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.

<table>
<thead>
<tr>
<th>Task</th>
<th>IOS Command</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase the startup-config file on all routers.</td>
<td>R1# erase startup-config</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Reload all routers.</td>
<td>R1# reload</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>(Verify by using show run command to see if loopback addresses are missing. Hostnames should be reset back to Router.)</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R1</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>
| 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.
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td>no ip domain lookup</td>
<td>R1# show run (Look for: no ip domain lookup)</td>
</tr>
<tr>
<td>Router name</td>
<td>R1</td>
<td>(Look for: R1&gt; or R1# command prompt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>R1&gt; enable (Type in privileged exec password)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>R1# exit (Type in access password)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>R1# show run (Look under line VTY 0 4 for: password 7 094F471A1A0A)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td>service password-encryption</td>
<td>R1# show run (Look for: service password-encryption)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>banner motd @ Unauthorized Access is Prohibited! @</td>
<td>(Verify banner during above step)</td>
</tr>
<tr>
<td>Configure G0/0</td>
<td>interface g0/0 description Connection to 192.168.11.0 LAN ip address 192.168.11.1 255.255.255.0 no shutdown</td>
<td>R1# show run interface g0/0 (Verify configuration.) R1# show ip interface brief (Verify that the interface is active.)</td>
</tr>
</tbody>
</table>

**Step 3: Configure R2.**

Configuration tasks for R2 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure G0/0</td>
<td>Set the description.</td>
<td>(1 1/2 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Use the IP address information listed in the Topology.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Item or Task

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

### Step 4: Configure R3.

Configuration tasks for R3 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure G0/0</td>
<td>Set the description. Set the Layer 3 IPv4 address. Use the IP address information listed in the Topology. Activate the interface.</td>
<td>(1 1/2 point)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy the running-config on R1 to flash. Name the file <em>BasicConfig</em>.</td>
<td>R1# <code>copy running-config BasicConfig</code></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Copy the running-config on R2 to flash. Name the file <em>BasicConfig</em>.</td>
<td>R2# <code>copy running-config BasicConfig</code></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Copy the running-config on R3 to flash. Name the file <em>BasicConfig</em>.</td>
<td>R3# <code>copy running-config BasicConfig</code></td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Instructor Sign-off Part 2: ______________________
Points: _________ of 18**

**Part 3: Configure PPP Connections**

Ref lab: 3.3.2.8 – Configuring Basic PPP with Authentication
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure S0/0/0.</strong></td>
<td>Set the description.</td>
<td>(2 points)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>at the top of Part 3 for IP address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set encapsulation to <strong>PPP</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the clocking rate to <strong>128000</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
</tbody>
</table>
| **Configure CHAP authentication on S0/0/0.** | Username: **R2**  
Password: **cisco**                                                 | (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.
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| 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:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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.
Configure S0/0/0.

Task Specification | IOS Commands
--- | ---
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.

Task Specification | IOS Commands
--- | ---
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.

Task Specification | IOS Commands
--- | ---
username R1 password cisco | R2# show run | section user (Verify that configuration line: username R1 password 702050D480809 is listed.)

Configure S0/0/1.

Task Specification | IOS Commands
--- | ---
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.

Task Specification | IOS Commands
--- | ---
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.

Task Specification | IOS Commands
--- | ---
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/1.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

---

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.
Configure S0/0/1.

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface s0/0/1 description PPP connection to ISP</td>
<td>R3# show run interface s0/0/1 (Verify configuration.)</td>
</tr>
<tr>
<td></td>
<td>ip address 209.165.200.230 255.255.255.248 encapsulation ppp</td>
<td>R3# show ip interface brief (Verify that the interface is active.)</td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

Step 4: Verify network connectivity.

Verify connectivity using the ping command.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-B</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>R3 G0/1</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>R2 S0/0/1</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>PC-B</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a static NAT to map the inside local IP address for PC-B to a Inside Global address.</td>
<td>Inside Global: <strong>209.165.200.226</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define an access control list to permit the R1 LAN for dynamic NAT.</td>
<td>Access List: 1</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define the dynamic NAT pool for the R1 LAN.</td>
<td>Pool: <strong>R1-LAN</strong></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>
| 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**            | (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) |
<p>| 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) |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign the static NAT address 209.165.200.226 to map to the IP address for PC-B.</td>
<td>ip nat inside source static 192.168.22.3 209.165.200.226</td>
<td>R2# show run</td>
</tr>
<tr>
<td>Define an access control list to permit the R1 LAN for dynamic NAT.</td>
<td>access-list 1 permit 192.168.11.0 0.0.0.255</td>
<td>R2# show access-lists (Verify the command in the Specification box is listed.)</td>
</tr>
<tr>
<td>Define the dynamic NAT pool for the R1 LAN.</td>
<td>ip nat pool R1-LAN 209.165.200.227 209.165.200.227 netmask 255.255.255.248</td>
<td>R2# show run</td>
</tr>
<tr>
<td>Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address.</td>
<td>ip nat inside source list 1 pool R1-LAN overload</td>
<td>R2# show run</td>
</tr>
<tr>
<td>Define an access control list to permit the R2 LAN for dynamic NAT.</td>
<td>access-list 2 permit 192.168.22.0 0.0.0.255</td>
<td>R2# show access-lists (Verify the command in the Specification box is listed.)</td>
</tr>
<tr>
<td>Define the dynamic NAT pool for the R2 LAN.</td>
<td>ip nat pool R2-LAN 209.165.200.228 209.165.200.228 netmask 255.255.255.248</td>
<td>R2# show run</td>
</tr>
<tr>
<td>Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address.</td>
<td>ip nat inside source list 2 pool R2-LAN overload</td>
<td>R2# show run</td>
</tr>
<tr>
<td>Assign the outside NAT interface.</td>
<td>interface s0/0/1 ip nat outside</td>
<td>R2# show run interface s0/0/1 (Verify the command in the Specification box is listed.)</td>
</tr>
<tr>
<td>Assign the inside NAT interface for the R1 LAN.</td>
<td>interface s0/0/0 ip nat inside</td>
<td>R2# show run interface s0/0/0 (Verify the command in the Specification box is listed.)</td>
</tr>
<tr>
<td>Assign the inside NAT interface for the R2 LAN.</td>
<td>interface g0/0 ip nat inside</td>
<td>R2# show run interface g0/0 (Verify the command in the Specification box is listed.)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configured access lists.</td>
<td>show access-lists</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the current active NAT translations.</td>
<td>show ip nat translations</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display detailed information about NAT including interface, access list, and pool assignments.</td>
<td>show ip nat statistics</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the timestamp service on R1 and R2 for system logging purposes.</td>
<td>Include milliseconds in the timestamp.</td>
<td>(1 points)</td>
</tr>
<tr>
<td>Enable logging of messages on R1 and R2.</td>
<td>Syslog server: <strong>192.168.11.3</strong></td>
<td>(1 points)</td>
</tr>
<tr>
<td>Change message trapping level on R1 and R2.</td>
<td>Level: <strong>debugging</strong> (severity 7)</td>
<td>(1 points)</td>
</tr>
</tbody>
</table>
### Task Specification

#### Enable the timestamp service on R1 and R2 for system logging purposes.

- **Service**
  - `service timestamps log datetime msec`

- **Verification**
  - `R1# show run | include service`
  - `R2# show run | include service`

#### Enable logging of messages on R1 and R2.

- **Service**
  - `logging host 192.168.11.3`

- **Verification**
  - `R1# show run | include logging`
  - `R2# show run | include logging`

#### Change message trapping level on R1 and R2.

- **Service**
  - `logging trap debugging`

- **Verification**
  - `R1# show run | include logging`
  - `R2# show run | include logging`

### Step 3: Configure SNMP on R1.

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a standard access list to permit the SNMP management station (PC-A) to retrieve SNMP information from R1.</td>
<td>Access List: <strong>SNMP-ACCESS</strong></td>
<td>(1 points)</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a standard access list to permit PC-A to retrieve SNMP information from R1.</td>
<td>ip access-list standard SNMP-ACCESS permit 192.168.11.3</td>
<td>R1# show run</td>
</tr>
<tr>
<td>Enable SNMP community access to the SNMP-ACCESS access list.</td>
<td>snmp-server community SA-LAB ro SNMP-ACCESS</td>
<td>R1# show run</td>
</tr>
<tr>
<td>Set the SNMP notification host.</td>
<td>snmp-server host 192.168.11.3 version 2c SA-LAB</td>
<td>R1# show snmp host (Look for: Notification host: 192.168.11.3 udp-port: 162 type: trap user: SA-LAB security model: v2c.)</td>
</tr>
<tr>
<td>Enable all SNMP traps.</td>
<td>snmp-server enable traps</td>
<td>R1# show run</td>
</tr>
</tbody>
</table>

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

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure NetFlow data capture on both serial interfaces. Capture ingress and egress data packets.</td>
<td></td>
<td>(1 points)</td>
</tr>
<tr>
<td>Configure NetFlow data export.</td>
<td>Destination: <strong>PC-B IP address</strong> UDP Port: <strong>9996</strong></td>
<td>(1 points)</td>
</tr>
<tr>
<td>Configure the NetFlow export version.</td>
<td>Version: <strong>9</strong></td>
<td>(1 points)</td>
</tr>
</tbody>
</table>
### Task Specification IOS Commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the date and time.</td>
<td>show clock</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Display the contents of logging buffers.</td>
<td>show logging</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display information about the SNMP communities.</td>
<td>show snmp community</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Display the protocol using the highest volume of traffic.</td>
<td>show ip cache flow</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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**
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:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/0.</td>
<td>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 <strong>frame-relay</strong> Set the clocking rate to 128000</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Disable Inverse ARP on S0/0/0.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Map the IP local address to the DLCI.</td>
<td>Refer to Figure 2 for DLCI information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Map the remote IP address to the DLCI. Allow for multicast or broadcast traffic.</td>
<td>Refer to Figure 2 for IP address and DLCI information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Change the LMI type to the ANSI standard.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Activate the interface.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Create a default route to the IP address on the other side of the Frame Relay link.</td>
<td>Refer to Figure 2 for the IP address.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Instructor Note:** Ask the student to connect to R1, and then verify the proper configuration.
### Task Specification IOS Commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| 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.    | 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:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/1.</td>
<td>Configure Frame Relay Encapsulation. Set encapsulation to frame-relay (use the IETF standard). Activate the interface.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Create a point-to-point subinterface on S0/0/1.</td>
<td>Subinterface #: 321 Set the description.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Set the Layer 3 IPv4 address on the subinterface.</td>
<td>Refer to Figure 2 at the top of Part 6 for IP address information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable Inverse ARP on the subinterface.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Map the subinterface to the DLCI.</td>
<td>Refer to Figure 2 for DLCI information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Create a default route to the IP address on the other side of the Frame Relay link.</td>
<td>Refer to Figure 2 for IP address.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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

**Step 5: Verify network connectivity.**

Verify connectivity using the **ping** command.
### Step 6: Verify Frame Relay configuration.

Enter the appropriate CLI command needed to display the following:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Frame Relay LMI statistics.</td>
<td>show frame-relay lmi</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the input and output packet count totals on a Frame Relay permanent virtual circuit (PVC).</td>
<td>Show frame-relay pvc</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the Frame Relay maps between DLCIs and IP addresses.</td>
<td>show frame-relay map</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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
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:

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

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

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

b. Configuration tasks for R2 include the following:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/0.</td>
<td>Set the description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation to <strong>HDLC</strong>.</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
<tr>
<td>Configure S0/0/1.</td>
<td>Set the description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation to <strong>HDLC</strong>.</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the clocking rate to <strong>128000</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| Configure S0/0/0.  | `interface s0/0/0`<br>description HDLC connection to R1<br>ip address 172.27.12.2 255.255.255.252<br>encapsulation hdlc<br>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`<br>description HDLC connection to R3.<br>ip address 172.27.23.2 255.255.255.252<br>encapsulation hdlc<br>clock rate 128000<br>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:**

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/1.</td>
<td>Set the description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation to <strong>HDLC</strong>.</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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.
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel 0 description GRE VPN tunnel to R1 ip address 172.27.13.2 255.255.255.252</td>
<td>R3# show run interface tunnel 0 (Verify configuration.)</td>
</tr>
</tbody>
</table>

**Use S0/0/0 as the tunnel source.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel source s0/0/1</td>
<td>R3# show run interface tunnel 0 (Verify configuration.)</td>
</tr>
</tbody>
</table>

**Set the tunnel destination with the IP address of the R3 S0/0/1 interface.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel destination 172.27.12.1</td>
<td>R3# show run interface tunnel 0 (Verify configuration.)</td>
</tr>
</tbody>
</table>

**Create a default route out S0/0/1.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route 0.0.0.0 0.0.0.0 s0/0/1</td>
<td>R3# show ip route (Verify that the static route is in the routing table.)</td>
</tr>
</tbody>
</table>

**Configure EIGRP on R1.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>router eigrp 1</td>
<td>R3# show run</td>
</tr>
</tbody>
</table>

**Advertise the LAN and Tunnel subnets in EIGRP. Set the LAN interface to passive.**

<table>
<thead>
<tr>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>network 10.10.33.0 0.0.0.255 network 172.27.13.0 0.0.0.3 passive-interface g0/0</td>
<td>R3# show run</td>
</tr>
</tbody>
</table>

### Step 5: Verify network connectivity.

Verify connectivity using the following commands.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>R1</td>
<td>traceroute</td>
<td>172.27.23.1</td>
<td>R2 should show up in the traceroute.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>R1</td>
<td>traceroute</td>
<td>172.27.13.2</td>
<td>R2 should be absent from traceroute.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display detail information about the GRE tunnel interface.</td>
<td>show interfaces tunnel 0</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2801</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/1/0 (S0/1/0)</td>
<td>Serial 0/1/1 (S0/1/1)</td>
</tr>
<tr>
<td>2811</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

**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.

---

### Device Configs

**Router R1 (After Part 2 - BasicConfig)**

```bash
R1#show run
Building configuration...

Current configuration : 1547 bytes

# version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
#
hostname R1
```
boot-start-marker

boot-end-marker

! 

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

no aaa new-model

memory-size iomem 15

ip cef

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

interface Embedded-Service-Engine0/0

no ip address

shutdown

interface GigabitEthernet0/0

description Connection to the 192.168.11.0 LAN

ip address 192.168.11.1 255.255.255.0

duplex auto

speed auto

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

interface Serial0/0/1

no ip address

shutdown

ip forward-protocol nd

no ip http server

no ip http secure-server

control-plane

banner motd ^C Unauthorized Access is Prohibited! ^C
line con 0
  password 7 045802150C2E
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 1511021F0725
  login
  transport input all
  scheduler allocate 20000 1000
end

Router R2 (After Part 2 - BasicConfig)

R2#show run
Building configuration...

Current configuration : 1487 bytes

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

hostname R2

boot-start-marker
boot-end-marker

enable secret 4 06YFDUHH61wAE/klKd9Bgho1QM5EnRtoyr8cHAUg.2

no aaa new-model
memory-size iomem 15

ip cef

no ip domain lookup
no ipv6 cef

multilink bundle-name authenticated
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  description Connection to the 192.168.22.0 LAN
  ip address 192.168.22.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 1511021F0725
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 094F471A1A0A
  login
  transport input all
! scheduler allocate 20000 1000
!
end

Router R3 (After Part 2 - BasicConfig)

R3#show run
Building configuration...

Current configuration : 1522 bytes

! version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  description Connection to the 10.10.33.0 LAN
  ip address 10.10.33.1 255.255.255.0
duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000

! interface Serial0/0/1
  no ip address
  shutdown
  ip forward-protocol nd
  no ip http server
  no ip http secure-server
  control-plane
  banner motd ^C Unauthorized Access is Prohibited! ^C

! line con 0
  password 7 030752180500
  login
  line aux 0
  line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
  line vty 0 4
  password 7 030752180500
  login
  transport input all
  scheduler allocate 20000 1000

end

Router R1 (After Part 5)

R1#show run
Building configuration...

Current configuration : 6286 bytes

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
username R2 password 7 110A1016141D
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
  description Connection to the 192.168.11.0 LAN
  ip address 192.168.11.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/0/0
  description Connection to R2
  ip address 172.27.12.1 255.255.255.252
  encapsulation ppp
  ppp authentication chap
clock rate 128000
!
interface Serial0/0/1
no ip address
  shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip access-list standard SNMP-ACCESS
 ip permit 192.168.11.3
!
logging trap debugging
logging host 192.168.11.3
!
!
snmp-server community SA-LAB RO SNMP-ACCESS
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps dsl
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eligrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps c3g
snmp-server enable traps entity-sensor threshold
snmp-server enable traps adslline
snmp-server enable traps vds12line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps dsl1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp cbgp2
snmp-server enable traps isis
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps waas
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps firewall serverstatus
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.11.3 version 2c SA-LAB
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 045802150C2E
login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
  password 7 1511021F0725
login
  transport input all
!
scheduler allocate 20000 1000
ntp server 172.27.12.2
!
end

Router R2 (After Part 5)

R2#show run
Building configuration...

Current configuration : 2488 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

hostname R2

boot-start-marker
boot-end-marker

enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2

no aaa new-model
memory-size lomem 15

ip cef

no ip domain lookup
no ipv6 cef

multilink bundle-name authenticated

username R1 password 7 104D000A0618

interface Embedded-Service-Engine0/0
no ip address
shutdown

interface GigabitEthernet0/0
  description Connection to the 192.168.22.0 LAN
  ip address 192.168.22.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
duplex auto
  speed auto

interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
  speed auto

interface Serial0/0/0
  description PPP connection to R1
  ip address 172.27.12.2 255.255.255.252
  ip flow ingress
  ip flow egress
  ip nat inside
  ip virtual-reassembly in
encapsulation ppp
ppp authentication chap
!
interface Serial0/0/1
description PPP connection to ISP
ip address 209.165.200.225 255.255.255.248
ip flow ingress
ip flow egress
ip nat outside
ip virtual-reassembly in
encapsulation ppp
clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip flow-export version 9
ip flow-export destination 192.168.22.3 9996
!
ip nat pool R1-LAN 209.165.200.227 209.165.200.227 netmask 255.255.255.248
ip nat pool R2-LAN 209.165.200.228 209.165.200.228 netmask 255.255.255.248
ip nat inside source list 1 pool R1-LAN overload
ip nat inside source list 2 pool R2-LAN overload
ip nat inside source static 192.168.22.3 209.165.200.226
ip route 0.0.0.0 0.0.0.0 0.0.0.0 Serial0/0/1
ip route 192.168.11.0 255.255.255.0 Serial0/0/0
!
logging trap debugging
logging host 192.168.11.3
access-list 1 permit 192.168.11.0 0.0.0.255
access-list 2 permit 192.168.22.0 0.0.0.255
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 1511021F0725
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
Router R3 (After Part 5)

R3#show run
Building configuration...

Current configuration : 1595 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to the 10.10.33.0 LAN
ip address 10.10.33.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
```
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
description PPP connection to ISP
ip address 209.165.200.230 255.255.255.248
encapsulation ppp
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 030752180500
login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 030752180500
  login
  transport input all
!
scheduler allocate 20000 1000
!
end

Router R1 (After Part 6)
R1# show run
Building configuration...

Current configuration : 1875 bytes
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDg9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  description Connection to the 192.168.11.0 LAN
  ip address 192.168.11.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  description Frame Relay connection to R3.
  ip address 172.27.13.1 255.255.255.252
  encapsulation frame-relay
  clock rate 128000
  frame-relay map ip 172.27.13.2 123 broadcast
  frame-relay map ip 172.27.13.1 123
  no frame-relay inverse-arp
  frame-relay lmi-type ansi
!
interface Serial0/0/1
no ip address
shutdown
!
router eigrp 1
   network 172.27.13.0 0.0.0.3
   network 192.168.11.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.27.13.2
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
   password 7 045802150C2E
   login
line aux 0
line 2
   no activation-character
   no exec
   transport preferred none
   transport input all
   transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
   stopbits 1
line vty 0 4
   password 7 1511021F0725
   login
   transport input all
!
scheduler allocate 20000 1000
!
end

**Router R2 (After Part 6)**

R2#show run
Building configuration...

Current configuration : 1726 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
frame-relay switching
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
  description Connection to the 192.168.22.0 LAN
  ip address 192.168.22.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay intf-type dce
frame-relay route 123 interface Serial0/0/1 321
!
interface Serial0/0/1
no ip address
encapsulation frame-relay IETF
clock rate 128000
frame-relay intf-type dce
frame-relay route 321 interface Serial0/0/0 123
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
    password 7 1511021F0725
    login
line aux 0
line 2
    no activation-character
    no exec
    transport preferred none
    transport input all
    transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
    stopbits 1
line vty 0 4
    password 7 094F471A1A0A
    login
    transport input all
!
scheduler allocate 20000 1000
!
end

Router R3 (After Part 6)

R3#show run
Building configuration...

Current configuration : 1741 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to the 10.10.33.0 LAN
ip address 10.10.33.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
encapsulation frame-relay IETF
!
interface Serial0/0/1.321 point-to-point
description Frame Relay connection to R1
ip address 172.27.13.2 255.255.255.252
frame-relay interface-dlci 321
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.27.13.1
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
line con 0
  password 7 030752180500
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 030752180500
  login
  transport input all

! scheduler allocate 20000 1000
!
end

**Router R1 (After Part 7)**

R1#show run
Building configuration...

Current configuration : 1787 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Tunnel0
description GRE VPN tunnel to R3
ip address 172.27.13.1 255.255.255.252
tunnel source Serial0/0/0
tunnel destination 172.27.23.1
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
description Connection to the 192.168.11.0 LAN
  ip address 192.168.11.1 255.255.255.0
duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/0/0
description HDLC connection to ISP
  ip address 172.27.12.1 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
  no ip address
  shutdown
!
!
router eigrp 1
  network 172.27.13.0 0.0.0.3
  network 192.168.11.0
  passive-interface GigabitEthernet0/0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 045802150C2E
login
line aux 0
line 2
   no activation-character
   no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 sah
stopbits 1
line vty 0 4
   password 7 1511021F0725
login
   transport input all
!
scheduler allocate 20000 1000
!
end

Router R2 (After Part 7)
R2#show run
Building configuration...

Current configuration : 1596 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
   no ip address
   shutdown
```
!
interface GigabitEthernet0/0
    description Connection to the 192.168.22.0 LAN
    ip address 192.168.22.1 255.255.255.0
    shutdown
duplex auto
    speed auto
!
interface GigabitEthernet0/1
    no ip address
    shutdown
duplex auto
speed auto
!
interface Serial0/0/0
    description HDLC connection to R1
    ip address 172.27.12.2 255.255.255.252
!
interface Serial0/0/1
    description HDLC connection to R3
    ip address 172.27.23.2 255.255.255.252
clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
    password 7 1511021F0725
    login
line aux 0
line 2
    no activation-character
    no exec
    transport preferred none
    transport input all
    transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
    stopbits 1
line vty 0 4
    password 7 094F471A1A0A
    login
    transport input all
!
scheduler allocate 20000 1000
```
Router R3 (After Part 7)

R3#show run
Building configuration...

Current configuration : 1759 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUH61wAE/kLkDq9BGholQM5EnRtoyr8cHAg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Tunnel0
  description GRE tunnel to R1
  ip address 172.27.13.2 255.255.255.252
  tunnel source Serial0/0/1
  tunnel destination 172.27.12.1
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  description Connection to the 10.10.33.0 LAN
  ip address 10.10.33.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
clock rate 2000000
!
interface Serial0/0/1
  description HDLC connection to ISP
  ip address 172.27.23.1 255.255.255.252
!
router eigrp 1
  network 10.10.33.0 0.0.0.255
  network 172.27.13.0 0.0.0.3
  passive-interface GigabitEthernet0/0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 030752180500
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 030752180500
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
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.

<table>
<thead>
<tr>
<th>Task</th>
<th>IOS Command</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase the startup-config file on all routers.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Reload all routers.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static IPv4 address information on PC-A.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-B.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-C.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

Step 2: Configure R1.

Configuration tasks for R1 include the following:
### Configuration Item or Task Specification Points

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

### Step 3: Configure R2.

Configuration tasks for R2 include the following:

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

### 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**
Step 1: Configure R1.

Configuration tasks for R1 include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/0.</td>
<td>Set the description.</td>
<td>(2 points)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set encapsulation to PPP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the clocking rate to 128000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
<tr>
<td>Configure CHAP authentication on S0/0/0.</td>
<td>Username: R2</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Password: cisco</td>
<td></td>
</tr>
<tr>
<td>Create a local database entry for CHAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set a static default route out S0/0/0.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

Step 2: Configure R2.

Configuration tasks for R2 include the following:
### Task Specification Points

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

### Step 3: Configure R3.

Configuration tasks for R3 include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/1.</td>
<td>Set the description.</td>
<td>(2 points)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 1 at the top of Part 3 for IP address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation to <strong>PPP</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4: Verify network connectivity.

Verify connectivity using the **ping** command.
Part 3: From Command To Expected Results Points

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-B</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>R3 G0/1</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>R2 S0/0/1</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>PC-B</td>
<td>Ping should not be successful.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a static NAT to map the inside local IP address for PC-B to a Inside Global address.</td>
<td>Inside Global: 209.165.200.226</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define an access control list to permit the R1 LAN for dynamic NAT.</td>
<td>Access List: 1</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define the dynamic NAT pool for the R1 LAN.</td>
<td>Pool: R1-LAN Inside Global: 209.165.200.227</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address.</td>
<td>Inside source: Access list 1 Outside pool: R1-LAN</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define an access control list to permit the R2 LAN for dynamic NAT.</td>
<td>Access List: 2</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define the dynamic NAT pool for the R2 LAN.</td>
<td>Pool: R2-LAN Inside Global: 209.165.200.228</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Define the NAT from the inside source to the outside pool. Make sure to allow multiple PCs access to this single Inside Global address.</td>
<td>Inside source: Access list 2 Outside pool: R2-LAN</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Assign the outside NAT interface.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Assign the inside NAT interface for the R1 LAN.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Assign the inside NAT interface for the R2 LAN.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>
Step 2:  Verify network connectivity.

Verify connectivity using the ping command.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>Inside Global address for PC-B (209.165.200.226).</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configured access lists.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the current active NAT translations.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display detailed information about NAT including interface, access list, and pool assignments.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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:
Table 1: Task Specification Points

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the timestamp service on R1 and R2 for system logging purposes.</td>
<td>Include milliseconds in the timestamp.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Enable logging of messages on R1 and R2.</td>
<td>Syslog server: <strong>192.168.11.3</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Change message trapping level on R1 and R2.</td>
<td>Level: <strong>debugging</strong> (severity 7)</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a standard access list to permit the SNMP management station (PC-A) to retrieve SNMP information from R1.</td>
<td>Access List: <strong>SNMP-ACCESS</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Enable SNMP community access to the SNMP-ACCESS access list.</td>
<td>Community: <strong>SA-LAB</strong>&lt;br&gt;Access level: <strong>Read-only</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Set the SNMP notification host.</td>
<td>Host: <strong>192.168.11.3</strong>&lt;br&gt;Version: <strong>2c</strong>&lt;br&gt;Community: <strong>SA-LAB</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Enable all SNMP traps.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure NetFlow data capture on both serial interfaces. Capture ingress and egress data packets.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Configure NetFlow data export.</td>
<td>Destination: <strong>PC-B IP address</strong>&lt;br&gt;UDP Port: <strong>9996</strong></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Configure the NetFlow export version.</td>
<td>Version: <strong>9</strong></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/0.</td>
<td>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 <strong>frame-relay</strong></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Disable Inverse ARP on S0/0/0.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Map the IP local address to the DLCI.</td>
<td>Refer to Figure 2 for DLCI information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Map the remote IP address to the DLCI.</td>
<td>Allow for multicast or broadcast traffic. Refer to Figure 2 for IP address and DLCI information.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Change the LMI type to the ANSI standard.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Activate the interface.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Create a default route to the IP address on the other side of the Frame Relay link.</td>
<td>Refer to Figure 2 for the IP address.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

Step 4: Configure R3.

Configure Frame Relay on a subinterface of S0/0/1 on R3. Configuration tasks for R3 include the following:
<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure S0/0/1.</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>
|      | Configure Frame Relay Encapsulation. Set encapsulation to **frame-relay** (use the IETF standard).  
|      | Activate the interface.                                                       |        |
|      | Create a point-to-point subinterface on S0/0/1.                              |        |
|      | Subinterface #: **321**                                                       | (1 point) |
|      | Set the description.                                                         |        |
|      | Set the Layer 3 IPv4 address on the subinterface.                             | (1 point) |
|      | Refer to Figure 2 at the top of Part 6 for IP address information.           |        |
|      | Disable Inverse ARP on the subinterface.                                     | (1/2 point) |
|      | Map the subinterface to the DLCI.                                            | (1 point) |
|      | Refer to Figure 2 for DLCI information.                                      |        |
|      | Create a default route to the IP address on the other side of the Frame Relay link. | (1/2 point) |
|      | Refer to Figure 2 for IP address.                                            |        |

**Step 5: Verify network connectivity.**

Verify connectivity using the **ping** command.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>172.27.13.2</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>172.27.13.1</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Frame Relay LMI statistics.</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the input and output packet count totals on a Frame Relay permanent virtual circuit (PVC).</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>Display the Frame Relay maps between DLCIs and IP addresses.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure S0/0/0.</td>
<td>Set the description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to Figure 3 at the top of Part 7 for IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation to <strong>HDLC</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the clocking rate to <strong>128000</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate the interface.</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-C</td>
<td>ping</td>
<td>Default gateway</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>R1</td>
<td>traceroute</td>
<td>172.27.23.1</td>
<td>R2 should show up in the traceroute.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>R1</td>
<td>traceroute</td>
<td>172.27.13.2</td>
<td>R2 should be absent from traceroute.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Student Input (command)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display detail information about the GRE tunnel interface.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2801</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/1/0 (S0/1/0)</td>
<td>Serial 0/1/1 (S0/1/1)</td>
</tr>
<tr>
<td>2811</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

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

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

# 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)

**Part 2: Configure Device Basic Settings**

**Total points:** 45  
**Time:** 30 minutes

**Step 1: Configure R1.**

Configuration tasks for R1 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R1</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description</td>
<td>(1 points)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set a clocking rate of 128000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 1 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 2 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 3 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Instructor Note:** Ask the student to connect to R1, and then verify the proper configuration.
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td>no ip domain lookup</td>
<td>R1# show run (Look for: no ip domain lookup)</td>
</tr>
<tr>
<td>Router name</td>
<td>hostname R1</td>
<td>(Look for: R1&gt; or R1# command prompt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>enable secret class</td>
<td>R1&gt; enable (Type in privileged exec password)</td>
</tr>
<tr>
<td>Console access password</td>
<td>line con 0 password cisco login</td>
<td>R1# exit (Type in access password)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>line vty 0 4 password cisco login</td>
<td>R1# show run (Look under line VTY 0 4 for: password 7 121A0C041104)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td>service password-encryption</td>
<td>R1# show run (Look for: service password-encryption)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>banner motd @ Unauthorized Access is Prohibited! @</td>
<td>(Verify banner during above step)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>interface g0/1 description Connection to S1 ip address 172.27.0.1 255.255.255.0 no shutdown</td>
<td>R1# show ip interface G0/1 (Look for IP address and correct subnet mask)</td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>interface s0/0/0 description Connection to R2 ip add 172.27.123.1 255.255.255.252 clock rate 128000 no shutdown</td>
<td>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)</td>
</tr>
<tr>
<td>Interface Loopback 1</td>
<td>interface lo1 ip address 172.27.1.1 255.255.255.0</td>
<td>R1# show ip interface lo1 (Look for IP address and correct subnet mask)</td>
</tr>
<tr>
<td>Interface Loopback 2</td>
<td>interface lo2 ip address 172.27.2.1 255.255.255.0</td>
<td>R1# show ip interface lo2 (Look for IP address and correct subnet mask)</td>
</tr>
<tr>
<td>Interface Loopback 3</td>
<td>interface lo3 ip address 172.27.3.1 255.255.255.0</td>
<td>R1# show ip interface lo3 (Look for IP address and correct subnet mask)</td>
</tr>
</tbody>
</table>

**Step 2:** Configure R2.
Configuration tasks for R2 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set a clocking rate of 128000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 0 (Simulated Internet</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td>connection)</td>
<td>Set the Layer 3 IPv4 address to 209.165.200.225/29.</td>
<td></td>
</tr>
<tr>
<td>Default route</td>
<td>Configure a default route out Lo0.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Instructor Note:** Ask the student to connect to R2, and then verify the proper configuration.
Step 3: Configure R3.

Configuration tasks for R3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td>no ip domain lookup</td>
<td>R2# show run (Look for: no ip domain lookup)</td>
</tr>
<tr>
<td>Router name</td>
<td>hostname R2</td>
<td>(Look for : R2&gt; or R2# command prompt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>enable secret class</td>
<td>R2&gt; enable (Type in privileged exec password)</td>
</tr>
<tr>
<td>Console access password</td>
<td>line con 0 password cisco login</td>
<td>R2# exit (Type in access password)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>line vty 0 4 password cisco login</td>
<td>R2# show run (Look under line VTY 0 4 for: password 7 121A0C041104)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td>service password-encryption</td>
<td>R2# show run (Look for: service password-encryption)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>banner motd @ Unauthorized Access is Prohibited! @</td>
<td>(Verify banner during above step)</td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>interface s0/0/0 description Connection to R1 ip add 172.27.123.2 255.255.255.252 no shutdown</td>
<td>R2# show interface S0/0/0 (Look for Description, Internet address, and verify that interface is not administratively down.)</td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>interface s0/0/1 description Connection to R3 ip add 172.27.123.5 255.255.255.252 clock rate 128000 no shutdown</td>
<td>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)</td>
</tr>
<tr>
<td>Interface Loopback 0 (Simulated Internet connection)</td>
<td>description Connection to Internet ip address 209.165.200.225 255.255.255.248</td>
<td>R2# show run interface lo0 (Verify description, IP address, and subnet mask)</td>
</tr>
<tr>
<td>Default route</td>
<td>ip route 0.0.0.0 0.0.0.0 lo0</td>
<td>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)</td>
</tr>
<tr>
<td>Configuration Item or Task</td>
<td>Specification</td>
<td>Points</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

| Interface G0/1                                  | Set the description                                                         | (1 point)       |
|                                                 | Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. |                |
|                                                 | Activate Interface                                                          |                |

| Interface S0/0/1                                 | Set the description                                                         | (1 point)       |
|                                                 | Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. |                |
|                                                 | Activate Interface                                                          |                |

| 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.
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td>no ip domain lookup</td>
<td>R3# show run (Look for: <code>no ip domain lookup</code>)</td>
</tr>
<tr>
<td>Router name</td>
<td>hostname R3</td>
<td>(Look for: <code>R3&gt;</code> or <code>R3#</code> command prompt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>enable secret class</td>
<td>R3# enable (Type in privileged exec password)</td>
</tr>
<tr>
<td>Console access password</td>
<td>line con 0 password cisco login</td>
<td>R3# exit (Type in access password)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>line vty 0 4 password cisco login</td>
<td>R3# show run (Look under line VTY 0 4 for: <code>password 7 121A0C041104</code>)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td>service password-encryption</td>
<td>R3# show run (Look for: <code>service password-encryption</code>)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>banner motd @ Unauthorized Access is Prohibited! @</td>
<td>(Verify banner during above step)</td>
</tr>
</tbody>
</table>

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

Configuration tasks for S2 include the following:

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

**Instructor Note:** Ask the student to connect to S2, and then verify the proper configuration.
<table>
<thead>
<tr>
<th><strong>Configuration Item or Task</strong></th>
<th><strong>Specification</strong></th>
<th><strong>IOS Commands</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td>no ip domain lookup</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Look for: no ip domain lookup)</td>
</tr>
<tr>
<td>Switch name</td>
<td>hostname S2</td>
<td>(Look for: S2&gt; or S2# command prompt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>enable secret class</td>
<td>S2&gt; enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Type in privileged exec password)</td>
</tr>
<tr>
<td>Console access password</td>
<td>line con 0</td>
<td>S2# exit</td>
</tr>
<tr>
<td></td>
<td>password cisco</td>
<td>(Type in access password)</td>
</tr>
<tr>
<td></td>
<td>login</td>
<td></td>
</tr>
<tr>
<td>Telnet access password</td>
<td>line vty 0 15</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td>password cisco</td>
<td>(Look under line VTY 0 15 for: password 7 121A0C041104)</td>
</tr>
<tr>
<td></td>
<td>login</td>
<td></td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td>service password-encryption</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Look for: service password-encryption)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>banner motd @ Unauthorized Access is Prohibited! @</td>
<td>(Verify banner during above step)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>interface vlan 1</td>
<td>S2# show ip interface vlan1</td>
</tr>
<tr>
<td></td>
<td>ip address 172.27.0.12 255.255.255.0</td>
<td>(Look for IP address and correct subnet mask)</td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>ip default-gateway 172.27.0.2</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Look for ip default-gateway 172.27.0.2)</td>
</tr>
<tr>
<td>Force trunking on all interfaces connected to S1 and S3.</td>
<td>interface range f0/1-4</td>
<td>S2# show interface trunk</td>
</tr>
<tr>
<td></td>
<td>switchport mode trunk</td>
<td>(Look to see if interfaces F0/1-4 are listed. If not listed check to see if interfaces are active.)</td>
</tr>
<tr>
<td></td>
<td>switchport trunk native vlan 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: VLAN 1 is the native VLAN by default, the previous command is not necessary.</td>
<td></td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>interface range f0/5-24, g0/1-2</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td>switchport mode access</td>
<td>(Look to see if these ports have been set as access switch ports.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The <strong>switchport nonegotiate</strong> command may have also been issued, this is not incorrect but it is important that these ports have been changed to access ports.</td>
<td></td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td>interface range f0/5-17, f0/19-24, g0/1-2</td>
<td>S2# show run</td>
</tr>
<tr>
<td></td>
<td>shutdown</td>
<td>(Verify that these ports are administratively shutdown.)</td>
</tr>
</tbody>
</table>
### Step 6: Configure S3

Configuration tasks for S3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S1 and S2.</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static IPv4 address information on PC-A</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-B</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-C</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Command</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as primary root bridge for VLAN 1.</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-A.</td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

### Configuration Item or Task Specification

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
</tr>
<tr>
<td>Configure as primary root bridge for VLAN 1.</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-A.</td>
</tr>
</tbody>
</table>

### IOS Commands

<table>
<thead>
<tr>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1# show spanning-tree summary (Verify that the switch is in rapid-pvst mode.)</td>
</tr>
<tr>
<td>S1# show spanning-tree (Verify that the switch is the root bridge for VLAN 1.)</td>
</tr>
<tr>
<td>S1# show run interface f0/6 (Verify that portfast and bpduguard have been enabled.)</td>
</tr>
</tbody>
</table>

### Step 2: Configure Spanning Tree on S2.

Configuration tasks for S2 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-B.</td>
</tr>
</tbody>
</table>

### Configuration Item or Task Specification

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-B</td>
</tr>
</tbody>
</table>

### IOS Commands

<table>
<thead>
<tr>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2# show spanning-tree summary (Verify that the switch is in rapid-pvst mode.)</td>
</tr>
<tr>
<td>S2# show run interface f0/18 (Verify that portfast and bpduguard have been enabled.)</td>
</tr>
</tbody>
</table>
Step 3: Configure Spanning Tree on S3.

Configuration tasks for S3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as secondary root bridge for VLAN 1.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-C.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+</td>
<td>spanning-tree mode rapid-pvst</td>
<td>S3# show spanning-tree summary (Verify that the switch is in rapid-pvst mode.)</td>
</tr>
<tr>
<td>Configure as secondary root bridge for VLAN 1.</td>
<td>spanning-tree vlan 1 root secondary</td>
<td>S3# show run</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-C</td>
<td>interface f0/18 spanning-tree portfast spanning-tree bpduguard enable</td>
<td>S3# show run interface f0/18 (Verify that portfast and bpduguard have been enabled.)</td>
</tr>
</tbody>
</table>

Step 4: Configure HSRP on R1.

Configuration tasks for R1 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the HSRP virtual IP address on interface G0/1.</td>
<td>Group: 1 Virtual IP address: 172.27.0.2</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Make this the primary HSRP router.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure so this router becomes the primary HSRP router on a reboot.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>
Step 5: Configure HSRP on R3.

Configuration tasks for R3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the HSRP virtual IP address on interface G0/1.</td>
<td>Group: 1</td>
<td>(2 points)</td>
</tr>
<tr>
<td></td>
<td>Virtual IP address: 172.27.0.2</td>
<td></td>
</tr>
</tbody>
</table>

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

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>On S1, configure an LACP EtherChannel on interfaces connected to S3.</td>
<td>Use group 1 and enable LACP unconditionally.</td>
<td>(2 points)</td>
</tr>
<tr>
<td>On S3, configure an LACP EtherChannel on interfaces connected to S1.</td>
<td>Use group 1 and enable LACP only if a LACP device is detected.</td>
<td>(2 points)</td>
</tr>
</tbody>
</table>
## Part 3: Configure EtherChannel

**Configuration Item or Task**
On S1, configure an LACP EtherChannel on interfaces connected to S3.

**Specification**
interface range f0/3-4 channel-group 1 mode active

**IOS Commands**
S1# show etherchannel summary
(Verify that group 1 is connected to interfaces f0/3 and f0/4, and that the status is SU.)

**Configuration Item or Task**
On S3, configure an LACP EtherChannel on interfaces connected to S1.

**Specification**
interface range f0/3-4 channel-group 1 mode passive

**IOS Commands**
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

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

**Instructor Note:** Ask the student to connect to R1, and then verify the proper configuration.
### Configuration Item or Task

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Process ID</td>
<td>router ospf 1</td>
<td>R1# show ip protocols (Look for: Routing Protocol is &quot;ospf 1&quot;)</td>
</tr>
<tr>
<td>Router ID</td>
<td>router-id 1.1.1.1</td>
<td>(From output from previous command, look for: Router-ID: 1.1.1.1)</td>
</tr>
<tr>
<td>Advertise directly connected networks.</td>
<td>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</td>
<td>R1# show run</td>
</tr>
<tr>
<td>Set all LAN interfaces as passive.</td>
<td>passive-interface g0/1 passive-interface lo1 passive-interface lo2 passive-interface lo3</td>
<td>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</td>
</tr>
<tr>
<td>Configure an inter-area summary route for the networks in area 1.</td>
<td>area 1 range 172.27.0.0 255.255.252.0</td>
<td>R1# show ip route ospf (Look for the OSPF route: O 172.27.0.0/22 is a summary, 00:01:01, Null0)</td>
</tr>
<tr>
<td>Change the default cost reference bandwidth to allow for Gigabit interfaces.</td>
<td>auto-cost reference-bandwidth 1000</td>
<td>R1# show run</td>
</tr>
<tr>
<td>Set the bandwidth on S0/0/0.</td>
<td>interface s0/0/0 bandwidth 128</td>
<td>R1# show interface s0/0/0 (Look for: BW 128 Kbit/sec.)</td>
</tr>
<tr>
<td>Adjust the metric cost of S0/0/0.</td>
<td>ip ospf cost 7500</td>
<td>R1# show ip ospf interface brief (Look for: Se0/0/0 1 0 172.27.123.1/30 7500 P2P 1/1)</td>
</tr>
<tr>
<td>Create an OSPF MD5 key on S0/0/0.</td>
<td>ip ospf message-digest-key 1 md5 CISCO</td>
<td>R1# show run interface s0/0/0 (Look for: ip ospf message-digest-key 1 md5 7 0802657D2A36)</td>
</tr>
<tr>
<td>Apply MD5 authentication to S0/0/0.</td>
<td>ip ospf authentication message-digest</td>
<td>R1# show run interface s0/0/0 (Look for: ip ospf authentication message-digest)</td>
</tr>
</tbody>
</table>

### Step 2: Configure OSPFv2 on R2.

Configuration tasks for R2 include the following:
### Configuration Item or Task

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

**Instructor Note:** Ask the student to connect to R2, and then verify the proper configuration.
### Configuration Item or Task

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
</table>
| 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 ospf  
(Look for: **auto-cost reference-bandwidth 1000**) |
| Set the bandwidth on all serial interfaces. | interface s0/0/0  
banner 128  
interface s0/0/1  
banner 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:  
S0/0/0 1 0 12.12.12.130 7500 P2P 1/1) |
| Create an OSPF MD5 key on the serial interfaces. | interface s0/0/0  
ip ospf md5  
im message digest 1 md5 CISCO  
interface s0/0/1  
ip ospf md5  
im message digest 1 md5 CISCO | R2# show run interface s0/0/0  
R2# show run interface s0/0/1  
(Look for:  
ip ospf message.digest 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 s0/0/0  
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:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Process ID</td>
<td>1</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Router ID</td>
<td>3.3.3.3</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Advertise directly connected networks.</td>
<td>Use classless network addresses Assign S0/0/1 and G0/1 interfaces to Area 0 Assign Loopback interfaces to Area 3</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Set all LAN interfaces as passive.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure an inter-area summary route for the networks in area 3.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Change the default cost reference bandwidth to support Gigabit interface calculations.</td>
<td>1000</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Set the serial interface bandwidth.</td>
<td>128 Kb/s</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Create an OSPF MD5 key on S0/0/1.</td>
<td>Key: 1 Password: CISCO</td>
<td>(2 points)</td>
</tr>
<tr>
<td>Apply MD5 authentication to S0/0/1.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

**Instructor Note**: Ask the student to connect to R3, and then verify the proper configuration.
### Configuration Item or Task

<table>
<thead>
<tr>
<th></th>
<th>Specification</th>
<th>IOS Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Process ID</td>
<td>router ospf 1</td>
<td>R3# show ip protocols (Look for: <strong>Routing Protocol is &quot;ospf 1&quot;</strong>)</td>
</tr>
<tr>
<td>Router ID</td>
<td>router-id 3.3.3.3</td>
<td>(From output from previous command, look for: <strong>Router-ID: 3.3.3.3</strong>)</td>
</tr>
<tr>
<td>Advertise directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected networks</td>
<td>network 172.27.0.0 0.0.0.255 area 0</td>
<td>R3# show run</td>
</tr>
<tr>
<td></td>
<td>network 172.27.123.4 0.0.0.3 area 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>network 172.27.4.0 0.0.0.255 area 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>network 172.27.5.0 0.0.0.255 area 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>network 172.27.6.0 0.0.0.255 area 3</td>
<td></td>
</tr>
<tr>
<td>Set all LAN (Loopback)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interfaces as passive.</td>
<td>passive-interface g0/1</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>passive-interface lo4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>passive-interface lo5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>passive-interface lo6</td>
<td></td>
</tr>
<tr>
<td>Configure an inter-</td>
<td>area 3 range 172.27.4.0</td>
<td>R3# show ip route ospf (Look for the OSPF route: <strong>O 172.27.4.0/22 is a summary, 00:01:01, Null0</strong>)</td>
</tr>
<tr>
<td>area summary route for</td>
<td>255.255.252.0</td>
<td></td>
</tr>
<tr>
<td>the networks in area 3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change the default</td>
<td>auto-cost reference-bandwidth 1000</td>
<td>R3# show run</td>
</tr>
<tr>
<td>cost reference bandwidth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to allow for Gigabit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interfaces.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the bandwidth on</td>
<td>interface s0/0/1</td>
<td>R3# show interface s0/0/1 (Look for: <strong>BW 128 Kbit/sec.</strong>)</td>
</tr>
<tr>
<td>S0/0/1.</td>
<td>bandwidth 128</td>
<td></td>
</tr>
<tr>
<td>Create an OSPF MD5</td>
<td>ip ospf message-digest-key 1 md5</td>
<td>R3# show run interface s0/0/1 (Look for: <strong>ip ospf message-digest-key 1 md5 7 0802657D2A36</strong>)</td>
</tr>
<tr>
<td>key on S0/0/1.</td>
<td>CISCO</td>
<td></td>
</tr>
<tr>
<td>Apply MD5</td>
<td>ip ospf authentication message-digest</td>
<td>R3# show run interface s0/0/0 (Look for: <strong>ip ospf authentication message-digest</strong>)</td>
</tr>
<tr>
<td>authentication to S0/0/1.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-A</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>Default Gateway</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>209.165.200.225</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>tracert</td>
<td>209.165.200.225</td>
<td>Trace should route through R1.</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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:
Part 5:  From Command To Expected Results Points

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>172.27.0.1</td>
<td>Ping should not be successful.</td>
<td>1 point</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>Default Gateway</td>
<td>Ping should be successful.</td>
<td>1 point</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>209.165.200.225</td>
<td>Ping should be successful.</td>
<td>1 point</td>
</tr>
<tr>
<td>PC-B</td>
<td>tracert</td>
<td>209.165.200.225</td>
<td>Trace should route through R3.</td>
<td>1 point</td>
</tr>
</tbody>
</table>

**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:

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

**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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2801</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/1/0 (S0/1/0)</td>
<td>Serial 0/1/1 (S0/0/1)</td>
</tr>
<tr>
<td>2811</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

**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.

## Device Configs

### Router R1 (Final)

```
R1# show run
Building configuration...

Current configuration : 2361 bytes

! version 15.2
! service timestamps debug datetime msec
! service timestamps log datetime msec
! service password-encryption
! hostname R1
!
! boot-start-marker
boot-end-marker
!
! enable secret 4 06YFDUHH61wAE/kLkDg9BGho1QM5EnRtoyr8cHAUg.z
!
! no aaa new-model
memory-size iomem 15
!
ip cef
!
```
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback1
ip address 172.27.1.1 255.255.255.0
!
interface Loopback2
ip address 172.27.2.1 255.255.255.0
!
interface Loopback3
ip address 172.27.3.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connection to S1
ip address 172.27.0.1 255.255.255.0
standby 1 ip 172.27.0.2
standby 1 priority 150
standby 1 preempt
duplex auto
speed auto
!
interface Serial0/0/0
description Connection to R2
bandwidth 128
ip address 172.27.123.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 106D202A2638
ip ospf cost 7500
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
router ospf 1
router-id 1.1.1.1
auto-cost reference-bandwidth 1000
area 1 range 172.27.0.0 255.255.252.0
passive-interface GigabitEthernet0/1
passive-interface Loopback1
passive-interface Loopback2
passive-interface Loopback3
network 172.27.0.0 0.0.0.255 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
network 172.27.123.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 070C285F4D06
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 14141B180F0B
  login
  transport input all
!
scheduler allocate 20000 1000
!
end

Router R2 (Final)

R2# show run
Building configuration...

Current configuration : 2056 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback0
   description Conneciton to Internet
   ip address 209.165.200.225 255.255.255.248
!
interface Embedded-Service-Engine0/0
   no ip address
   shutdown
!
interface GigabitEthernet0/0
   no ip address
   shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
   no ip address
   shutdown
duplex auto
speed auto
!
interface Serial0/0/0
   description Connection to R1
   bandwidth 128
   ip address 172.27.123.2 255.255.255.252
   ip ospf authentication message-digest
   ip ospf message-digest-key 1 md5 7 02252D682829
   ip ospf cost 7500
!
interface Serial0/0/1
   description Connection to R3
bandwidth 128
ip address 172.27.123.5 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 14343B382F2B
clock rate 128000
!
router ospf 1
  router-id 2.2.2.2
  auto-cost reference-bandwidth 1000
  network 172.27.123.0 0.0.0.3 area 0
  network 172.27.123.4 0.0.0.3 area 0
  default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 00071A150754
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 01100F175804
  login
  transport input all
!
scheduler allocate 20000 1000
!
end

Router R3 (Final)
R3# show run
Building configuration...

Current configuration : 2278 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback4
  ip address 172.27.4.1 255.255.255.0
!
interface Loopback5
  ip address 172.27.5.1 255.255.255.0
!
interface Loopback6
  ip address 172.27.6.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connection to S3
  ip address 172.27.0.3 255.255.255.0
  standby 1 ip 172.27.0.2
duplex auto
speed auto
interface Serial0/0/0
   no ip address
   shutdown
clock rate 2000000
!
interface Serial0/0/1
description Connection to R2
   bandwidth 128
   ip address 172.27.123.6 255.255.255.252
   ip ospf authentication message-digest
   ip ospf message-digest-key 1 md5 7 13263E212823
!
routing ospf 1
   router-id 3.3.3.3
   auto-cost reference-bandwidth 1000
   area 3 range 172.27.4.0 255.255.252.0
   passive-interface GigabitEthernet0/1
   passive-interface Loopback4
   passive-interface Loopback5
   passive-interface Loopback6
   network 172.27.0.0 0.0.0.255 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
   network 172.27.123.4 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
   password 7 121A0C041104
   login
line aux 0
line 2
   no activation-character
   no exec
   transport preferred none
   transport input all
   transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
   stopbits 1
line vty 0 4
   password 7 045802150C2E
   login
transport input all
! scheduler allocate 20000 1000
! end

**Switch S1 (Final)**

S1# show run
Building configuration...

Current configuration : 2599 bytes
! version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGo1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
!
vlan internal allocation policy ascending
!
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
interface FastEthernet0/3
  switchport mode trunk
  channel-group 1 mode active
interface FastEthernet0/4
  switchport mode trunk
  channel-group 1 mode active
!
interface FastEthernet0/5
  switchport mode access
!
interface FastEthernet0/6
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/7
  switchport mode access
  shutdown
!
interface FastEthernet0/8
  switchport mode access
  shutdown
!
interface FastEthernet0/9
  switchport mode access
  shutdown
!
interface FastEthernet0/10
  switchport mode access
  shutdown
!
interface FastEthernet0/11
  switchport mode access
  shutdown
!
interface FastEthernet0/12
  switchport mode access
  shutdown
!
interface FastEthernet0/13
  switchport mode access
  shutdown
!
interface FastEthernet0/14
  switchport mode access
  shutdown
!
interface FastEthernet0/15
  switchport mode access
  shutdown
!
interface FastEthernet0/16
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport mode access
shutdown
!
interface GigabitEthernet0/2
switchport mode access
shutdown
!
interface Vlan1
ip address 172.27.0.11 255.255.255.0
!
ip default-gateway 172.27.0.2
ip http server
ip http secure-server
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 030752180500
login
line vty 0 4
  password 7 030752180500
login
line vty 5 15
  password 7 030752180500
login
!
end

Switch S2 (Final)

S2# show run
Building configuration...

Current configuration : 2464 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
interface FastEthernet0/3
  switchport mode trunk

interface FastEthernet0/4
  switchport mode trunk

interface FastEthernet0/5
  switchport mode access
  shutdown

interface FastEthernet0/6
  switchport mode access
  shutdown

interface FastEthernet0/7
  switchport mode access
  shutdown

interface FastEthernet0/8
  switchport mode access
  shutdown

interface FastEthernet0/9
  switchport mode access
  shutdown

interface FastEthernet0/10
  switchport mode access
  shutdown

interface FastEthernet0/11
  switchport mode access
  shutdown

interface FastEthernet0/12
  switchport mode access
  shutdown

interface FastEthernet0/13
  switchport mode access
  shutdown

interface FastEthernet0/14
  switchport mode access
  shutdown

interface FastEthernet0/15
  switchport mode access
```plaintext
shutdown
!
interface FastEthernet0/16
    switchport mode access
    shutdown
!
interface FastEthernet0/17
    switchport mode access
    shutdown
!
interface FastEthernet0/18
    switchport mode access
    spanning-tree portfast
    spanning-tree bpduGuard enable
!
interface FastEthernet0/19
    switchport mode access
    shutdown
!
interface FastEthernet0/20
    switchport mode access
    shutdown
!
interface FastEthernet0/21
    switchport mode access
    shutdown
!
interface FastEthernet0/22
    switchport mode access
    shutdown
!
interface FastEthernet0/23
    switchport mode access
    shutdown
!
interface FastEthernet0/24
    switchport mode access
    shutdown
!
interface GigabitEthernet0/1
    switchport mode access
    shutdown
!
interface GigabitEthernet0/2
    switchport mode access
    shutdown
!
interface Vlan1
    ip address 172.27.0.12 255.255.255.0
```
Switch S3 (Final)

S3# show run
Building configuration...

Current configuration : 2599 bytes

! version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 28672
!
vlan internal allocation policy ascending
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
interface FastEthernet0/3
  switchport mode trunk
  channel-group 1 mode passive
!
interface FastEthernet0/4
  switchport mode trunk
  channel-group 1 mode passive
!
interface FastEthernet0/5
  switchport mode access
!
interface FastEthernet0/6
  switchport mode access
  shutdown
!
interface FastEthernet0/7
  switchport mode access
  shutdown
!
interface FastEthernet0/8
  switchport mode access
  shutdown
!
interface FastEthernet0/9
  switchport mode access
  shutdown
!
interface FastEthernet0/10
  switchport mode access
  shutdown
!
interface FastEthernet0/11
  switchport mode access
  shutdown
!
interface FastEthernet0/12
  switchport mode access
  shutdown
!
interface FastEthernet0/13
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport mode access
shutdown
!
interface GigabitEthernet0/2
    switchport mode access
    shutdown
!
interface Vlan1
    ip address 172.27.0.13 255.255.255.0
    !
    ip default-gateway 172.27.0.2
    ip http server
    ip http secure-server
    !
    banner motd ^C Unauthorized Access is Prohibited! ^C
    !
    line con 0
    password 7 030752180500
    login
    line vty 0 4
    password 7 030752180500
    login
    line vty 5 15
    password 7 030752180500
    login
    !
end
CCNA: Scaling Networks
Skills Assessment (OSPF) – Student Training Exam

Topology

![Topology Diagram]

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.
Addressing Table

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

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>IOS Command</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase the startup-config file on all routers.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Reload all routers.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Erase the startup-config file on all switches and remove the old VLAN database.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Reload all switches.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Verify VLAN database is absent from flash on all switches.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R1</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description</td>
<td>(1 points)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set a clocking rate of 128000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 1 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 2 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 3 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Step 2: Configure R2.**

Configuration tasks for R2 include the following:
Step 3: Configure R3.

Configuration tasks for R3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set a clocking rate of 128000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 0 (Simulated Internet connection)</td>
<td>Set the description.</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address to 209.165.200.225/29.</td>
<td></td>
</tr>
<tr>
<td>Default route</td>
<td>Configure a default route out Lo0.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>
### Configuration Item or Task

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 4 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 5 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 6 (LAN)</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

### Step 4: Configure S1.

Configuration tasks for S1 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S1</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S2 and S3.</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**Step 5: Configure S2.**

Configuration tasks for S2 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged exec password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the clear text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S1 and S3.</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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.**

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static IPv4 address information on PC-A</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-B</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-C</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as primary root bridge for VLAN 1.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-A.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

#### Step 2: Configure Spanning Tree on S2.

Configuration tasks for S2 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-B.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

#### Step 3: Configure Spanning Tree on S3.

Configuration tasks for S3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as secondary root bridge for VLAN 1.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-C.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

#### 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:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>On S1, configure an LACP EtherChannel on interfaces connected to S3.</td>
<td>Use group 1 and enable LACP unconditionally.</td>
<td>(2 points)</td>
</tr>
<tr>
<td>On S3, configure an LACP EtherChannel on interfaces connected to S1.</td>
<td>Use group 1 and enable LACP only if a LACP device is detected.</td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

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

**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:

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

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.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-A</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>Default Gateway</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>209.165.200.225</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>tracert</td>
<td>209.165.200.225</td>
<td>Trace should route through R1.</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>172.27.0.1</td>
<td>Ping should not be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>Default Gateway</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>209.165.200.225</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>tracert</td>
<td>209.165.200.225</td>
<td>Trace should route through R3.</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>What command displays the IOS image that is currently being used by the network device?</td>
<td>(1 point)</td>
<td></td>
</tr>
<tr>
<td>What command displays the size of an IOS image loaded on a network device?</td>
<td>(1 point)</td>
<td></td>
</tr>
<tr>
<td>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?</td>
<td>(1 point)</td>
<td></td>
</tr>
<tr>
<td>What command displays the amount of space available to install an additional IOS image to a network device?</td>
<td>(1 point)</td>
<td></td>
</tr>
<tr>
<td>What command displays a list of all the licenses on an ISR-G2 device?</td>
<td>(1 point)</td>
<td></td>
</tr>
<tr>
<td>What command would you use to accept the end user license agreement?</td>
<td>(1 point)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2801</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/1/0 (S0/1/0)</td>
<td>Serial 0/1/1 (S0/0/1)</td>
</tr>
<tr>
<td>2811</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

**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   Student: ___________________________ Date: __________

Skills Assessment (OSPF) – Student Training Exam

Score: ___________ (125)

Topology
### Addressing Table

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

### 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** (60 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>IOS Command</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase the startup-config file on all routers.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Reload all routers.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Erase the startup-config file on all switches and remove the old VLAN database.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Reload all switches.</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Verify VLAN database is absent from flash on all switches.</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Router name</td>
<td>R1</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>Set the description&lt;br&gt;Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.&lt;br&gt;Activate Interface</td>
<td>(1 pt)</td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description&lt;br&gt;Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.&lt;br&gt;Set a clocking rate of 128000.&lt;br&gt;Activate Interface</td>
<td>(1 pt)</td>
</tr>
<tr>
<td>Interface Loopback 1 (LAN) Area 1</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Interface Loopback 2 (LAN) Area 1</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 pt)</td>
</tr>
<tr>
<td>Interface Loopback 3 (LAN) Area 1</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 pt)</td>
</tr>
</tbody>
</table>

**Step 2: Configure R2.**

Configuration tasks for R2 include the following:
### Configuration Item or Task

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name R2</td>
<td>R2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password class</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password cisco</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password cisco</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/0</td>
<td>Set the description Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information. Activate Interface</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>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</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Interface Loopback 0 (Simulated Internet connection)</td>
<td>Set the description. Set the Layer 3 IPv4 address to 209.165.200.225/29.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Default route</td>
<td>Configure a default route out Lo0.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

### Step 3: Configure R3.

Configuration tasks for R3 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Router name</td>
<td>R3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface G0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface S0/0/1</td>
<td>Set the description</td>
<td>(1 point)</td>
</tr>
<tr>
<td></td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activate Interface</td>
<td></td>
</tr>
<tr>
<td>Interface Loopback 4 (LAN) Area 3</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 5 (LAN) Area 3</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Interface Loopback 6 (LAN) Area 3</td>
<td>Set the Layer 3 IPv4 address. Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

**Step 4: Configure S1.**

Configuration tasks for S1 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S1</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S2 and S3.</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**Step 5: Configure S2.**

Configuration tasks for S2 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S2</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged exec-password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the clear text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S1 and S3</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**Step 6: Configure S3**

Configuration tasks for S3 include the following:
<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS lookup</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Switch name</td>
<td>S3</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypted privileged EXEC password</td>
<td>class</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Console access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Telnet access password</td>
<td>cisco</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Encrypt the plain text passwords.</td>
<td></td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>Unauthorized Access is Prohibited!</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign an IPv4 address to the default SVI.</td>
<td>Refer to the Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Assign the default-gateway.</td>
<td>Refer to the Addressing Table.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Force trunking on interfaces connected to S1 and S2.</td>
<td>Use VLAN 1 as the native VLAN.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Disable the Dynamic Trunking Protocol (DTP) on all other ports.</td>
<td>Make sure ports are configured as access ports.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>Shutdown all unused ports.</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

Step 7: Configure IPv4 addresses on PCs.

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static IPv4 address information on PC-A</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-B</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
<tr>
<td>Configure static IPv4 address information on PC-C</td>
<td>Refer to Addressing Table for IPv4 address information.</td>
<td>(1/2 point)</td>
</tr>
</tbody>
</table>

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:
Step 2: Configure Spanning Tree on S2.

Configuration tasks for S2 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as primary root bridge for VLAN 1</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-A</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

Step 3: Configure Spanning Tree on S3.

Configuration tasks for S3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Rapid PVST+</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure as secondary root bridge for VLAN 1</td>
<td></td>
<td>(2 points)</td>
</tr>
<tr>
<td>Configure PortFast and BPDU Guard on the interface connected to PC-C</td>
<td></td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

Step 4: Configure HSRP on R1.

Configuration tasks for R1 include the following:
### Step 5: Configure HSRP on R3.

Configuration tasks for R3 include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the HSRP virtual IP address on interface G0/1.</td>
<td>Group: 1 Virtual IP address: 172.27.0.2</td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

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

Configuration tasks include the following:

<table>
<thead>
<tr>
<th>Configuration Item or Task</th>
<th>Specification</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>On S1, configure an LACP EtherChannel on interfaces connected to S3.</td>
<td>Use group 1 and enable LACP unconditionally.</td>
<td>(2 points)</td>
</tr>
<tr>
<td>On S3, configure an LACP EtherChannel on interfaces connected to S1.</td>
<td>Use group 1 and enable LACP only if a LACP device is detected.</td>
<td>(2 points)</td>
</tr>
</tbody>
</table>

**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

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

**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:

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

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.

<table>
<thead>
<tr>
<th>From</th>
<th>Command</th>
<th>To</th>
<th>Expected Results</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-A</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-A</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>PC-C</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>Default Gateway</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>ping</td>
<td>209.165.200.225</td>
<td>Ping should be successful.</td>
<td>(1 point)</td>
</tr>
<tr>
<td>PC-B</td>
<td>tracert</td>
<td>209.165.200.225</td>
<td>Trace should route through R1.</td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

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-A | ping | PC-C | 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:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>What command displays the IOS image that is currently being used by the network device?</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>What command displays the size of an IOS image loaded on a network device?</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>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?</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>What command displays the amount of space available to install an additional IOS image to a network device?</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>What command displays a list of all the licenses on an ISR-G2 device?</td>
<td></td>
<td>(1 point)</td>
</tr>
<tr>
<td>What command would you use to accept the end user license agreement?</td>
<td></td>
<td>(1 point)</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2801</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/1/0 (S0/1/0)</td>
<td>Serial 0/1/1 (S0/0/1)</td>
</tr>
<tr>
<td>2811</td>
<td>Fast Ethernet 0/0 (F0/0)</td>
<td>Fast Ethernet 0/1 (F0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

**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.
Router 1 int G0/1 Commands for HSRP
R1(config)# int G0/1
R1(config-if)# standby 1 ip 172.27.0.2
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt

Router 3 int G0/1 Commands for HSRP
R3(config)# int G0/1
R3(config-if)# standby 1 ip 172.27.0.2
Student: _____________________  Score: ________(175 points)

Ping Results: ________ (25 points of 175 points)

CIS 196a Scaling Networks Skills Exam Check Points (2 points for each item)

Router R1: (50 points)

```
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BCholQM5EnRtoyr8cHAUg.2
!
interface Loopback1
  ip address 172.27.1.1 255.255.255.0
!
interface Loopback2
  ip address 172.27.2.1 255.255.255.0
!
interface Loopback3
  ip address 172.27.3.1 255.255.255.0
!
interface GigabitEthernet0/1
  ip address 172.27.0.1 255.255.255.0
  standby 1 ip 172.27.0.2
  standby 1 priority 150
  standby 1 preempt

!
interface Serial0/0/0
  ip address 172.27.123.1 255.255.255.252
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 7 106D202A2638
!
routing ospf 1
  router-id 1.1.1.1
  area 1 range 172.27.0.0 255.255.255.0
  network 172.27.0.0 0.0.0.255 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
  network 172.27.123.0 0.0.0.3 area 0
!
end
```
Router 2: (40 points)

hostname R2
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGo1QM5EnRtoyr8cHAug.2
!
interface Loopback0
ip address 209.165.200.225 255.255.255.248
!
interface Serial0/0/0
ip address 172.27.123.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 02252D682829
ip ospf cost 7500
!
interface Serial0/0/1
ip address 172.27.123.5 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 14343B382F2B
clock rate 128000
!
router ospf 1
router-id 2.2.2.2
auto-cost reference-bandwidth 1000
network 172.27.123.0 0.0.0.3 area 0
network 172.27.123.4 0.0.0.3 area 0
default-information originate
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end

Router R3: (40 points)

hostname R3
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGo1QM5EnRtoyr8cHAug.2
!
interface Loopback4
ip address 172.27.4.1 255.255.255.0
!
interface Loopback5
ip address 172.27.5.1 255.255.255.0
!
interface Loopback6
ip address 172.27.6.1 255.255.255.0
interface GigabitEthernet0/1
  ip address 172.27.0.3 255.255.255.0
  standby 1 ip 172.27.0.2

interface Serial0/0/1
  ip address 172.27.123.6 255.255.255.252
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 7 13263E212823

router ospf 1
  router-id 3.3.3.3
  auto-cost reference-bandwidth 1000
  area 3 range 172.27.4.0 255.255.252.0
  network 172.27.0.0 0.0.0.255 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
  network 172.27.123.4 0.0.0.3 area 0

end

Switch S1: (10 points)

hostname S1

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

interface Vlan1
  ip address 172.27.0.11 255.255.255.0

ip default-gateway 172.27.0.2

Switch S3: (10 points)

hostname S3

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

interface Vlan1
  ip address 172.27.0.13 255.255.255.0

ip default-gateway 172.27.0.2