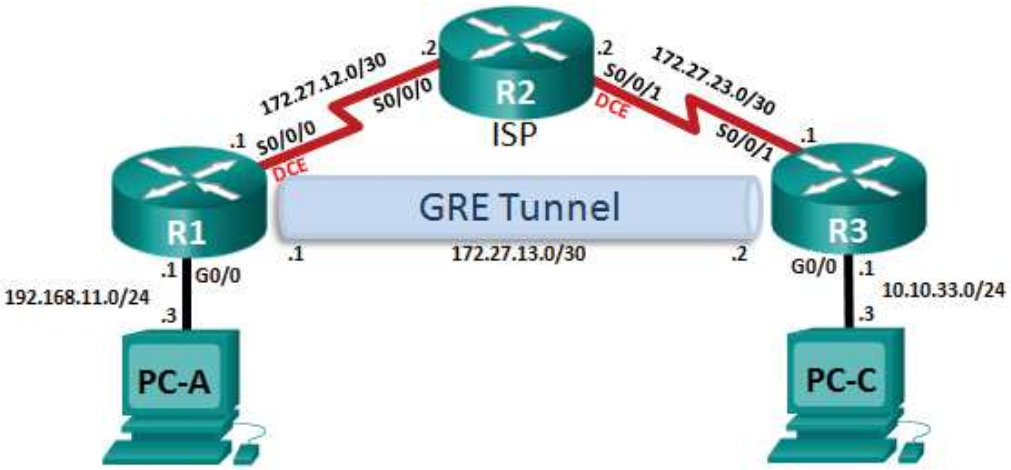


Figure 3: GRE VPN Topology

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.

a. Erase the startup configurations and reload the devices.

b. 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.

c. Issue the **no shutdown** command for the G0/0 interface on R1 and R3.

Step 2: Configure Serial Interfaces.

a. Configuration tasks for R1 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Set the clocking rate to **128000**. Activate the interface.	(1 point)

b. Configuration tasks for R2 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Activate the interface.	(1 point)
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Set the clocking rate to **128000.** Activate the interface.	(1 point)

c. Configuration tasks for R3 include the following:

Task	Specification	Points
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Activate the interface.	(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.	Interface: **tunnel 0** Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information.	(2 points)
Use S0/0/0 as the tunnel source.		(1/2 point)
Set the tunnel destination with the IP address of the R3 S0/0/1 interface.	Refer to Figure 3 for IP address information.	(1/2 point)
Create a default route out S0/0/0.		(1/2 point)
Configure EIGRP on R1	Autonomous System (AS) number: **1**	(1/2 point)
Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.	Refer to the GRE VPN topology.	(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.	Interface: **tunnel 0** Set the description. Set the Layer 3 IPv4 address. Use the IP address information listed in Figure 3 at the top of Part 7.	(2 points)
Use S0/0/1 as the tunnel source.		(1/2 point)
Set the tunnel destination with the IP address of the R1 S0/0/0 interface.	Refer to Figure 3 at the top of Part 7 for IP address information.	(1/2 point)
Create a default route out S0/0/1.		(1/2 point)
Configure EIGRP on R3	Autonomous System (AS) number: **1**	(1/2 point)
Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.	Refer to the GRE VPN topology.	(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.		(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)

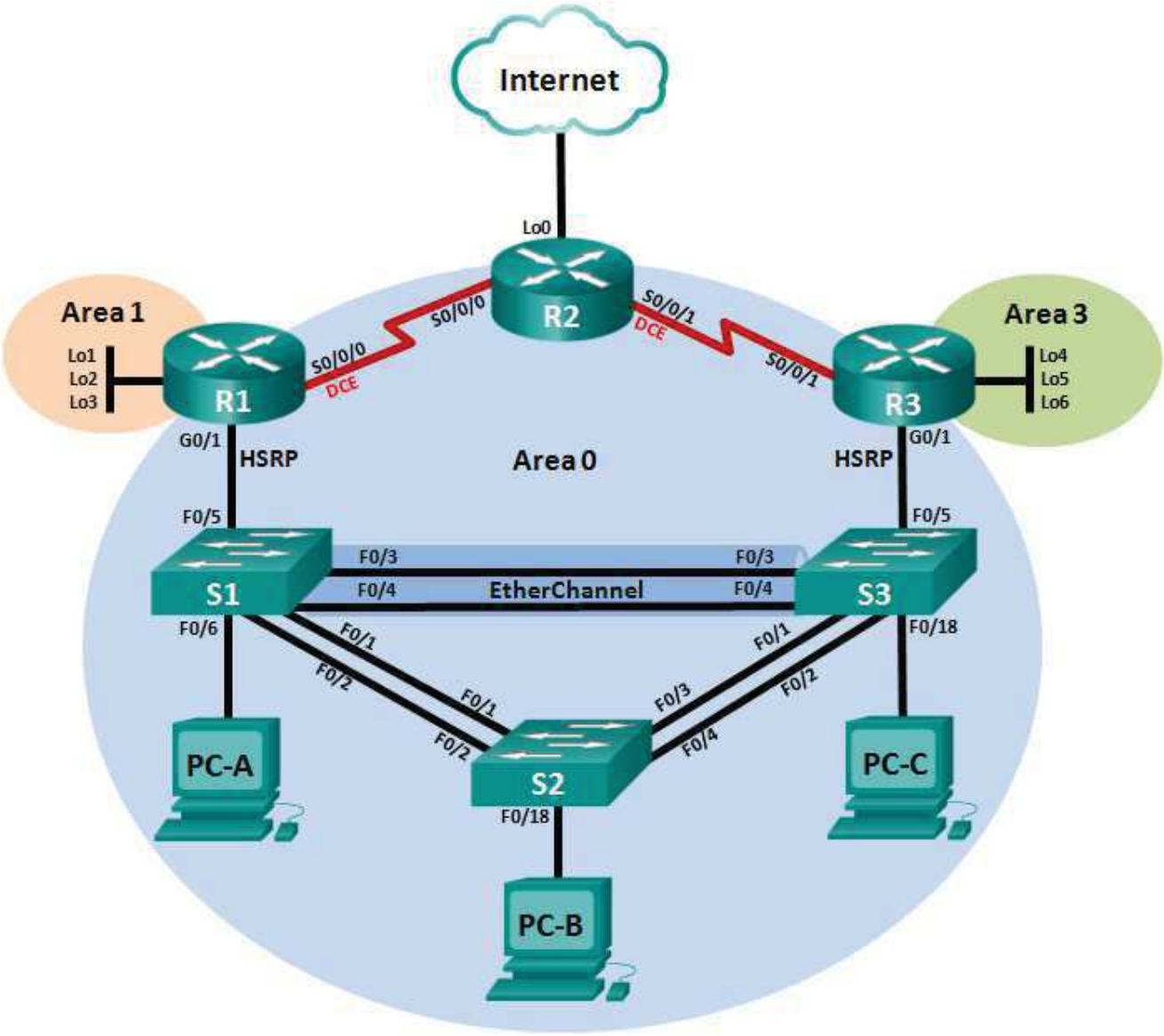
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

CCNA: Scaling Networks

Skills Assessment (OSPF) – Student Training (Answer Key)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.27.0.1	255.255.255.0	N/A
	S0/0/0	172.27.123.1	255.255.255.252	N/A
	Lo1	172.27.1.1	255.255.255.0	N/A
	Lo2	172.27.2.1	255.255.255.0	N/A
	Lo3	172.27.3.1	255.255.255.0	N/A
R2	S0/0/0	172.27.123.2	255.255.255.252	N/A
	S0/0/1	172.27.123.5	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.248	N/A
R3	G0/1	172.27.0.3	255.255.255.0	N/A
	S0/0/1	172.27.123.6	255.255.255.252	N/A
	Lo4	172.27.4.1	255.255.255.0	N/A
	Lo5	172.27.5.1	255.255.255.0	N/A
	Lo6	172.27.6.1	255.255.255.0	N/A
S1	VLAN 1	172.27.0.11	255.255.255.0	172.27.0.2
S2	VLAN 1	172.27.0.12	255.255.255.0	172.27.0.2
S3	VLAN 1	172.27.0.13	255.255.255.0	172.27.0.2
PC-A	NIC	172.27.0.21	255.255.255.0	172.27.0.2
PC-B	NIC	172.27.0.22	255.255.255.0	172.27.0.2
PC-C	NIC	172.27.0.23	255.255.255.0	172.27.0.2

Assessment Objectives

Part 1: Initialize Devices (10 points, 5 minutes)

Part 2: Configure Device Basic Settings (45 points, 30 minutes)

Part 3: Configure LAN Redundancy and Link Aggregation (28 points, 25 minutes)

Part 4: Configure OSPFv2 Dynamic Routing Protocol (51 points, 30 minutes)

Part 5: Verify Network Connectivity and HSRP Configuration (10 points, 15 minutes)

Part 6: Display IOS Image and License Information (6 points, 5 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 IPv4 connectivity, LAN redundancy, and link aggregation. You will then configure OSPFv2 and HSRP on the network and verify connectivity. Finally, you will demonstrate your knowledge of IOS images and licensing.

Instructor Note: For the student version of this exam, the instructor should build the network and connect devices prior to the student starting the exam. This will save time and reduce wear on cables and equipment. The student will need to initialize and reload devices. Scoring is adjusted accordingly.

Instructor Note: Sample scoring and estimated times for each exam part are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 150 and total time is estimated at 110 minutes. The instructor may elect to deduct points if excessive time is taken for a part of the assessment.

Instructor Note: For the initial SBA setup, the routers should have a startup-configuration saved with a hostname (Rtr). The router should also have a loopback address configured. The switches should have a startup-configuration saved with a hostname (Sw) and have VLAN 99 created. These configurations will be used to verify that the student initialized the devices correctly in Part 1, Step 1. It is recommended that these configurations are saved to flash as SBA_Init and used to reset the device for the next student.

Instructor Note: The routers used with this SA are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the SA. Refer to the Router Interface Summary Table at the end of the SA for the correct interface identifiers.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 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 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: 10

Time: 5 minutes

Step 1: Initialize and reload the routers and switches.

Erase the startup configurations and reload the devices.

Before proceeding, have your instructor verify device initializations.

Task	IOS Command	Points
Erase the startup-config file on all routers.	R1# **erase startup-config**	(2 points)
Reload all routers.	R1# **reload** (Hostnames should be reset back to **Router**.)	(2 points)
Erase the startup-config file on all switches and remove the old VLAN database.	S1# **erase startup-config** S1# **del vlan.dat**	(2 points)
Reload all switches.	S1# **reload** (Hostnames should be reset back to **Switch**.)	(2 points)
Verify VLAN database is absent from flash on all switches.	S1# **show flash** (Have student execute the CLI command on the switch.)	(2 points)

Instructor Sign-off Part 1: _____

Points: _____ of 10

Part 2: Configure Device Basic Settings

Total points: 45

Time: 30 minutes

Step 1: 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)
Interface G0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Set a clocking rate of 128000. Activate Interface	(1 points)
Interface Loopback 1 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 2 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 3 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R1# **show run** (Look for: **no ip domain lookup**)
Router name	hostname R1	(Look for : **R1>** or **R1#** command prompt)
Encrypted privileged EXEC password	enable secret class	R1> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	R1# **exit** (Type in access password)
Telnet access password	line vty 0 4 password cisco login	R1# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	R1# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface G0/1	interface g0/1 description Connection to S1 ip address 172.27.0.1 255.255.255.0 no shutdown	R1# **show ip interface G0/1** (Look for IP address and correct subnet mask)
Interface S0/0/0	interface s0/0/0 description Connection to R2 ip add 172.27.123.1 255.255.255.252 clock rate 128000 no shutdown	R1# **show interface S0/0/0** (Look for Description, Internet address, and verify that interface is not administratively down.) R1# **show controllers S0/0/0** (Look for DCE V.35, clock rate 128000)
Interface Loopback 1	interface lo1 ip address 172.27.1.1 255.255.255.0	R1# **show ip interface lo1** (Look for IP address and correct subnet mask)
Interface Loopback 2	interface lo2 ip address 172.27.2.1 255.255.255.0	R1# **show ip interface lo2** (Look for IP address and correct subnet mask)
Interface Loopback 3	interface lo3 ip address 172.27.3.1 255.255.255.0	R1# **show ip interface lo3** (Look for IP address and correct subnet mask)

Step 2: 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)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Set a clocking rate of 128000. Activate Interface	(1 point)
Interface Loopback 0 (Simulated Internet connection)	Set the description. Set the Layer 3 IPv4 address to 209.165.200.225/29.	(1 point)
Default route	Configure a default route out Lo0.	(1/2 point)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R2# **show run** (Look for: **no ip domain lookup**)
Router name	hostname R2	(Look for : **R2>** or **R2#** command prompt)
Encrypted privileged EXEC password	enable secret class	R2> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	R2# **exit** (Type in access password)
Telnet access password	line vty 0 4 password cisco login	R2# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	R2# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface S0/0/0	interface s0/0/0 description Connection to R1 ip add 172.27.123.2 255.255.255.252 no shutdown	R2# **show interface S0/0/0** (Look for Description, Internet address, and verify that interface is not administratively down.)
Interface S0/0/1	interface s0/0/1 description Connection to R3 ip add 172.27.123.5 255.255.255.252 clock rate 128000 no shutdown	R2# **show interface S0/0/1** (Look for Description, Internet address, and verify that interface is not administratively down.) R2# **show controllers S0/0/1** (Look for DCE V.35, clock rate 128000)
Interface Loopback 0 (Simulated Internet connection)	description Connection to Internet ip address 209.165.200.225 255.255.255.248	R2# **show run interface lo0** (Verify description, IP address, and subnet mask)
Default route	ip route 0.0.0.0 0.0.0.0 lo0	R2# **show ip route** (Look for: **Gateway of last resort is 0.0.0.0 to network 0.0.0.0** **S* 0.0.0.0/0 is directly connected, Loopback0**)

Step 3: 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)
Interface G0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface	(1 point)
Interface Loopback 4 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 5 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Interface Loopback 6 (LAN)	Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.	(1/2 point)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R3# **show run** (Look for: **no ip domain lookup**)
Router name	hostname R3	(Look for : **R3>** or **R3#** command prompt)
Encrypted privileged EXEC password	enable secret class	R3> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	R3# **exit** (Type in access password)
Telnet access password	line vty 0 4 password cisco login	R3# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	R3# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface G0/1	interface g0/1 description Connection to S3 ip address 172.27.0.3 255.255.255.0 no shutdown	R3# **show ip interface G0/1** (Look for IP address and correct subnet mask, and verify that interface is not administratively down.)
Interface S0/0/1	interface s0/0/1 description Connection to R2 ip add 172.27.123.6 255.255.255.252 no shutdown	R3# **show interface S0/0/1** (Look for Description, Internet address, and verify that interface is not administratively down.)
Interface Loopback 4	interface lo4 ip address 172.27.4.1 255.255.255.0	R3# **show ip interface lo4** (Look for IP address and correct subnet mask)
Interface Loopback 5	interface lo5 ip address 172.27.5.1 255.255.255.0	R3# **show ip interface lo5** (Look for IP address and correct subnet mask)
Interface Loopback 6	interface lo6 ip address 172.27.6.1 255.255.255.0	R3# **show ip interface lo6** (Look for IP address and correct subnet mask)

Step 4: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S1	(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)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S2 and S3.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Instructor Note: Ask the student to connect to S1, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	S1# **show run** (Look for: **no ip domain lookup**)
Switch name	hostname S1	(Look for : **S1>** or **S1#** command prompt)
Encrypted privileged exec password	enable secret class	S1> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	S1# **exit** (Type in access password)
Telnet access password	line vty 0 15 password cisco login	S1# **show run** (Look under line VTY 0 15 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	S1# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Assign an IPv4 address to the default SVI.	interface vlan 1 ip address 172.27.0.11 255.255.255.0 no shutdown	S1# **show ip interface vlan1** (Look for IP address and correct subnet mask)
Assign the default-gateway.	ip default-gateway 172.27.0.2	S1# **show run | section default** (Look for **ip default-gateway 172.27.0.2**)
Force trunking on all interfaces connected to S2 and S3.	interface range f0/1-4 switchport mode trunk switchport trunk native vlan 1 **Note:** VLAN 1 is the native VLAN by default, the previous command is not necessary.	S1# **show interface trunk** (Look to see if interfaces F0/1-4 are listed. If not listed check to see if interfaces are active.)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	interface range f0/5-24, g0/1-2 switchport mode access Note: The **switchport nonegotiate** command may have also been issued, this is not incorrect but it is important that these ports have been changed to access ports.	S1# **show run | begin interface** (Look to see if these ports have been set as access switch ports.)
Shutdown all unused ports.	interface range f0/7-24, g0/1-2 shutdown	S1# **show run | begin interface** (Verify that these ports are administratively shutdown.)

Step 5: Configure S2.

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S2	(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 clear text passwords.		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S1 and S3.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Instructor Note: Ask the student to connect to S2, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	S2# **show run** (Look for: **no ip domain lookup**)
Switch name	hostname S2	(Look for : **S2>** or **S2#** command prompt)
Encrypted privileged EXEC password	enable secret class	S2> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	S2# **exit** (Type in access password)
Telnet access password	line vty 0 15 password cisco login	S2# **show run** (Look under line VTY 0 15 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	S2# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Assign an IPv4 address to the default SVI.	interface vlan 1 ip address 172.27.0.12 255.255.255.0 no shutdown	S2# **show ip interface vlan1** (Look for IP address and correct subnet mask)
Assign the default-gateway.	ip default-gateway 172.27.0.2	S2# **show run | section default** (Look for **ip default-gateway 172.27.0.2**)
Force trunking on all interfaces connected to S1 and S3.	interface range f0/1-4 switchport mode trunk switchport trunk native vlan 1 **Note:** VLAN 1 is the native VLAN by default, the previous command is not necessary.	S2# **show interface trunk** (Look to see if interfaces F0/1-4 are listed. If not listed check to see if interfaces are active.)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	interface range f0/5-24, g0/1-2 switchport mode access Note: The **switchport nonegotiate** command may have also been issued, this is not incorrect but it is important that these ports have been changed to access ports.	S2# **show run | begin interface** (Look to see if these ports have been set as access switch ports.)
Shutdown all unused ports.	interface range f0/5-17, f0/19-24, g0/1-2 shutdown	S2# **show run | begin interface** (Verify that these ports are administratively shutdown.)

Step 6: Configure S3

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S3	(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)
Assign an IPv4 address to the default SVI.	Refer to the Addressing Table for IPv4 address information.	(1/2 point)
Assign the default-gateway.	Refer to the Addressing Table.	(1/2 point)
Force trunking on interfaces connected to S1 and S2.	Use VLAN 1 as the native VLAN.	(1 point)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	Make sure ports are configured as access ports.	(1 point)
Shutdown all unused ports.		(1 point)

Instructor Note: Ask the student to connect to S3, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	S3# **show run** (Look for: **no ip domain lookup**)
Switch name	hostname S3	(Look for : **S3>** or **S3#** command prompt)
Encrypted privileged EXEC password	enable secret class	S3> **enable** (Type in privileged exec password)
Console access password	line con 0 password cisco login	S3# **exit** (Type in access password)
Telnet access password	line vty 0 15 password cisco login	S3# **show run** (Look under line VTY 0 15 for: **password 7 121A0C041104**)
Encrypt the plain text passwords.	service password-encryption	S3# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Assign an IPv4 address to the default SVI.	interface vlan 1 ip address 172.27.0.13 255.255.255.0 no shutdown	S3# **show ip interface vlan1** (Look for IP address and correct subnet mask)
Assign the default-gateway.	ip default-gateway 172.27.0.2	S3# **show run | section default** (Look for **ip default-gateway 172.27.0.2**)
Force trunking on all interfaces connected to S1 and S2.	interface range f0/1-4 switchport mode trunk switchport trunk native vlan 1 **Note:** VLAN 1 is the native VLAN by default, the previous command is not necessary.	S3# **show interface trunk** (Look to see if interfaces f0/1-4 are listed. If not listed check to see if interfaces are active.)
Disable the Dynamic Trunking Protocol (DTP) on all other ports.	interface range f0/5-24, g0/1-2 switchport mode access Note: The **switchport nonegotiate** command may have also been issued, this is not incorrect but it is important that these ports have been changed to access ports.	S3# **show run | begin interface** (Look to see if these ports have been set as access switch ports.)
Shutdown all unused ports.	interface range f0/6-17, f0/19-24, g0/1-2 shutdown	S3# **show run | begin interface** (Verify that these ports are administratively shutdown.)

Step 7: Configure IPv4 addresses on PCs.

Configuration Item or Task	Specification	Points
Configure static IPv4 address information on PC-A	Refer to Addressing Table for IPv4 address information.	(1/2 point)
Configure static IPv4 address information on PC-B	Refer to Addressing Table for IPv4 address information.	(1/2 point)
Configure static IPv4 address information on PC-C	Refer to Addressing Table for IPv4 address information.	(1/2 point)

Configuration Item or Task	Specification	Command
Configure static IPv4 address information on PC-A	IPv4 address:172.27.0.21 Subnet mask: 255.255.255.0 Default gateway:172.27.0.2	**ipconfig**
Configure static IPv4 address information on PC-B	IPv4 address:172.27.0.22 Subnet mask: 255.255.255.0 Default gateway:172.27.0.2	**ipconfig**
Configure static IPv4 address information on PC-C	IPv4 address:172.27.0.23 Subnet mask: 255.255.255.0 Default gateway:172.27.0.2	**ipconfig**

Instructor Sign-off Part 2: _____

Points: _____ of 45

Part 3: Configure LAN Redundancy and Link Aggregation

Ref lab: 2.1.2.10 Lab – Building a Switched Network with Redundant Links

Ref lab: 2.3.2.3 Lab – Configuring Rapid PVST+, PortFast, and BPDU Guard

Ref lab: 2.4.3.4 Lab – Configuring HSRP and GLBP

Ref lab: 3.2.1.4 Lab – Configuring EtherChannel

Total points: 28

Time: 25 minutes

Step 1: Configure Spanning Tree on S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure as primary root bridge for VLAN 1.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-A.		(2 points)

Configuration Item or Task	Specification	IOS Commands
Configure Rapid PVST+.	spanning-tree mode rapid-pvst	S1# **show spanning-tree summary** (Verify that the switch is in rapid-pvst mode.)
Configure as primary root bridge for VLAN 1.	spanning-tree vlan 1 root primary	S1# **show spanning-tree** (Verify that the switch is the root bridge for VLAN 1.)
Configure PortFast and BPDU Guard on the interface connected to PC-A.	interface f0/6 spanning-tree portfast spanning-tree bpduguard enable	S1# **show run interface f0/6** (Verify that portfast and bpduguard have been enabled.)

Step 2: Configure Spanning Tree on S2.

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-B.		(2 points)

Configuration Item or Task	Specification	IOS Commands
Configure Rapid PVST+.	spanning-tree mode rapid-pvst	S2# **show spanning-tree summary** (Verify that the switch is in rapid-pvst mode.)
Configure PortFast and BPDU Guard on the interface connected to PC-B	interface f0/18 spanning-tree portfast spanning-tree bpduguard enable	S2# **show run interface f0/18** (Verify that portfast and bpduguard have been enabled.)

Step 3: Configure Spanning Tree on S3.

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Configure Rapid PVST+.		(2 points)
Configure as secondary root bridge for VLAN 1.		(2 points)
Configure PortFast and BPDU Guard on the interface connected to PC-C.		(2 points)

Configuration Item or Task	Specification	IOS Commands
Configure Rapid PVST+	spanning-tree mode rapid-pvst	S3# **show spanning-tree summary** (Verify that the switch is in rapid-pvst mode.)
Configure as secondary root bridge for VLAN 1.	spanning-tree vlan 1 root secondary	S3# **show run | section spanning** (Verify configuration line: **spanning-tree vlan 1 priority 28672**.)
Configure PortFast and BPDU Guard on the interface connected to PC-C	interface f0/18 spanning-tree portfast spanning-tree bpduguard enable	S3# **show run interface f0/18** (Verify that portfast and bpduguard have been enabled.)

Step 4: Configure HSRP on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
Configure the HSRP virtual IP address on interface G0/1.	Group: 1 Virtual IP address: 172.27.0.2	(2 points)
Make this the primary HSRP router.		(2 points)
Configure so this router becomes the primary HSRP router on a reboot.		(2 points)

Configuration Item or Task	Specification	IOS Commands
Configure the HSRP virtual IP address on interface G0/1.	interface g0/1 standby 1 ip 172.27.0.2	R1# **show standby** (Verify that thel G0/1 interface has been configured with HSRP using Group 1, the interface Virtual IP has a 172.27.0.2 address, and that interface is active.)
Make this the primary HSRP router.	standby 1 priority 150	R1# **show standby** (Verify that interface G0/1 has been configured with a HSRP priority greater than 100 and that the active router is local.)
Configure so this router becomes the primary HSRP router on a reboot.	standby 1 preempt	R1# **show standby** (Verify that interface G0/1 has Preemption enabled.)

Step 5: Configure HSRP on R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification	Points
Configure the HSRP virtual IP address on interface G0/1.	Group: 1 Virtual IP address: 172.27.0.2	(2 points)

Configuration Item or Task	Specification	IOS Commands
Configure the HSRP virtual IP address on interface G0/1.	interface g0/1 standby 1 ip 172.27.0.2	R3# **show standby** (Verify that interface G0/1 has been configured with HSRP using Group 1, the interface Virtual IP address is 172.27.0.2, and that the interface is in a standby state.)

Step 6: Configure an LACP EtherChannel between S1 and S3.

Configuration tasks include the following:

Configuration Item or Task	Specification	Points
On S1, configure an LACP EtherChannel on interfaces connected to S3.	Use group 1 and enable LACP unconditionally.	(2 points)
On S3, configure an LACP EtherChannel on interfaces connected to S1.	Use group 1 and enable LACP only if a LACP device is detected.	(2 points)

Configuration Item or Task	Specification	IOS Commands
On S1, configure an LACP EtherChannel on interfaces connected to S3.	interface range f0/3-4 channel-group 1 mode active	S1# **show etherchannel summary** (Verify that group 1 is connected to interfaces f0/3 and f0/4, and that the status is SU.)
On S3, configure an LACP EtherChannel on interfaces connected to S1.	interface range f0/3-4 channel-group 1 mode passive	S3# **show etherchannel summary** (Verify that group 1 is connected to interfaces f0/3 and f0/4, and that the status is SU.)

Instructor Sign-off Part 3: _____

Points: _____ of 28

Part 4: Configure OSPFv2 Dynamic Routing Protocol

Ref lab: 5.1.1.13 Lab - Configuring OSPFv2 on a Multiaccess Network

Ref lab: 5.1.4.8 Lab - Configuring OSPFv2 Advanced Features

Ref lab: 6.2.3.8 Lab - Configuring Multiarea OSPFv2

Total points: 51

Time: 30 minutes

Step 1: Configure OSPFv2 on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	1.1.1.1	(1 point)
Advertise directly connected networks.	Use classless network addresses. Assign S0/0/0 and G0/1 interfaces to Area 0. Assign Loopback interfaces to Area 1.	(2 points)
Set all LAN interfaces as passive.		(2 points)
Configure an inter-area summary route for the networks in area 1.		(2 points)
Change the default cost reference bandwidth to support Gigabit interface calculations.	1000	(2 points)
Set the bandwidth on S0/0/0.	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0.	Cost: 7500	(1 point)
Create an OSPF MD5 key on S0/0/0.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication to S0/0/0.		(2 points)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
OSPF Process ID	router ospf 1	R1# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router ID	router-id 1.1.1.1	(From output from previous command, look for: **Router-ID: 1.1.1.1**)
Advertise directly connected networks.	network 172.27.0.0 0.0.0.255 area 0 network 172.27.123.0 0.0.0.3 area 0 network 172.27.1.0 0.0.0.255 area 1 network 172.27.2.0 0.0.0.255 area 1 network 172.27.3.0 0.0.0.255 area 1	R1# **show run | section router ospf** (Compare network commands to specifications.) Can also use **show ip protocols** command.
Set all LAN interfaces as passive.	passive-interface g0/1 passive-interface lo1 passive-interface lo2 passive-interface lo3	R1# **show ip protocols** (Look at passive interface section at bottom of output. If not there, then either the network wasn't added or the passive interface command was not applied. Use the **show run | section router ospf** command to verify.)
Configure an inter-area summary route for the networks in area 1.	area 1 range 172.27.0.0 255.255.252.0	R1# **show ip route ospf** (Look for the OSPF route: **O 172.27.0.0/22 is a summary, 00:01:01, Null0**)
Change the default cost reference bandwidth to allow for Gigabit interfaces.	auto-cost reference-bandwidth 1000	R1# **show run | section router** (Look for: auto-cost reference-bandwidth 1000)
Set the bandwidth on S0/0/0.	interface s0/0/0 bandwidth 128	R1# **show interface s0/0/0** (Look for **BW 128 Kbit/sec**,)
Adjust the metric cost of S0/0/0.	ip ospf cost 7500	R1# **show ip ospf interface brief** (Look for: Se0/0/0 1 0 172.27.123.1/30 **7500** P2P 1/1)
Create an OSPF MD5 key on S0/0/0.	ip ospf message-digest-key 1 md5 CISCO	R1# **show run interface s0/0/0** (Look for: **ip ospf message-digest-key 1 md5 7 0802657D2A36**)
Apply MD5 authentication to S0/0/0.	ip ospf authentication message-digest	R1# **show run interface s0/0/0** (Look for: **ip ospf authentication message-digest**)

Step 2: Configure OSPFv2 on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	2.2.2.2	(1 point)
Advertise directly connected networks.	Use classless network addresses. All connected networks should be assigned to Area 0 except the Lo0 network.	(2 points)
Propagate the default route to all other OSPF routers.		(2 points)
Change the default cost reference bandwidth to allow for Gigabit interfaces.	1000	(2 points)
Set the bandwidth on all serial interfaces.	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0.	Cost: 7500	(1 point)
Create an OSPF MD5 key on the serial interfaces.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication on the serial interfaces.		(2 points)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
OSPF Process ID	router ospf 1	R2# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router ID	router-id 2.2.2.2	(From output from previous command, look for: **Router-ID: 2.2.2.2**)
Advertise directly connected networks.	network 172.27.123.0 0.0.0.3 area 0 network 172.27.123.4 0.0.0.3 area 0	R2# **show run | section router ospf** (Compare network commands to specifications.) Can also use **show ip protocols** command.
Propagate the default route to all other OSPF routers.	default-information originate	R2# **show run |section router ospf** (Look for the **default-information originate** command.)
Change the default cost reference bandwidth to allow for Gigabit interfaces.	auto-cost reference-bandwidth 1000	R2# **show run | section router** (Look for: **auto-cost reference-bandwidth 1000**)
Set the bandwidth on all serial interfaces.	interface s0/0/0 bandwidth 128 interface s0/0/1 bandwidth 128	R2# **show interface s0/0/0** R2# **show interface s0/0/1** (Look for **BW 128 Kbit/sec**,)
Adjust the metric cost of S0/0/0.	interface s0/0/0 ip ospf cost 7500	R2# **show ip ospf interface brief** (Look for: Se0/0/0 1 0 172.16.12.1/30 **7500** P2P 1/1)
Create an OSPF MD5 key on the serial interfaces.	interface s0/0/0 ip ospf message-digest-key 1 md5 CISCO interface s0/0/1 ip ospf message-digest-key 1 md5 CISCO	R2# **show run interface s0/0/0** R2# **show run interface s0/0/1** (Look for: **ip ospf message-digest-key 1 md5 7 0802657D2A36**)
Apply MD5 authentication on the serial interfaces.	interface s0/0/0 ip ospf authentication message-digest interface s0/0/1 ip ospf authentication message-digest	R2# **show run interface s0/0/1** R2# **show run interface s0/0/1** (Look for: **ip ospf authentication message-digest**)

Step 3: Configure OSPFv2 on R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	3.3.3.3	(1 point)
Advertise directly connected networks.	Use classless network addresses Assign S0/0/1 and G0/1 interfaces to Area 0 Assign Loopback interfaces to Area 3	(2 points)
Set all LAN interfaces as passive.		(2 points)
Configure an inter-area summary route for the networks in area 3.		(2 points)
Change the default cost reference bandwidth to support Gigabit interface calculations.	1000	(2 points)
Set the serial interface bandwidth.	128 Kb/s	(1 point)
Create an OSPF MD5 key on S0/0/1.	Key: **1** Password: **CISCO**	(2 points)
Apply MD5 authentication to S0/0/1.		(2 points)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
OSPF Process ID	router ospf 1	R3# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router ID	router-id 3.3.3.3	(From output from previous command, look for: **Router-ID: 3.3.3.3**)
Advertise directly connected networks.	network 172.27.0.0 0.0.0.255 area 0 network 172.27.123.4 0.0.0.3 area 0 network 172.27.4.0 0.0.0.255 area 3 network 172.27.5.0 0.0.0.255 area 3 network 172.27.6.0 0.0.0.255 area 3	R3# **show run | section router ospf** (Compare network commands to specifications. Can also use **show ip protocols** command.)
Set all LAN (Loopback) interfaces as passive.	passive-interface g0/1 passive-interface lo4 passive-interface lo5 passive-interface lo6	R3# **show ip protocols** (Look at passive interface section at bottom of output. If not there then either the network wasn't added or the passive interface command was not applied. Use the **show run | section router ospf** command to verify.)
Configure an inter-area summary route for the networks in area 3.	area 3 range 172.27.4.0 255.255.252.0	R3# **show ip route ospf** (Look for the OSPF route: **O 172.27.4.0/22 is a summary, 00:01:01, Null0**)
Change the default cost reference bandwidth to allow for Gigabit interfaces.	auto-cost reference-bandwidth 1000	R3# **show run | section router** (Look for: **auto-cost reference-bandwidth 1000**)
Set the bandwidth on S0/0/1.	interface s0/0/1 bandwidth 128	R3# **show interface s0/0/1** (Look for **BW 128 Kbit/sec**,)
Create an OSPF MD5 key on S0/0/1.	ip ospf message-digest-key 1 md5 CISCO	R3# **show run interface s0/0/1** (Look for: **ip ospf message-digest-key 1 md5 7 0802657D2A36**)
Apply MD5 authentication to S0/0/1.	ip ospf authentication message-digest	R3# **show run interface s0/0/0** (Look for: **ip ospf authentication message-digest**)

Step 4: Verify network connectivity.

Verify that OSPF is functioning as expected. Enter the appropriate CLI command to discover the following information:

Question	Response	Points
What command will display all connected OSPFv2 routers?	show ip ospf neighbor	(1 point)
What command displays a summary list of OSPF interfaces that includes a column for the cost of each interface?	show ip ospf interface brief	(1 point)
What command displays the OSPF Process ID, Router ID, Address summarizations, Routing Networks, and Passive Interfaces configured on a router?	show ip protocols	(1 point)
What command displays only OSPF routes?	show ip route ospf	(1 point)
What command displays detailed information about the OSPF interfaces, including the authentication method?	show ip ospf interface	(1 point)
What command displays the OSPF section of the running-configuration?	show run | section router ospf	(1 point)

Instructor Sign-off Part 4: _____

Points: _____ of 51

Part 5: Verify Network Connectivity and HSRP Configuration

Total points: 10

Time: 15 minutes

Use the listed command to verify that network is working as expected.

Step 1: Verify end-to-end connectivity.

Take corrective action if results are other than expected.

From	Command	To	Expected Results	Points
PC-A	ping	PC-C	Ping should be successful.	(1 point)
PC-B	ping	PC-A	Ping should be successful.	(1 point)
PC-B	ping	PC-C	Ping should be successful.	(1 point)
PC-B	ping	Default Gateway	Ping should be successful.	(1 point)
PC-B	ping	209.165.200.225	Ping should be successful.	(1 point)
PC-B	tracert	209.165.200.225	Trace should route through R1.	(1 point)

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

Step 2: Verify HSRP is working as expected.

Issue the **shutdown** command on R1 G0/1, and then re-issue the following commands to verify that HSRP is working as expected:

From	Command	To	Expected Results	Points
PC-B	ping	172.27.0.1	Ping should **not** be successful.	(1 point)
PC-B	ping	Default Gateway	Ping should be successful.	(1 point)
PC-B	ping	209.165.200.225	Ping should be successful.	(1 point)
PC-B	tracert	209.165.200.225	Trace should route through R3.	(1 point)

Note: Wait a few seconds before testing after shutting down the interface on R1.

Instructor Sign-off Part 5: _____

Points: _____ of 10

Part 6: Display IOS Image and License Information

Ref Video: 9.1.2.6 – Managing Cisco IOS Images

Ref Video: 9.2.2.5 – Working with IOS 15 Image Licenses

Total points: 6

Time: 5 minutes

Enter the appropriate CLI command to discover the following information:

Question	Response	Points
What command displays the IOS image that is currently being used by the network device?	show version	(1 point)
What command displays the size of an IOS image loaded on a network device?	show flash	(1 point)
What command displays a summary list of the Technology Package licenses on an ISR-G2 device that includes the current the state of each of those licenses?	show version	(1 point)
What command displays the amount of space available to install an additional IOS image to a network device?	show flash	(1 point)
What command displays a list of all the licenses on an ISR-G2 device?	show license	(1 point)
What command would you use to accept the end user license agreement?	config t license accept end user agreement	(1 point)

Instructor Sign-off Part 6: _____

Points: _____ of 6

Part 7: 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.

Disconnect and neatly put away all cables that were used in the SA exam.

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 (S0/0/1)
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)

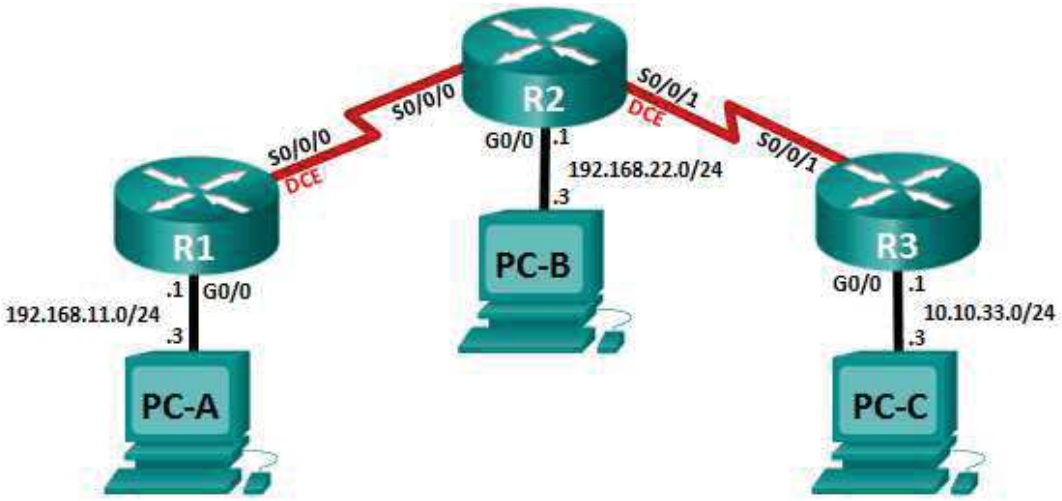
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

CCNA: Connecting Networks

Skills Assessment – Student Training (Answer Key)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

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.

Instructor Note: For the student version of this exam, the instructor should build the network and connect devices prior to the student starting the exam. This will save time and reduce wear on cables and equipment. The student will need to initialize and reload devices. Scoring is adjusted accordingly.

Instructor Note: Sample scoring and estimated times for each exam part are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 100 and total time is estimated at 115 minutes. The instructor may elect to deduct points if excessive time is taken for a part of the assessment.

Instructor Note: For the initial SBA setup, the routers should have a startup-configuration saved with a hostname (Rtr). The router should also have a loopback address configured. These configurations will be used to verify that the student initialized the devices correctly in Part 1, Step 1. It is recommended that these configurations are saved to flash as SBA_Init and used to reset the device for the next student.

Instructor Note: The routers used with this SA are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the SA. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

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

Instructor Note: Optionally, SNMP management software, such as PowerSNMP Free Manager, may be installed on PC-A. Refer to Lab 8.2.2.5 – Configuring SNMP)

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.	R1# **erase startup-config**	(1 point)
Reload all routers.	R1# **reload** (Verify by using **show run** command to see if loopback addresses are missing. Hostnames should be reset back to **Router**.)	(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.	IP Address: 192.168.11.3 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.11.1	(1 point)
Configure static IPv4 address information on PC-B.	IP Address: 192.168.22.3 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.22.1	(1 point)
Configure static IPv4 address information on PC-C.	IP Address: 10.10.33.3 Subnet Mask: 255.255.255.0 Default Gateway: 10.10.33.1	(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)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R1# **show run** (Look for: **no ip domain lookup**)
Router name	R1	(Look for : **R1>** or **R1#** command prompt)
Encrypted privileged EXEC password	class	R1> **enable** (Type in privileged exec password)
Console access password	cisco	R1# **exit** (Type in access password)
Telnet access password	cisco	R1# **show run** (Look under line VTY 0 4 for: **password 7 094F471A1A0A**)
Encrypt the plain text passwords	service password-encryption	R1# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Configure G0/0	interface g0/0 description Connection to 192.168.11.0 LAN ip address 192.168.11.1 255.255.255.0 no shutdown	R1# **show run interface g0/0** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)

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)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R2# **show run** (Look for: **no ip domain lookup**)
Router name	R2	(Look for : **R2>** or **R2#** command prompt)
Encrypted privileged EXEC password	class	R2> **enable** (Type in privileged exec password)
Console access password	cisco	R2# **exit** (Type in access password)
Telnet access password	cisco	R2# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	R2# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Configure G0/0	interface g0/0 description Connection to 192.168.22.0 LAN ip address 192.168.22.1 255.255.255.0 no shutdown	R2# **show run interface g0/0** (Verify configuration.) R2# **show ip interface brief** (Verify that the interface is active.)

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)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R3# **show run** (Look for: **no ip domain lookup**)
Router name	R3	(Look for : **R3>** or **R3#** command prompt)
Encrypted privileged EXEC password	class	R3> **enable** (Type in privileged exec password)
Console access password	cisco	R3# **exit** (Type in access password)
Telnet access password	cisco	R3# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	R3# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Configure G0/0	interface g0/0 description Connection to 10.10.33.0 LAN ip address 10.10.33.1 255.255.255.0 no shutdown	R3# **show run interface g0/0** (Verify configuration.) R3# **show ip interface brief** (Verify that the interface is active.)

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**.	R1# **copy running-config BasicConfig**	(1/2 point)
Copy the running-config on R2 to flash. Name the file **BasicConfig**.	R2# **copy running-config BasicConfig**	(1/2 point)
Copy the running-config on R3 to flash. Name the file **BasicConfig**.	R3# **copy running-config BasicConfig**	(1/2 point)

Instructor Sign-off Part 2: _____

Points: _____ of 18

Part 3: Configure PPP Connections

Ref lab: 3.3.2.8 – Configuring Basic PPP with Authentication

Total points: 17

Time: 20 minutes

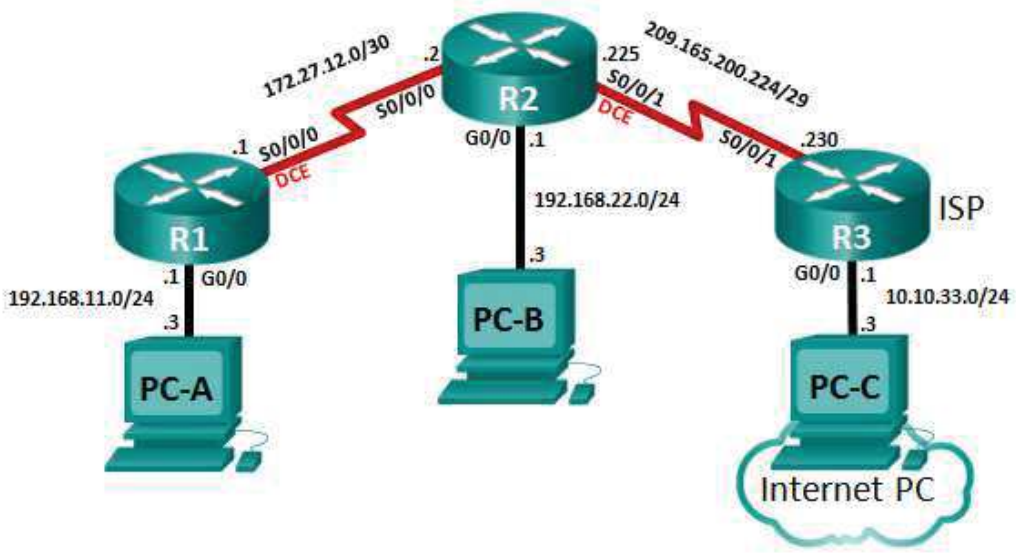


Figure 1: PPP Topology

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.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set encapsulation to **PPP**. Set the clocking rate to **128000**. Activate the interface.	(2 points)
Configure CHAP authentication on S0/0/0.		(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.		(1/2 point)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/0.	interface s0/0/0 description PPP connection to R2. ip address 172.27.12.1 255.255.255.252 encapsulation ppp clock rate 128000 no shutdown	R1# **show run interface s0/0/0** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)
Configure CHAP authentication on S0/0/0.	Interface s0/0/0 ppp authentication chap	R1# **show run interface s0/0/0** (Look for the configuration line: **ppp authentication chap**)
Create a local database entry to use for CHAP authentication.	username R2 password cisco	R1# **show run | section user** (Verify that configuration line: **username R2 password 7 02050D480809** is listed.)
Set a static default route out S0/0/0.	ip route 0.0.0.0 0.0.0.0 s0/0/0	R1# **show ip route** (Verify that the static route is in the routing table.)

Step 2: Configure R2.

Configuration tasks for R2 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Activate the interface.	(2 point)
Configure CHAP authentication on S0/0/0.		(1 point)
Create a local database entry for CHAP authentication.	Username: **R1** Password: **cisco**	(1 point)
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Set the clocking rate to **128000**. Activate the interface.	(2 points)
Set a static default route out S0/0/1.		(1/2 point)
Set a static route for R1 LAN traffic out S0/0/0.		(1 point)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/0.	interface s0/0/0 description PPP connection to R1. ip address 172.27.12.2 255.255.255.252 encapsulation ppp no shutdown	R2# **show run interface s0/0/0** (Verify configuration.) R2# **show ip interface brief** (Verify that the interface is active.)
Configure CHAP authentication on S0/0/0.	Interface s0/0/0 ppp authentication chap	R2# **show run interface s0/0/0** (Look for the configuration line: **ppp authentication chap**)
Create a local database entry to use for CHAP authentication.	username R1 password cisco	R2# **show run | section user** (Verify that configuration line: **username R1 password 7 02050D480809** is listed.)
Configure S0/0/1.	interface s0/0/1 description PPP connection to ISP ip address 209.165.200.225 255.255.255.248 encapsulation ppp clock rate 128000 no shutdown	R2# **show run interface s0/0/1** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)
Set a static default route out S0/0/1.	ip route 0.0.0.0 0.0.0.0 s0/0/1	R1# **show ip route** (Verify that the static route is in the routing table.)
Set a static route for R1 LAN traffic out S0/0/0.	ip route 192.168.11.0 255.255.255.0 s0/0/0	R1# **show ip route** (Verify that the static route is in the routing table.)

Step 3: Configure R3.

Configuration tasks for R3 include the following:

Task	Specification	Points
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information. Set the encapsulation to **PPP**. Activate the interface.	(2 points)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/1.	interface s0/0/1 description PPP connection to ISP ip address 209.165.200.230 255.255.255.248 encapsulation ppp no shutdown	R3# **show run interface s0/0/1** (Verify configuration.) R3# **show ip interface brief** (Verify that the interface is active.)

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

Ref lab: 5.2.2.6 - Configuring Dynamic and Static 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.	Inside Global: **209.165.200.226**	(1 point)
Define an access control list to permit the R1 LAN for dynamic NAT.	Access List: **1**	(1 point)
Define the dynamic NAT pool for the R1 LAN.	Pool: **R1-LAN** Inside Global: **209.165.200.227**	(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.	Inside source: **Access list 1** Outside pool: **R1-LAN**	(1 point)
Define an access control list to permit the R2 LAN for dynamic NAT.	Access List: **2**	(1 point)
Define the dynamic NAT pool for the R2 LAN.	Pool: **R2-LAN** Inside Global: **209.165.200.228**	(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.	Inside source: **Access list 2** Outside pool: **R2-LAN**	(1 point)
Assign the outside NAT interface.		(1 point)
Assign the inside NAT interface for the R1 LAN.		(1 point)
Assign the inside NAT interface for the R2 LAN.		(1 point)

Task	Specification	IOS Commands
Assign the static NAT address 209.165.200.226 to map to the IP address for PC-B.	ip nat inside source static 192.168.22.3 209.165.200.226	R2# **show run | include ip nat** (Verify the command in the Specification box is listed.)
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	R2# **show access-lists** (Verify the command in the Specification box is listed.)
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	R2# **show run | include ip nat** (Verify the command in the Specification box is listed.)
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	R2# **show run | include ip nat** (Verify the command in the Specification box is listed.)
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	R2# **show access-lists** (Verify the command in the Specification box is listed.)
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	R2# **show run | include ip nat** (Verify the command in the Specification box is listed.)
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	R2# **show run | include ip nat** (Verify the command in the Specification box is listed.)
Assign the outside NAT interface.	interface s0/0/1 ip nat outside	R2# **show run interface s0/0/1** (Verify the command in the Specification box is listed.)
Assign the inside NAT interface for the R1 LAN.	interface s0/0/0 ip nat inside	R2# **show run interface s0/0/0** (Verify the command in the Specification box is listed.)
Assign the inside NAT interface for the R2 LAN.	interface g0/0 ip nat inside	R2# **show run interface g0/0** (Verify the command in the Specification box is listed.)

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

Ref lab: 8.1.2.6 – Configuring Syslog and NTP

Ref lab: 8.2.2.5 – Configuring SNMP

Ref lab: 8.3.3.3 – Collecting and Analyzing NetFlow Data

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.	Date: **August 25, 2013** Time: **9 am**	(1 point)
Configure R2 as the NTP Master.	Stratum Number: **5**	(1 point)
Configure R1 so that it uses R2 as its NTP Server.		(1 point)

Task	Specification	IOS Commands
Set the clock on R2 to a date and time unique for NTP testing.	clock set 9:00:00 25 August 2013	R2# **show clock** (Verify that the clock is set to the correct date and time.)
Configure R2 as the NTP Master.	ntp master 5	R2# **show ntp status** (Verify that R2 is the master with a stratum setting of 5.)
Configure R1 so that it uses R2 as its NTP Server.	ntp server 172.27.12.2	R1# **show ntp associations** (Verify that the reference clock has R2's IP address.)

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.	Include milliseconds in the timestamp.	(1 points)
Enable logging of messages on R1 and R2.	Syslog server: **192.168.11.3**	(1 points)
Change message trapping level on R1 and R2.	Level: **debugging** (severity 7)	(1 points)

Task	Specification	IOS Commands
Enable the timestamp service on R1 and R2 for system logging purposes.	service timestamps log datetime msec	R1# **show run | include service** (Verify the command in the Specification box is listed.) R2# **show run | include service** (Verify the command in the Specification box is listed.)
Enable logging of messages on R1 and R2.	logging host 192.168.11.3	R1# **show run | include logging** (Verify the command in the Specification box is listed.) R2# **show run | include logging** (Verify the command in the Specification box is listed.)
Change message trapping level on R1 and R2.	logging trap debugging	R1# **show run | include logging** (Verify the command in the Specification box is listed.) R2# **show run | include logging** (Verify the command in the Specification box is listed.)

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.	Access List: **SNMP-ACCESS**	(1 points)
Enable SNMP community access to the SNMP-ACCESS access list.	Community: **SA-LAB** Access level: **Read-only**	(1 points)
Set the SNMP notification host.	Host: **192.168.11.3** Version: **2c** Community: **SA-LAB**	(1 points)
Enable all SNMP traps.		(1 points)

Task	Specification	IOS Commands
Create a standard access list to permit PC-A to retrieve SNMP information from R1.	ip access-list standard SNMP-ACCESS permit 192.168.11.3	R1# **show run | include snmp** (Verify the command in the Specification box is listed. It should be the first line listed.)
Enable SNMP community access to the SNMP-ACCESS access list.	snmp-server community SA-LAB ro SNMP-ACCESS	R1# **show run | include snmp** (Verify the command in the Specification box is listed. It should be the first line listed.)
Set the SNMP notification host.	snmp-server host 192.168.11.3 version 2c SA-LAB	R1# **show snmp host** (Look for: **Notification host: 192.168.11.3 udp-port: 162 type: trap** **user: SA-LAB security model: v2c**.)
Enable all SNMP traps.	snmp-server enable traps	R1# **show run | include snmp** (There should be pages of traps listed.)

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.		(1 points)
Configure NetFlow data export.	Destination: **PC-B IP address** UDP Port: **9996**	(1 points)
Configure the NetFlow export version.	Version: **9**	(1 points)

Task	Specification	IOS Commands
Configure NetFlow data capture on both serial interfaces. Capture ingress and egress data packets.	interface s0/0/0 ip flow ingress ip flow egress interface s0/0/1 ip flow ingress ip flow egress	R2# **show ip flow interface** (Verify that both serial interfaces have ip flow ingress and ip flow egress configured.)
Configure NetFlow data Export.	ip flow-export destination 192.168.22.3 9996	R2# **show ip flow export** (Verify that the destination points to 192.168.22.3 (9996).)
Configure the NetFlow export version.	ip flow-export version 9	R2# **show ip flow export** (Verify that Version 9 flow records is listed.)

Step 5: Verify monitoring configurations.

Enter the appropriate CLI command needed to display the following:

Command Description	Student Input (command)	Points
Display the date and time.	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

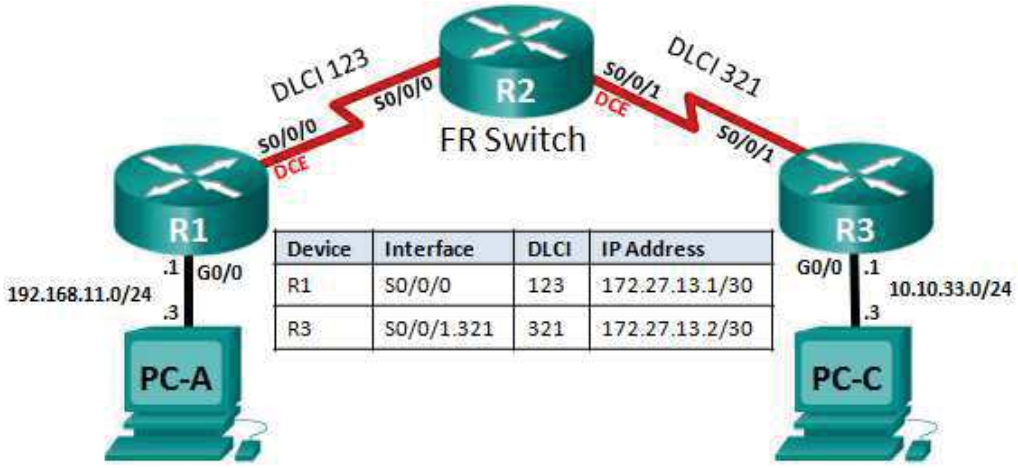
Part 6: Configure Frame Relay

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

Ref lab: 4.2.2.7 – Configuring Frame Relay and Subinterfaces

Total points: 17

Time: 20 minutes



Device	Interface	DLCI	IP Address
R1	S0/0/0	123	172.27.13.1/30
R3	S0/0/1.321	321	172.27.13.2/30

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.

a. Erase the startup configurations and reload the devices.

b. 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.

c. 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
```

Instructor Note: Students may need assistance with copying this configuration to R2.

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.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 2 at the top of Part 6 for IP address information. Set encapsulation to **frame-relay** Set the clocking rate to 128000	(2 points)
Disable Inverse ARP on S0/0/0.		(1/2 point)
Map the IP local address to the DLCI.	Refer to Figure 2 for DLCI information.	(1 point)
Map the remote IP address to the DLCI. Allow for multicast or broadcast traffic.	Refer to Figure 2 for IP address and DLCI information.	(1 point)
Change the LMI type to the ANSI standard.		(1 point)
Activate the interface.		(1/2 point)
Create a default route to the IP address on the other side of the Frame Relay link.	Refer to Figure 2 for the IP address.	(1/2 point)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/0.	interface s0/0/0 description Frame Relay connection to R3. ip address 172.27.13.1 255.255.255.252 encapsulation frame-relay clock rate 128000 no shutdown	R1# **show run interface s0/0/0** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)
Disable Inverse ARP on S0/0/0.	no frame-relay inverse-arp	R1# **show run interface s0/0/0** (Verify the command in the Specification box is listed.)
Map the local IP address to the DLCI.	frame-relay map ip 172.27.13.1 123	R1# **show run interface s0/0/0** (Verify the command in the Specification box is listed.)
Map the remote IP address to the DLCI. Allow for multicast or broadcast traffic.	frame-relay map ip 172.27.13.2 123 broadcast	R1# **show run interface s0/0/0** (Verify the command in the Specification box is listed.)
Change the LMI type to the ANSI standard.	frame-relay lmi-type ansi	R1# **show frame-relay lmi** (Verify that the **LMI TYPE = ANSI**.)
Activate the interface.	no shutdown	R1# **show ip interface brief** (Verify that the interface is not administratively shutdown.)
Create a default route to the IP address on the other side of the Frame Relay link.	ip route 0.0.0.0 0.0.0.0 172.27.13.2	R1# **show ip route** (Verify that a static default route to 172.27.13.2 is listed in the routing table.)

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.	Configure Frame Relay Encapsulation. Set encapsulation to **frame-relay** (use the IETF standard). Activate the interface.	(1 point)
Create a point-to-point subinterface on S0/0/1.	Subinterface #: **321** Set the description.	(1 point)
Set the Layer 3 IPv4 address on the subinterface.	Refer to Figure 2 at the top of Part 6 for IP address information.	(1 point)
Disable Inverse ARP on the subinterface.		(1/2 point)
Map the subinterface to the DLCI.	Refer to Figure 2 for DLCI information.	(1 point)
Create a default route to the IP address on the other side of the Frame Relay link.	Refer to Figure 2 for IP address.	(1/2 point)

Task	Specification	IOS Commands
Configure S0/0/1.	interface s0/0/1 encapsulation frame-relay ietf no shutdown	R3# **show run interface s0/0/1** (Verify configuration.) R3# **show ip interface brief** (Verify that the interface is active.)
Create a point-to-point subinterface on S0/0/1	interface s0/0/1.321 point-to-point description Frame Relay connection to R1	R3# **show run interface s0/0/1.321** (Verify the commands in the Specification box are listed.)
Set the Layer 3 IPv4 address on the subinterface.	ip address 172.27.13.2 255.255.255.252	R3# **show run interface s0/0/1.321** (Verify the command in the Specification box is listed.)
Disable Inverse ARP on the subinterface.	no frame-relay inverse-arp	R3# **show run interface s0/0/1.321** (Verify the command in the Specification box is listed.)
Map the subinterface to the DLCI.	frame-relay interface-dlci 321	R3# **show run interface s0/0/1.321** (Verify the command in the Specification box is listed.)
Create a default route to the IP address on the other side of the Frame Relay link.	ip route 0.0.0.0 0.0.0.0 172.27.13.1	R3# **show ip route** (Verify that a static default route to IP address 172.27.13.1 is listed in the routing table.)

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.

Ref lab: 7.2.2.5 – Configuring a Point-to-Point GRE VPN Tunnel

Total points: 16

Time: 20 minutes

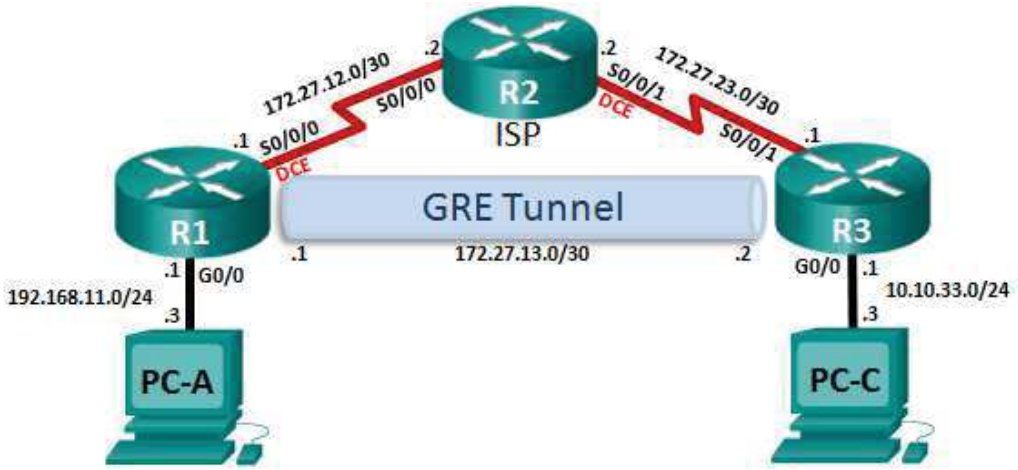


Figure 3: GRE VPN Topology

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.

a. Erase the startup configurations and reload the devices.

b. 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.

c. Issue the **no shutdown** command for the G0/0 interface on R1 and R3.

Step 2: Configure Serial Interfaces.

a. Configuration tasks for R1 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Set the clocking rate to **128000**. Activate the interface.	(1 point)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/0.	interface s0/0/0 description HDLC connection to ISP ip address 172.27.12.1 255.255.255.252 encapsulation hdlc clock rate 128000 no shutdown	R1# **show run interface s0/0/0** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)

b. Configuration tasks for R2 include the following:

Task	Specification	Points
Configure S0/0/0.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Activate the interface.	(1 point)
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Set the clocking rate to **128000.** Activate the interface.	(1 point)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/0.	interface s0/0/0 description HDLC connection to R1 ip address 172.27.12.2 255.255.255.252 encapsulation hdlc no shutdown	R2# **show run interface s0/0/0** (Verify configuration.) R2# **show ip interface brief** (Verify that the interface is active.)
Configure S0/0/1.	interface s0/0/1 description HDLC connection to R3. ip address 172.27.23.2 255.255.255.252 encapsulation hdlc clock rate 128000 no shutdown	R2# **show run interface s0/0/1** (Verify configuration.) R1# **show ip interface brief** (Verify that the interface is active.)

c. Configuration tasks for R3 include the following:

Task	Specification	Points
Configure S0/0/1.	Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information. Set the encapsulation to **HDLC.** Activate the interface.	(1 point)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Task	Specification	IOS Commands
Configure S0/0/1.	interface s0/0/1 description HDLC connection to ISP. ip address 172.27.23.1 255.255.255.252 encapsulation hdlc no shutdown	R3# **show run interface s0/0/1** (Verify configuration.) R3# **show ip interface brief** (Verify that the interface is active.)

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.	Interface: **tunnel 0** Set the description. Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP address information.	(2 points)
Use S0/0/0 as the tunnel source.		(1/2 point)
Set the tunnel destination with the IP address of the R3 S0/0/1 interface.	Refer to Figure 3 for IP address information.	(1/2 point)
Create a default route out S0/0/0.		(1/2 point)
Configure EIGRP on R1	Autonomous System (AS) number: **1**	(1/2 point)
Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.	Refer to the GRE VPN topology.	(1/2 point)

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

Task	Specification	IOS Commands
Create a GRE tunnel interface.	interface tunnel 0 description GRE VPN tunnel to R3 ip address 172.27.13.1 255.255.255.252	R1# **show run interface tunnel 0** (Verify configuration.)
Use S0/0/0 as the tunnel source.	tunnel source s0/0/0	R1# **show run interface tunnel 0** (Verify configuration.)
Set the tunnel destination with the IP address of the R3 S0/0/1 interface.	tunnel destination 172.27.23.1	R1# **show run interface tunnel 0** (Verify configuration.)
Create a default route out S0/0/0.	ip route 0.0.0.0 0.0.0.0 s0/0/0	R1# **show ip route** (Verify that the static route is in the routing table.)
Configure EIGRP on R1	router eigrp 1	R1# **show run | section eigrp** (Verify the command in the Specification box is listed.)
Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.	network 192.168.11.0 0.0.0.255 network 172.27.13.0 0.0.0.3 passive-interface g0/0	R1# **show run | section eigrp** (Verify the commands in the Specification box are listed.)

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.	Interface: **tunnel 0** Set the description. Set the Layer 3 IPv4 address. Use the IP address information listed in Figure 3 at the top of Part 7.	(2 points)
Use S0/0/1 as the tunnel source.		(1/2 point)
Set the tunnel destination with the IP address of the R1 S0/0/0 interface.	Refer to Figure 3 at the top of Part 7 for IP address information.	(1/2 point)
Create a default route out S0/0/1.		(1/2 point)
Configure EIGRP on R3	Autonomous System (AS) number: **1**	(1/2 point)
Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.	Refer to the GRE VPN topology.	(1/2 point)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Task	Specification	IOS Commands
Create a GRE tunnel interface.	interface tunnel 0 description GRE VPN tunnel to R1 ip address 172.27.13.2 255.255.255.252	R3# **show run interface tunnel 0** (Verify configuration.)
Use S0/0/0 as the tunnel source	tunnel source s0/0/1	R3# **show run interface tunnel 0** (Verify configuration.)
Set the tunnel destination with the IP address of the R3 S0/0/1 interface.	tunnel destination 172.27.12.1	R3# **show run interface tunnel 0** (Verify configuration.)
Create a default route out S0/0/1.	ip route 0.0.0.0 0.0.0.0 s0/0/1	R3# **show ip route** (Verify that the static route is in the routing table.)
Configure EIGRP on R1	router eigrp 1	R3# **show run | section eigrp** (Verify the commands in the Specification box are listed.)
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 g0/0	R3# **show run | section eigrp** (Verify the commands in the Specification box are listed.)

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 interfaces tunnel 0	(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.

Disconnect and neatly put away all cables that were used in the Final.

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)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.