Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2013 Cisco Systems, Inc.
# Table of Contents

**Lab S-1: Review**  
L-1
- Visual Objective
- Required Resources
- Command List
- Job Aids
- Task 1: Configure Basic Settings, VLANs, Trunks, and Port Security on Switches
- Task 2: Configure Inter-VLAN Routing
- Task 3: Configure Internet Connectivity
- Task 4: Configure WAN Connectivity and a Dynamic Routing Protocol

**Lab 1-1: Troubleshooting VLANs and Trunks**  
L-29
- Visual Objective
- Required Resources
- Command List
- Job Aids
- Task 1: Troubleshoot VLAN Connectivity
- Task 2: Troubleshoot Trunk Connectivity Between the Switches

**Lab 1-2: Optimizing STP**  
L-43
- Visual Objective
- Required Resources
- Command List
- Job Aids
- Task 1: Verify STP Operation
- Task 2: Influence Root Bridge Selection
- Task 3: Implement STP PortFast
- Task 4: Implement STP BPDU Guard

**Lab 1-3: Configuring EtherChannel**  
L-59
- Visual Objective
- Required Resources
- Command List
- Job Aids
- Task 1: Configure EtherChannel
- Task 2: Verify EtherChannel Redundancy

**Lab 2-1: Troubleshooting IP Connectivity**  
L-71
- Visual Objective
- Required Resources
- Command List
- Job Aids
- Task 1: Troubleshoot the Default Route
- Task 2: Troubleshoot an ACL
- Task 3: Troubleshoot the Default Gateway and Name Resolution Settings
Lab 3-1: Implementing EIGRP

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Verify Connectivity to Remote Network
Task 2: Configure and Verify EIGRP
Task 3: Investigate Neighbor Events
Task 4: Disable OSPF Routing Process

Lab 3-2: Troubleshooting EIGRP

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Troubleshoot Basic Connectivity
Task 2: Troubleshooting EIGRP Neighbors
Task 3: Troubleshooting Routing Table Issues

Lab 3-3: Implementing EIGRP for IPv6

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Enable IPv6 on the Interfaces
Task 2: Enable IPv6 EIGRP

Lab 4-1: Configuring Multiarea OSPF

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Configure Multiarea OSPF
Task 2: Verify Multiarea OSPF

Lab 4-2: Troubleshooting Multiarea OSPF

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Troubleshoot OSPF Neighbor Issues
Task 2: Troubleshoot OSPF Routing Table Issues

Lab 4-3: Configuring OSPF for IPv6

Visual Objective
Required Resources
Command List
Lab 5-1: Configuring and Troubleshooting a Serial Connection

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Troubleshoot PPP
Task 2: Enable HDLC Encapsulation

Lab 5-2: Establishing a Frame Relay WAN

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Configure and Verify Basic Frame Relay
Task 2: Configure and Verify Frame Relay Subinterfaces
Task 3: Remove Frame Relay Configuration

Lab 5-3: Establishing a GRE Tunnel

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Configure and Verify a GRE Tunnel
Task 2: Configure and Verify OSPF over a GRE Tunnel

Lab 6-1: SNMP and Syslog Basic Configuration

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Configure Router for SNMP Access
Task 2: Configure Router for Syslog

Lab 6-2: Analyzing NetFlow Data

Visual Objective
Required Resources
Command List
Job Aids
Task 1: Analyze NetFlow Data

Lab 6-3: Managing Cisco Devices and Licensing

Visual Objective
Required Resources
Command List
Job Aids
Lab S-2: ICND2 Superlab

Visual Objective

Required Resources

Command List

Job Aids

Task 1: Secure Router and Configure Inter-VLAN Routing

Task 2: Configure Basic Settings, VLANs, and Trunks on Switch

Task 3: Troubleshoot EtherChannel

Task 4: Port Security (Trouble Ticket)

Task 5: Enable SSH Access on the Branch Router

Task 6: Configure DHCP Server

Task 7: Stateless Autoconfiguration on the PC

Task 8: Configure PPP Encapsulation

Task 9: Configure Dynamic Routing Protocol

Task 10: Configure the OSPFv3 Routing Protocol

Task 11: Troubleshoot the IP Access Control List (Trouble Ticket)

Lab Answer Keys

Lab S-1: Review

Lab 1-1: Troubleshooting VLANs and Trunks

Lab 1-2: Optimizing STP

Lab 1-3: Configuring EtherChannel

Lab 2-1: Troubleshooting IP Connectivity

Lab 3-1: Implementing EIGRP

Lab 3-2: Troubleshooting EIGRP

Lab 3-3: Implementing EIGRP for IPv6

Lab 4-1: Configuring Multiarea OSPF

Lab 4-2: Troubleshooting Multiarea OSPF

Lab 4-3: Configuring OSPF for IPv6

Lab 5-1: Configuring and Troubleshooting a Serial Connection

Lab 5-2: Establishing a Frame Relay WAN

Lab 5-3: Establishing a GRE Tunnel

Lab 6-1: SNMP and Syslog Basic Configuration

Lab 6-2: Analyzing NetFlow Data

Lab 6-3: Managing Cisco Devices and Licensing

Lab S-2: ICND2 Superlab
Lab S-1: Review

Activity Overview

Objectives

In this lab, you will consolidate the knowledge that you gained in ICND1 by configuring a simple network. After completing this activity, you will be able to meet these objectives:

- Configure basic settings, VLANs, trunks, and port security on switches
- Configure inter-VLAN routing
- Configure Internet connectivity
- Configure WAN connectivity and a dynamic routing protocol

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list acl_id permit network</td>
<td>Creates a numbered access list entry.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Activates the configuration mode from the terminal.</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Generates an RSA crypto key pair.</td>
</tr>
<tr>
<td>delete name</td>
<td>Deletes a file from flash memory.</td>
</tr>
<tr>
<td>deny ip</td>
<td>tcp</td>
</tr>
<tr>
<td>description description</td>
<td>Under interface configuration mode, adds a description to the interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Activates privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.</td>
</tr>
<tr>
<td>enable secret password</td>
<td>Configures enable password in SHA-256 encrypted form.</td>
</tr>
<tr>
<td>erase startup-config</td>
<td>Erases the startup configuration that is stored in nonvolatile memory.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>encapsulation dot1Q vlan [native]</td>
<td>Sets encapsulation type and VLAN on a subinterface on a router. The &quot;native&quot; is an optional parameter that marks the VLAN as the native VLAN (not tagged).</td>
</tr>
<tr>
<td>hostname hostname</td>
<td>Sets the system name, which forms part of the prompt.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>interface interface.subinterface</td>
<td>Enters subinterface configuration mode.</td>
</tr>
<tr>
<td>ip access-list extended acl_name</td>
<td>Creates an extended named access list.</td>
</tr>
<tr>
<td>ip access-group acl_name in</td>
<td>out</td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td>Sets the IP address and mask on an interface.</td>
</tr>
<tr>
<td>ip default-gateway ip-address</td>
<td>Sets the default gateway.</td>
</tr>
<tr>
<td>ip domain-name domain</td>
<td>Sets a domain name.</td>
</tr>
<tr>
<td>ip nat inside source list acl_id interface overload</td>
<td>Configures dynamic NAT with PAT.</td>
</tr>
<tr>
<td>ip nat inside</td>
<td>Configures an interface as NAT inside.</td>
</tr>
<tr>
<td>ip nat outside</td>
<td>Configures an interface as NAT outside.</td>
</tr>
<tr>
<td>ip route network mask next_hop_ip_address</td>
<td>Configures a static route (including a default route).</td>
</tr>
<tr>
<td>ip ssh version 2</td>
<td>Enables SSH version 2.</td>
</tr>
<tr>
<td>line console 0</td>
<td>Enters line console configuration mode.</td>
</tr>
<tr>
<td>line vty start_line end_line</td>
<td>Enters virtual lines configuration mode.</td>
</tr>
<tr>
<td>logging synchronous</td>
<td>Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.</td>
</tr>
<tr>
<td>login</td>
<td>Enables verification of password on a line.</td>
</tr>
<tr>
<td>login local</td>
<td>Enables verification of username and password on a line.</td>
</tr>
<tr>
<td>network network wildcard_mask area area_id</td>
<td>Configures a router to advertise a network through OSPF.</td>
</tr>
<tr>
<td>password</td>
<td>Sets password on a line.</td>
</tr>
<tr>
<td>permit ip</td>
<td>tcp</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>Pings a destination IP address.</td>
</tr>
<tr>
<td>reload</td>
<td>Restarts the switch and reloads the Cisco IOS operating system and configuration.</td>
</tr>
<tr>
<td>router ospf process_id</td>
<td>Creates an OSPF process.</td>
</tr>
<tr>
<td>show interfaces interface</td>
<td>Displays status of an interface.</td>
</tr>
<tr>
<td>show interfaces interface switchport</td>
<td>Displays switch port status of a port.</td>
</tr>
<tr>
<td>show interfaces interface trunk</td>
<td>Displays trunking status of a port.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip access-lists</td>
<td>Displays configured access lists and hit counts.</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays brief status of interfaces and their IP addresses.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays routing table.</td>
</tr>
<tr>
<td>show ip nat translations</td>
<td>Displays NAT translation table.</td>
</tr>
<tr>
<td>show ip ospf neighbors</td>
<td>Displays OSPF neighbors.</td>
</tr>
<tr>
<td>show mac address-table</td>
<td>Displays MAC address table on a switch.</td>
</tr>
<tr>
<td>show users</td>
<td>Displays users that are currently logged in to a router.</td>
</tr>
<tr>
<td>show port-security interface</td>
<td>Displays port security information on an interface.</td>
</tr>
<tr>
<td>shutdown interface</td>
<td>Shuts down an interface. Use the no version of the command to enable the interface.</td>
</tr>
<tr>
<td>switchport access vlan vlan</td>
<td>Specifies an access VLAN on a switch port.</td>
</tr>
<tr>
<td>switchport mode access</td>
<td>trunk</td>
</tr>
<tr>
<td>switchport port-security</td>
<td>Enables port security on a switch port.</td>
</tr>
<tr>
<td>switchport port-security violation protect</td>
<td>Configures the port security violation to protect.</td>
</tr>
<tr>
<td>switchport port-security maximum number</td>
<td>Specifies maximum number of MAC addresses that can be seen on a port when port security is enabled.</td>
</tr>
<tr>
<td>switchport port-security mac-address mac_address</td>
<td>Manually defines MAC addresses that are allowed on a switch port when port security is enabled.</td>
</tr>
<tr>
<td>switchport trunk allowed vlan vlans</td>
<td>Specifies allowed VLANs on a trunk link.</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>Uses Telnet to connect to a destination IP address.</td>
</tr>
<tr>
<td>transport input ssh telnet</td>
<td>Allows Telnet and SSH on virtual lines.</td>
</tr>
<tr>
<td>username username password password</td>
<td>Creates a user account in the local user database.</td>
</tr>
<tr>
<td>vlan vlan_id</td>
<td>Creates VLAN on a switch.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>
The table shows the usernames and passwords that are used to access PC1 and PC2.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that will be used in this lab.

The table shows the interface identification and IP addresses that will be used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Looback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>Device</td>
<td>Interface</td>
<td>IP Address or Subnet Mask</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Setting the IP Address on a PC**

On a PC, click **Start** and choose **Control Panel**. Click **Change Adapter Settings** and then right-click **Local Area Network**. Choose **Properties**. When you are presented with the Local Area Connection Properties dialog, click **Internet Protocol version 4 (TCP/IPv4)** and then click **Properties**. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, click the **Use the Following IP Address** radio button and enter the appropriate IP address, subnet mask, and default gateway.

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)

**Task 1: Configure Basic Settings, VLANs, Trunks, and Port Security on Switches**

In this task, you will first delete existing configurations from SW1 and SW2 switches and reload them. Then, you will configure basic settings on the switches and secure administrative access to the switches. You will also configure VLANs and trunks on the switches and put PCs into different VLANs. Finally, you will enable port security on the switches to prevent unauthorized access to the LAN.

**Activity Procedure**

Complete the following steps:
**Step 1**

Delete the startup configuration from the SW1 and SW2 switches. Delete the `vlan.dat` file from the flash memory of the switches. Reload the switches in order to boot the switches with empty configurations.

**Step 2**

Configure a hostname (SW1, SW2) on the switches.

**Step 3**

Configure IP addresses on both switches for management purposes. Assign the IP address to the VLAN 1 interface. Use the lab job aids to determine the IP address for each switch.

**Step 4**

Configure the enable password on the SW1 and SW2 switches. Use the command that will store the configured password in SHA-256 encrypted form. Use `cisco` as the password.

**Step 5**

Secure console access to the switches by enabling a password on the console. Use `cisco` as the password.

By default, if the switch wants you to know something, it will let you know right away. It will interrupt your work to deliver a message. Disable this behavior on both switches, using the `logging synchronous` command.

**Step 6**

Enable SSH version 2 remote access to the SW1 and SW2 switches. Use 1024-bit RSA keys. Use `cisco.com` as the domain name. Telnet should not be allowed.

**Step 7**

Create a local user account on the switches that will be used to authenticate users accessing the switches via SSH or Telnet. Use `ccna` as a username and `cisco` as a password. Configure all of the virtual lines for checking for username and password. Do this step on SW1 and SW2.

**Step 8**

Create two additional VLANs on both switches. Use VLANs 10 and 20.

**Step 9**

Configure a trunk between SW1 and SW2 switches over the FastEthernet0/3 port. Allow only VLANs 1, 10, and 20 on the trunk link. Shut down the FastEthernet0/4 port on both switches.
**Step 10**
On the SW1, configure the port connecting to PC1 (FastEthernet0/1) as an access port. Put the port into VLAN 10.

**Step 11**
On the SW2, configure the port connecting to PC2 (FastEthernet0/1) as an access port. Put the port into VLAN 20.

**Step 12**
Access PC1. Log in with the username **Administrator** and password **admin**. Set the following IP settings on the LAB network adapter:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.100</td>
<td>255.255.255.0</td>
<td>10.1.10.1</td>
</tr>
</tbody>
</table>

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)
Step 13

Access PC2. Log in with the username **Administrator** and the password **admin**. Set the following IP settings on the LAB network adapter:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20.100</td>
<td>255.255.255.0</td>
<td>10.1.20.1</td>
</tr>
</tbody>
</table>

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- **Obtain an IP address automatically**
- **Use the following IP address:**
  - IP address: 10.1.20.100
  - Subnet mask: 255.255.255.0
  - Default gateway: 10.1.20.1
- **Obtain DNS server address automatically**
- **Use the following DNS server addresses:**
  - Preferred DNS server: 
  - Alternate DNS server: 

- Validate settings upon exit

[Advanced...]

[OK]  [Cancel]
Step 14

From PC1, which is in VLAN 10, ping the management IP address of the SW1 (10.1.1.11) in VLAN 1.

C:\Windows\system32> **ping 10.1.1.11**
Pinging 10.1.1.11 with 32 bytes of data:
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

The ping should be unsuccessful because routing between VLAN 1 and VLAN 10 has not yet been configured.

Step 15

From PC2, which is in VLAN 20, ping the management IP address of the SW1 (10.1.1.11) in VLAN 1.

C:\Windows\system32> **ping 10.1.1.11**
Pinging 10.1.1.11 with 32 bytes of data:
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

The ping should be unsuccessful because routing between VLAN 1 and VLAN 20 has not yet been configured.

Step 16

On PC1, issue the **ipconfig /all** command and identify its MAC address.

C:\> **ipconfig /all**
<output omitted>
Ethernet adapter Local Area Connection:
    Media State . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix .:
    Description . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
    Physical Address . . . . . . . . . : 00-0C-29-3B-70-9D
    DHCP Enabled. . . . . . . . . : Yes
    Autoconfiguration Enabled . . . : Yes
<output omitted>
**Step 17**

On PC2, issue the `ipconfig /all` command and identify its MAC address.

```
C:\>ipconfig /all
<output omitted>
Ethernet adapter Local Area Connection:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Description . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address . . . . . . . : 00-0C-29-A8-A05A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . : Yes
<output omitted>
```

**Step 18**

On the SW1 and SW2 switches, enable port security on the interfaces connecting to the PCs (FastEthernet0/1) in order to allow only PCs to connect to the switches. Use the following port security parameters:

- Violation action: Protect
- Maximum MAC addresses: 1
- MAC address: PC1 on SW1, PC2 on SW2

**Activity Verification**

Verification of this task will be done after configuration of inter-VLAN routing.

**Task 2: Configure Inter-VLAN Routing**

In this task, you will delete the existing configuration from the Branch router and then reload it. You will then secure administrative access to the router and configure inter-VLAN routing between VLANs 1, 10, and 20. In this way, you will enable connectivity between PC1, PC2, and management IP addresses on the switches. You will implement inter-VLAN routing on the Branch router by establishing a trunk link between the router and SW1 switch.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, delete the startup configuration. Reload the router in order to boot the router with the empty configuration.
**Step 2**
Configure the hostname on the Branch router.

**Step 3**
Configure the enable password on the Branch router. Use the command that will store the configured password in SHA-256 encrypted form. Use `cisco` as the password.

**Step 4**
Secure console access to the router by using the enable password on the console. Use `cisco` as the password.

By default, if the router wants you to know something, it will let you know right away. It will interrupt your work to pass you a message. Disable this behavior on the Branch router by using the `logging synchronous` command.

**Step 5**
Secure Telnet access to the router by enabling a password on virtual lines. Use `cisco` as the password.

**Step 6**
Enable the GigabitEthernet0/0 interface on the Branch router. Create three subinterfaces on the interface and configure them with the following parameters:

<table>
<thead>
<tr>
<th>Subinterface identifier</th>
<th>VLAN identifier</th>
<th>IP address/mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0.1</td>
<td>1 (native)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>GigabitEthernet0/0.10</td>
<td>10</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>GigabitEthernet0/0.20</td>
<td>20</td>
<td>10.1.20.1/24</td>
</tr>
</tbody>
</table>

**Step 7**
On the SW1 switch, configure the FastEthernet 0/13 port as a trunk. Allow only VLANs 1, 10, and 20 on the trunk link. In this way, you will enable the switch to send traffic to or from all VLANs over the same port toward the Branch router.

**Step 8**
On SW1 and SW2, configure the default gateway of 10.1.1.1.

**Activity Verification**
You have completed this task when you attain these results:
Step 1

Verified the switch port status of the FastEthernet0/13 port on the SW1 switch:

```
SW1#show interfaces FastEthernet0/13 switchport
Name: Fa0/13
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

You should see that the interface is in trunking mode.

Step 2

Verified the switch port status of the FastEthernet0/3 port on the SW1 switch:

```
SW1#show interfaces FastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

You should see that the interface is in trunking mode.
Step 3

Verified the trunking status of the FastEthernet0/3 port on the SW1 switch:

```
SW1# show interfaces FastEthernet0/3 trunk
Port  Mode        Encapsulation Status Native vlan
Fa0/3 on          802.1q trunking 1
Port  Vlans allowed on trunk
Fa0/3 1,10,20
Port  Vlans allowed and active in management domain
Fa0/3 1,10,20
Port  Vlans in spanning tree forwarding state and not pruned
Fa0/3 1,10,20
```

You should see that the interface is in trunking mode, encapsulation is 802.1q, and VLANs 1, 10, and 20 are active.

Step 4

Verified the trunking status of the FastEthernet0/3 port on the SW2 switch:

```
SW2# show interfaces FastEthernet0/3 trunk
Port  Mode        Encapsulation Status Native vlan
Fa0/3 on          802.1q trunking 1
Port  Vlans allowed on trunk
Fa0/3 1,10,20
Port  Vlans allowed and active in management domain
Fa0/3 1,10,20
Port  Vlans in spanning tree forwarding state and not pruned
Fa0/3 1,10,20
```

You should see that the interface is in trunking mode, encapsulation is 802.1q, and VLANs 1, 10, and 20 are active.

Step 5

On the Branch router, verified the state of configured subinterfaces:

```
Branch# show ip interface brief
Interface              IP-Address   OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned YES unset administratively down down
GigabitEthernet0/0     unassigned  YES unset up                    up
GigabitEthernet0/0.1   10.1.1.1     YES manual up                    up
GigabitEthernet0/0.10  10.1.10.1    YES manual up                    up
GigabitEthernet0/0.20  10.1.20.1    YES manual up                    up
<output omitted>
```

You should see that the subinterfaces are operational and configured with IP addresses.
**Step 6**

Access the PC1. Ping the SW1 management IP address at 10.1.1.11.

C:\Windows\system32>**ping 10.1.1.11**
Pinging 10.1.1.11 with 32 bytes of data:
Request timed out.
[output]
Reply from 10.1.1.11: bytes=32 time=8ms TTL=254
Reply from 10.1.1.11: bytes=32 time=2ms TTL=254
Reply from 10.1.1.11: bytes=32 time=2ms TTL=254
Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 8ms, Average = 4ms

The ping should be successful.

**Step 7**

From the PC1, ping PC2 at 10.1.20.100.

C:\Windows\system32>**ping 10.1.20.100**
Pinging 10.1.20.100 with 32 bytes of data:
Reply from 10.1.20.100: bytes=32 time=8ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Ping statistics for 10.1.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms

The ping should be successful.
Step 8

On the PC1, start PuTTY by double-clicking the PuTTY icon on the desktop. Establish an SSH session to the SW1 management IP address at 10.1.1.11. Accept the switch fingerprint, when asked. Use ccna as the username and cisco as the password in order to log in. Enter privileged EXEC mode, using the password cisco to verify that the enable password is correctly configured.

Establishment of the SSH session should be successful.
Step 9

Verified port security information on the FastEthernet0/1 port on the SW1 switch. Use the previously established SSH session to access SW1.

```
SW1#show port-security interface FastEthernet0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
<output omitted>
```

You should see that the port is protected, security violation is set to protect, and the last seen MAC address is PC1 in VLAN 10.
Step 10

On PC1, open another PuTTY window by double-clicking the PuTTY icon again. Establish a Telnet session to the Branch router at 10.1.10.1. Use the cisco password to log in. Enter privileged EXEC mode, using cisco as the password, to verify that the enable password is correctly configured.

User Access Verification
Password: cisco
Branch> enable
Password: cisco
Branch#

Establishment of the Telnet session should be successful.
Step 11

From PC2, ping the SW2 management IP address at 10.1.1.12.

C:\Windows\system32> ping 10.1.1.12
Pinging 10.1.1.12 with 32 bytes of data:
Request timed out.
Reply from 10.1.1.12: bytes=32 time=8ms TTL=254
Reply from 10.1.1.12: bytes=32 time=2ms TTL=254
Reply from 10.1.1.12: bytes=32 time=2ms TTL=254
Ping statistics for 10.1.1.12:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
   Approximate round trip times in milli-seconds:
       Minimum = 2ms, Maximum = 8ms, Average = 4ms

The ping should be successful.
Step 12

On PC2, start PuTTY by double-clicking the PuTTY icon on the desktop. Establish an SSH session to the SW2 management IP address at 10.1.1.12. Accept the switch fingerprint when asked. Use ccna as the username and cisco as the password to log in. Enter privileged EXEC mode, using cisco as the password to verify that the enable password is correctly configured.

```
login as: admin
Using keyboard-interactive authentication.
Password: cisco
SW2>enable
Password: cisco
SW2#
```

Establishment of the SSH session should be successful.
**Step 13**

Verify port security information on the FastEthernet0/1 port on the SW2 switch. Use the previously established SSH session to access SW2.

```
   SW2# show port-security interface FastEthernet0/1
   Port Security : Enabled
   Port Status    : Secure-up
   Violation Mode: Protect
   Aging Time     : 0 mins
   Aging Type     : Absolute
   SecureStatic Address Aging : Disabled
   Maximum MAC Addresses : 1
   Total MAC Addresses : 1
   <output omitted>
```

You should see that the port is protected, security violation is set to "protect," and the last seen MAC address is PC2 in VLAN 20.

**Step 14**

Close all SSH and Telnet sessions on PC1 and PC2.

**Task 3: Configure Internet Connectivity**

In this task, you will configure the Branch router to provide Internet connectivity. This includes configuring the IP address on an interface and default route. You will also configure NAT with PAT to hide internal addressing from the Internet.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, configure an IP address on the interface connecting to the Internet (GigabitEthernet0/1). Use 209.165.201.1/27 for the IP address. Enable the interface and add a description that says "Link to HQ".

**Step 2**

Configure a default route on the Branch router that will point to the HQ router as the next hop.

**Step 3**

Create a standard access list that will permit users on VLANs 10 and 20. This access list will be used to specify IP addresses that are eligible for NAT. Use 1 for the access list identifier.
**Step 4**

Configure NAT with PAT on the Branch router for all LAN users. This includes users on VLANs 10 and 20. Refer to the previously configured access list. Use the IP address on the GigabitEthernet0/1 interface for a translated IP address.

**Activity Verification**

You have completed this task when you attain these results:

**Step 1**

Verified status of the GigabitEthernet0/1 interface on the Branch router.

```
Branch# show interfaces GigabitEthernet0/1
GigabitEthernet0/1 is up, line protocol is up
   Hardware is CN Gigabit Ethernet, address is fc99.47e5.2701 (bia fc99.47e5.2701)
   Description: Link to HQ
   Internet address is 209.165.201.1/27
   MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full Duplex, 100Mbps, media type is RJ45
```

You should see that the interface is operational and that it has an IP address configured.

**Step 2**

Verified the routing table on the Branch router.

```
Branch# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
       Gateway of last resort is 209.165.201.2 to network 0.0.0.0
S*  0.0.0.0/0 [1/0] via 209.165.201.2
<output omitted>
```

You should see that the router has a default route configured, which points to the HQ router.
Step 3

Access PC1. Start PuTTY by double-clicking the PuTTY icon on the desktop. Establish a Telnet session to the server at 172.16.1.100.

![PuTTY Configuration](image)

Establishment of a Telnet session should be successful.

**Note**  The server is simulated as a loopback interface on the HQ router.
Step 4
Access the PC2. Start PuTTY by double-clicking the PuTTY icon on the desktop. Establish a Telnet session to the server at 172.16.1.100.

![PuTTY Configuration](image)

HQ#

Establishment of a Telnet session should be successful.

Step 5
Verified the translation table on the Branch router.

```
Branch#show ip nat translations
Pro Inside global   Inside local   Outside local   Outside global
  tcp 209.165.201.1:1037 10.1.10.100:1037   172.16.1.100:23   172.16.1.100:23
  tcp 209.165.201.1:1033 10.1.20.100:1033   172.16.1.100:23   172.16.1.100:23
```

You should see two PAT translations. One translation is for PC1 at 10.1.10.100 and the second translation is for PC2 at 10.1.20.100. Both IP addresses translated to the same global IP address, but with different source ports.
Step 6

Close all Telnet sessions on PC1 and PC2.

**Task 4: Configure WAN Connectivity and a Dynamic Routing Protocol**

In this task, you will configure the Branch router with WAN connectivity to the HQ router. This activity includes configuring an IP address on the serial interface and enabling the interface. You will also configure single-area OSPF on the Branch router in order to exchange routing information with the HQ router. The HQ router has been preconfigured with OSPF.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, configure an IP address on the WAN interface (Serial0/0/0). Use 192.168.1.1/24 for the IP address. Enable the interface.

The interface types that you are most familiar with are probably Fast Ethernet and Gigabit Ethernet. These are the most common interface types. In this task, you will configure an IP address on the serial interface of the Branch router. In a basic implementation, a serial connection will work with no additional configuration. In more complex implementations, there are a few optional settings.

**Step 2**

Create an OSPF routing process on the Branch router. Use 1 as OSPF process ID. Enable OSPF routing in Area 0 for the following networks:

- 192.168.1.0/24
- 10.1.1.0/24
- 10.1.10.0/24
- 10.1.20.0/24

**Activity Verification**

You have completed this task when you attain these results:

**Step 1**

Verified OSPF neighbors on the Branch router.

```
Branch#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
 1.1.1.1           0   FULL/  -        00:00:37    192.168.1.2     Serial0/0/0
```

You should see the HQ router as OSPF neighbor in FULL state.
Step 2

Verified the OSPF routing table on the Branch router.

```
Branch#show ip route ospf
172.16.0.0/24 is subnetted, 1 subnets
O 172.16.1.0 [110/65] via 192.168.1.2, 00:00:30, Serial0/0/0
```

You should see the 172.16.1.0/24 network as the OSPF route. The network should be accessible over the Serial0/0/0 interface.

Step 3

Access PC1. Open a command prompt and ping the server at 172.16.1.100.

```
C:\Windows\system32>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=42ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Reply from 172.16.1.100: bytes=32 time=35ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 35ms, Maximum = 42ms, Average = 37ms
```

The ping should be successful.
**Step 4**

On the PC1, start PuTTY by double-clicking the PuTTY icon on the desktop. Establish a Telnet session to the HQ router at 192.168.1.2.

![PuTTY Configuration](image)

HQ#

Establishment of Telnet session should be successful.
Step 5
On the HQ router, verify the routing table. Use the previously established Telnet session.

```
HQ#show ip route
Codes:  L - local,  C - connected,  S - static,  R - RIP,  M - mobile,  B - BGP
       D - EIGRP,  EX - EIGRP external,  O - OSPF,  IA - OSPF inter area
       N1 - OSPF NSSA external type 1,  N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,  E2 - OSPF external type 2
       i - IS-IS,  su - IS-IS summary,  L1 - IS-IS level-1,  L2 - IS-IS level-2
       ia - IS-IS inter area,  * - candidate default,  U - per-user static route
       o - ODR,  P - periodic downloaded static route,  H - NHRP,  l - LISP
       + - replicated route,  % - next hop override
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 3 subnets
 O        10.1.1.0 [110/65] via 192.168.1.1, 00:03:10, Serial0/0/0
 O        10.1.10.0 [110/65] via 192.168.1.1, 00:03:10, Serial0/0/0
 O        10.1.20.0 [110/65] via 192.168.1.1, 00:03:10, Serial0/0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
 C       172.16.1.0/24 is directly connected, Loopback0
 L       172.16.1.100/32 is directly connected, Loopback0
 O       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C       192.168.1.0/24 is directly connected, Serial10/0/0
 L       192.168.1.2/32 is directly connected, Serial10/0/0
 O       192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
 C       192.168.2.0/24 is directly connected, Tunnel0
 L       192.168.2.2/32 is directly connected, Tunnel0
 O       209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
 C       209.165.201.0/27 is directly connected, GigabitEthernet0/1
 L       209.165.201.2/32 is directly connected, GigabitEthernet0/1
```

You should see LAN networks accessible over the Serial0/0/0 interface, with Branch router as the next-hop router.

Step 6
Close the Telnet sessions on PC1.

Step 7
Save the configurations on the Branch router, switch SW1, and switch SW2.
Lab 1-1: Troubleshooting VLANs and Trunks

Activity Overview

Objectives

In this lab, you will explore various trouble tickets related to VLANs and trunks, identify the problems that they present, and correct the problems:

- Troubleshooting VLAN connectivity
- Troubleshoot trunk connectivity

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the interface status and statistics.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the switch port status of an interface.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays VLAN database.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Statically configures an interface for trunking.</td>
</tr>
<tr>
<td>switchport nonegotiate</td>
<td>Disables DTP on an interface.</td>
</tr>
<tr>
<td>switchport trunk native vlan vlan_id</td>
<td>Configures native VLAN on a trunk interface.</td>
</tr>
<tr>
<td>vlan vlan_id</td>
<td>Creates a VLAN.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

### Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.
The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. A trunk is configured on the link between switches SW1 and SW2. SW1 switch and the Branch router are connected by a single trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing
As the figure shows, OSPF is set up as the routing protocol on both routers.

Task 1: Troubleshoot VLAN Connectivity
After you configured the network, your colleague wanted to make some additional modifications and ended up breaking the connectivity for some users. Look at the job aids to remember how the network should be configured. The Branch router should be configured to route between VLANs 1, 10, and 20. PC1 and PC2 should be able to ping each other.

You have been informed that users in VLAN 10 cannot communicate. Specifically, a user on PC1 cannot ping the default gateway on the Branch router. As a network engineer, you have to troubleshoot and correct the problem. A senior network engineer has confirmed that the problem is not between the SW1 switch and the Branch router.

Activity Procedure
Complete the following steps:

Step 1
Access PC1.
Step 2

On PC1, open a command prompt. Ping the default gateway at 10.1.10.1.

```
c:\> ping 10.1.10.1
Pinging 10.1.10.1 with 32 bytes of data:
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Reply from 10.1.10.100: Destination host unreachable.
Ping statistics for 10.1.10.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100)
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The ping should not be successful. You should proceed to troubleshoot the connectivity between SW1 and PC1.

Step 3

Access the SW1 switch.

Step 4

On SW1, verify the status of the interface connecting to PC1.

```
SW1# show interfaces fastEthernet0/1
FastEthernet0/1 is up, line protocol is up (connected)
<output omitted>
```

You should see that the interface status is up/up.
**Step 5**

Verify the switch port status of the interface connecting to PC1. Examine the access VLAN of the interface.

```
SW1#show interfaces fastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

What is the access VLAN that the interface is configured in? Do you see the switch port status as active or inactive? Why is the interface inactive?

---

**Step 6**

Verify the VLAN database to confirm that VLAN 10 is missing on the switch.

```
SW1#show vlan
VLAN    Name                          Status    Ports
-----    ----------------------------- --------- -------------------------------
  1      default                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5    Fa0/6, Fa0/7, Fa0/8, Fa0/9
               Fa0/10, Fa0/11, Fa0/12, Fa0/14    Fa0/15, Fa0/16, Fa0/17, Fa0/18    Fa0/19, Fa0/20, Fa0/21, Fa0/22    Fa0/23, Fa0/24, Gi0/1, Gi0/2
  20     VLAN0020                      active
  100    VLAN0100                      active
  1002   fddi-default                 act/unsup
  1003   token-ring-default           act/unsup
  1004   fddinet-default              act/unsup
  1005   trnet-default                act/unsup
```

**Step 7**

Resolve the problem by creating VLAN 10 on SW1.
**Step 8**

Verify the VLAN database to confirm that VLAN 10 has been created.

```
SW1#show vlan
VLAN Name                  Status    Ports
---- -------------------------------- --------- -------------------------------
 1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
       Fa0/6, Fa0/7, Fa0/8, Fa0/9
       Fa0/10, Fa0/11, Fa0/12, Fa0/14
       Fa0/15, Fa0/16, Fa0/17, Fa0/18
       Fa0/19, Fa0/20, Fa0/21, Fa0/22
       Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active
100  VLAN0100                         active
1002 fddi-default                    act/unsup
1003 token-ring-default              act/unsup
1004 fddinet-default                 act/unsup
1005 trnet-default                   act/unsup
```

**Step 9**

Verify the switch port status of the interface connecting to PC1.

```
SW1#show interfaces fastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

The interface should be in VLAN 10 and should no longer be inactive.
Step 10

Finally, return to PC1 and ping the default gateway at 10.1.10.1 again.

c:\>ping 10.1.10.1
Pinging 10.1.10.1 with 32 bytes of data:
Reply from 10.1.10.1: bytes=32 time=2ms TTL=255
Reply from 10.1.10.1: bytes=32 time<1ms TTL=255
Reply from 10.1.10.1: bytes=32 time=1ms TTL=255
Reply from 10.1.10.1: bytes=32 time=1ms TTL=255
Ping statistics for 10.1.10.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 2ms, Average = 1ms

This time the ping should be successful.

Activity Verification
No additional verification is needed in this task.

Task 2: Troubleshoot Trunk Connectivity Between the Switches

You have been informed that users in VLAN 10 cannot communicate with users in VLAN 20. Specifically, a user on PC1 cannot ping PC2. As a network engineer, you have to troubleshoot and correct the problem. The senior network engineer has confirmed that the problem is on the trunk link between the SW1 and SW2 switches.

Activity Procedure
Complete the following steps:

Step 1

Access PC1.
**Step 2**

On PC1, open a command prompt. Ping PC2 at 10.1.20.100.

```
c:\> ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.20.100:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The ping should not be successful. You should proceed to troubleshoot the connectivity between SW1 and SW2.

**Step 3**

Access the SW1 switch.

**Step 4**

On SW1, examine the status of the FastEthernet0/3 interface. This interface connects SW1 and SW2.

```
SW1# show interfaces fastEthernet0/3
FastEthernet0/3 is up, line protocol is up (connected)
<output omitted>
```

You should see that the interface is up. Proceed with troubleshooting the configuration of the trunk between the switches.
Step 5

On SW1, verify the switch port configuration of the FastEthernet0/3 interface.

    SW1#show interfaces fastEthernet0/3 switchport
    Name: Fa0/3
    Switchport: Enabled
    Administrative Mode: dynamic auto
    Operational Mode: static access
    Administrative Trunking Encapsulation: dot1q
    Operational Trunking Encapsulation: native
    Negotiation of Trunking: On
    <output omitted>

You should see that the interface is in dynamic auto DTP mode. However, the operational mode is access.

Step 6

Access the SW2 switch.

Step 7

On SW2, verify the switch port configuration of the FastEthernet0/3 interface.

    SW2#show interfaces fastEthernet0/3 switchport
    Name: Fa0/3
    Switchport: Enabled
    Administrative Mode: dynamic auto
    Operational Mode: static access
    Administrative Trunking Encapsulation: dot1q
    Operational Trunking Encapsulation: native
    Negotiation of Trunking: On
    <output omitted>

You should see that the interface is in the same mode as the interface on SW1. What is the reason that the trunk has not established between the switches?

Step 8

On SW2, configure the FastEthernet0/3 interface as trunk. Disable DTP as well.

Step 9

Return to SW1, and configure the FastEthernet 0/3 interface as trunk. Disable DTP as well.
**Step 10**

On SW1, verify the switch port configuration of the FastEthernet0/3 interface.

```
SW1#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<output omitted>
```

You should see that the interface is in now in trunk operational mode and that negotiation of trunking is set to Off.

**Step 11**

Return to PC1 and ping PC2 at 10.1.20.100 again.

```
c:\>ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:
    Request timed out.
    Request timed out.
    Request timed out.
    Request timed out.
Ping statistics for 10.1.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The ping should still not be successful. There is obviously another problem on the trunk between the switches.
**Step 12**

Observe the console of both switches. You should see a Cisco Discovery Protocol message about a native VLAN mismatch on the trunk link.

```
SW1# show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 20 (VLAN0020)
```

```
SW2# show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 15 (VLAN0015)
```

You can verify the VLAN mismatch by viewing the switch port configuration of the FastEthernet0/3 interface on both switches.

Assume that the Branch router has a frame for PC2, which is in VLAN 20. This frame will reach SW1, but because SW1 has VLAN 20 configured as native, it will not be tagged to cross the trunk to SW2. SW2 has VLAN 15 configured as the native VLAN, and for that reason, all arriving frames that are untagged will belong to VLAN 15. The frame will never arrive to PC2.

**Step 13**

On SW1, set VLAN 1 as the native VLAN on the trunk link between the two switches.
Step 14
On SW2, set VLAN 1 as the native VLAN on the trunk link between the two switches.

Step 15
Return to PC1 and ping PC2 at 10.1.20.100 again.

```
C:\>ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:
   Reply from 10.1.20.100: bytes=32 time=4ms TTL=127
   Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
   Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
   Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Ping statistics for 10.1.20.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

The ping should finally be successful.

Note It can take up to a minute until an incomplete ARP entry on the Branch router expires. If your verification ping was not successful, retry after one minute.

Step 16
Save the configurations on the switches SW1 and SW2.

Activity Verification
No additional verification is needed in this task.
Lab 1-2: Optimizing STP

Activity Overview

Objectives

In this lab, you will optimize STP. When you have completed this activity, you will be able to meet these objectives:

- Verify STP operation
- Influence root bridge selection
- Implement STP PortFast
- Implement STP BPDU guard

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>[no] debug spanning-tree event</td>
<td>Enables or disables STP event debugging.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>show interfaces interface</td>
<td>Displays the interface status and statistics.</td>
</tr>
<tr>
<td>show spanning-tree summary</td>
<td>Displays the STP summary of port states and STP operation information.</td>
</tr>
<tr>
<td>show spanning-tree vlan vlan</td>
<td>Displays spanning-tree information for the specified VLAN.</td>
</tr>
<tr>
<td>show spanning-tree vlan vlan bridge detail</td>
<td>Displays detailed spanning-tree status and configuration of a bridge.</td>
</tr>
<tr>
<td>show spanning-tree vlan vlan root detail</td>
<td>Displays detailed spanning-tree status and configuration of the root bridge.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays VLAN status.</td>
</tr>
<tr>
<td>[no] shutdown</td>
<td>Enables or disables interface.</td>
</tr>
<tr>
<td>[no] spanning-tree bpduguard enable</td>
<td>Enables or disables the STP BPDU guard feature on the port.</td>
</tr>
<tr>
<td>spanning-tree portfast</td>
<td>Enables the STP PortFast feature on the port.</td>
</tr>
<tr>
<td>spanning-tree vlan vlan root primary</td>
<td>Forces this switch to be the root bridge for the specified VLAN.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Statically configures an interface for trunking.</td>
</tr>
<tr>
<td>switchport nonegotiate</td>
<td>Disables DTP on an interface.</td>
</tr>
<tr>
<td>switchport trunk allowed vlan vlan_list</td>
<td>Specifies VLANs that are allowed over the trunk link.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.
<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0/1</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.
Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. A trunk is configured on the link between switches SW1 and SW2. SW1 switch and the Branch router are connected by a single trunk link. The figure illustrates the trunk and VLAN setup.

IP Routing

As the figure shows, OSPF is set up as the routing protocol on both routers.

Task 1: Verify STP Operation

In this task, you will verify STP operation on the switches. First, you will determine which STP mode is running on the switches. You will then determine which switch is selected as the STP root bridge and which port is being put into the blocking state by STP.

Activity Procedure

Complete the following steps:

Step 1

On the SW1 and SW2 switches, enable the FastEthernet 0/4 port. Configure both ports as trunks and allow only VLANs 1, 10, and 20 to go across the trunk. Disable DTP negotiation on both ports.

SW1 and SW2 are now connected with two links.
Step 2

On SW1 and SW2, examine the STP mode that is running. The output of the `show spanning-tree summary` command displays the STP mode.

```
SW1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

Name       Blocking  Listening  Learning  Forwarding  STP Active
----------- ---------- ---------- ---------- ---------- ----------
VLAN0001    0         0         0          3          3
VLAN0010    0         0         0          4          4
VLAN0020    0         0         0          3          3
----------- ---------- ---------- ---------- ---------- ----------
3 vlans     0         0         0          10         10

SW2#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

Name       Blocking  Listening  Learning  Forwarding  STP Active
----------- ---------- ---------- ---------- ---------- ----------
VLAN0001    1         0         0          1          2
VLAN0010    1         0         0          1          2
VLAN0020    1         0         0          2          3
----------- ---------- ---------- ---------- ---------- ----------
3 vlans     3         0         0          4          7
```

The STP mode running on the SW1 and SW2 should be PVST.
**Step 3**

On SW1 and SW2, use the `show spanning-tree vlan 1 root detail` command to verify which switch is the STP root bridge.

```
SW1#show spanning-tree vlan 1 root detail
VLAN0001
 Root ID    Priority    32769
 Address     001e.145e.4980
This bridge is the root
 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
SW2#show spanning-tree vlan 1 root detail
VLAN0001
 Root ID    Priority    32769
 Address     001e.145e.4980
 Cost        19
 Port        3 (FastEthernet0/3)
 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

In the scenario shown, SW1 is selected as the STP root bridge. Because the switch priorities are equal, the MAC addresses will be compared. The switch with the lowest MAC address will become the STP root bridge. In your case, SW2 might be the root bridge if it has the lower MAC address.

To display the SW2 MAC address, use the `show spanning-tree vlan 1 bridge detail` command. Note that the SW2 MAC address is higher than the SW1 MAC address.

```
SW2#show spanning-tree vlan 1 bridge detail
VLAN0001
 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
 Address     001e.147c.6f00
 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```
Step 4

There are two FastEthernet links between switches SW1 and SW2. Switches SW1 and SW2 are connected with the FastEthernet 0/3 and FastEthernet 0/4 ports. On SW1 and SW2, use the `show spanning-tree vlan 1` command to check the STP states of these ports.

Note that the outputs are shown for a network where SW1 is the root bridge.

SW1# `show spanning-tree vlan 1`
```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address 001e.145e.4980
This bridge is the root
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001e.145e.4980
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/13              Desg FWD 19        128.13   P2p
```

SW2# `show spanning-tree vlan 1`
```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address 001e.147c.6f00
Cost 19
Port 3 (FastEthernet0/3)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001e.147c.6f00
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/3               Root FWD 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p
```  

In the scenario shown, only the FastEthernet 0/4 port on SW2 is in the blocking state. By putting one interface into the blocking state, STP prevents Layer 2 loops between the SW1 and SW2 switches.

Activity Verification
No additional verification is needed in this task.

Task 2: Influence Root Bridge Selection
In this task, you will change the STP root bridge selection for all active VLANs. In the previous task, you learned which switch is the root bridge. In this task, you will make the other switch the STP root bridge.
Activity Procedure

Complete the following steps:

Step 1

On SW2, use the `show spanning-tree vlan 20` command to verify the SW2 STP priority for VLAN 20. Check if SW2 is the root bridge for VLAN 20.

```
SW2#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
  Address     001e.145e.4980
  Cost        19
  Port        3 (FastEthernet0/3)
  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
  Address     001e.147c.6f00
  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec

  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/1               Desg FWD 19        128.1    P2p
  Fa0/3               Desg FWD 19        128.3    P2p
  Fa0/4               Desg BLK 19        128.4    P2p
```

Notice that the bridge ID priority is the sum of the configured or default priority and the VLAN ID. In the example here, the (default) priority is 32768 and VLAN ID is 20. The bridge ID sums up to 32788. SW2 is not the root bridge for VLAN 20 in this example.

Step 2

If SW2 is not the STP root bridge in your pod, make it the root bridge for VLAN 20.
**Step 3**

Because SW2 has a lower STP priority than SW1 for VLAN 20, switch SW2 should be the STP root bridge. Verify that SW2 is the STP root bridge for VLAN 20.

```
SW2#show spanning-tree vlan 20
VLAN0020
    Spanning tree enabled protocol ieee
    Root ID    Priority    24596
    Address     001e.147c.6f00
This bridge is the root
    Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
    Bridge ID  Priority    24596 (priority 24576 sys-id-ext 20)
    Address     001e.147c.6f00
    Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
    Aging Time  300 sec
    Interface           Role Sts Cost      Prio.Nbr Type
                       --- ---- --------- -------- --------------------------------
    Fa0/1               Desg FWD 19        128.1    P2p
    Fa0/3               Desg FWD 19        128.3    P2p
    Fa0/4               Desg FWD 19        128.4    P2p
```

**Step 4**

Using the `show vlan` command, verify which VLANs are active on SW1.

```
SW1#show vlan | include active
1    default  active Fa0/2, Fa0/4, Fa0/5, Fa0/6
10   VLAN0010 active Fa0/1
20   VLAN0020 active
```

In the example there are three active VLANs on SW1: VLAN 1, VLAN 10, and VLAN 20.

**Step 5**

Make SW1 the STP root bridge for VLAN 1 and VLAN 10 (if it is not already).
Step 6

Verify that SW1 is now the STP root bridge for VLANs 1 and 10.

SW1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
  Address     001e.145e.4980
  This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    24577  (priority 24576 sys-id-ext 1)
  Address     001e.145e.4980
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time   300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/3               Desg FWD 19        128.3    P2p
  Fa0/4               Desg FWD 19         128.4    P2p
  Fa0/13              Desg FWD 19        128.13   P2p

SW1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
  Address     001e.145e.4980
  This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    24586  (priority 24576 sys-id-ext 10)
  Address     001e.145e.4980
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time   300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/1               Desg FWD 19        128.1    P2p
  Fa0/3               Desg FWD 19         128.3    P2p
  Fa0/4               Desg FWD 19         128.4    P2p
  Fa0/13              Desg FWD 19        128.13   P2p

Activity Verification

No additional verification is needed in this task.

Task 3: Implement STP PortFast

First, you will determine how long it takes for a switch port to become fully operational when a host is connected. You will then configure a switch port connecting the host with the STP PortFast feature. You will again test how long it takes for the switch port to become fully operational. You will notice improvement in the switch port behavior.

Activity Procedure

Complete the following steps:
**Step 1**

On SW1, shut down the FastEthernet 0/1 port. PC1 is connected to the SW1 FastEthernet 0/1 port.

In the example, there are three active VLANs on SW2: VLAN 1, VLAN 10, and VLAN 20.

**Step 2**

On SW1, use the **debug spanning-tree events** command to enable STP event debugging.

```
SW1#debug spanning-tree events
Spanning Tree event debugging is on
```

STP event debugging will show you exactly how long it takes for the port to become fully operational after you enable the router interface.

**Step 3**

On SW1, enable the FastEthernet 0/1 port and examine the debugging output. Wait until the FastEthernet 0/1 port on SW1 is in the forwarding state.

```
Aug 30 08:05:42.704: set portid: VLAN0010 Fa0/1: new port id 8001
Aug 30 08:05:42.704: STP: VLAN0010 Fa0/1 -> listening
Aug 30 08:05:43.115: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Aug 30 08:05:44.122: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Aug 30 08:05:57.711: STP: VLAN0010 Fa0/1 -> learning
Aug 30 08:06:12.719: STP[10]: Generating TC trap for port FastEthernet0/1
Aug 30 08:06:12.719: STP: VLAN0010 sent Topology Change Notice on Fa0/3
Aug 30 08:06:12.744: STP: VLAN0010 sent Topology Change Notice on Fa0/3

Note that there is approximately 30 seconds between these two events:  
- FastEthernet 0/1 enters the listening state at Aug 30 08:05:42.704.  
- FastEthernet 0/1 enters the forwarding state at Aug 30 08:06:12.719.

**Step 4**

On SW1, configure FastEthernet 0/1 with the STP PortFast feature.
**Step 5**

Perform the test again by disabling and enabling the SW1 FastEthernet 0/1 port. On SW1, examine the debugging output.

```
Aug 30 08:27:42.685: STP: VLAN0010 sent Topology Change Notice on Fa0/3
Aug 30 08:27:42.685: STP[10]: Generating TC trap for port FastEthernet0/1
Aug 30 08:27:44.682: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
Aug 30 08:27:45.529: set portid: VLAN0010 Fa0/1: new port id 8001
Aug 30 08:27:45.529: STP: VLAN0010 Fa0/1 ->jump to forwarding from blocking
Aug 30 08:27:46.728: STP: VLAN0010 heard root 33274-000f.34f9.9200 on Fa0/1
Aug 30 08:27:46.737: STP: VLAN0010 Topology Change rcvd on Fa0/1
Aug 30 08:27:46.737: STP: VLAN0010 sent Topology Change Notice on Fa0/3
Aug 30 08:27:47.525: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
```

Note that after you enabled the STP PortFast feature, it takes less than a second for the port to become fully operational. STP puts the port immediately into the forwarding state.

**Step 6**

On SW1, use the `no debug all` command to disable all debugging.

```
SW1#no debug all
All possible debugging has been turned off
```

**Activity Verification**

No additional verification is needed in this task.

**Task 4: Implement STP BPDU Guard**

In this task, you will enable the STP BPDU guard feature. For testing purposes, you will enable the feature on a port that is connected to another switch. When the switch receives a BPDU from another switch, the port enters the down state, with an error-disable message.

**Activity Procedure**

Complete the following steps:

**Step 1**

On SW1, use the `debug spanning-tree events` command to enable STP event debugging.

```
SW1#debug spanning-tree events
Spanning Tree event debugging is on
```

The STP event debugging will show you what happens when STP BPDU guard is enabled on the port and a BPDU is received.
**Step 2**

On SW1, enable the STP BPDU guard feature on the FastEthernet 0/3 port and examine the debugging output. The FastEthernet 0/3 port connects to SW2.

```
Aug 30 09:12:29.875: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/3 with BPDU Guard enabled. Disabling port.
Aug 30 09:12:29.875: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/3, putting Fa0/3 in err-disable state
Aug 30 09:12:30.882: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
Aug 30 09:12:31.888: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
```

Note that the BPDU guard feature immediately disables the port because a BPDU was received from SW2.

**Step 3**

On SW1, use the `show interfaces FastEthernet 0/3` command to verify that the FastEthernet 0/3 port is down.

```
SW1#show interfaces FastEthernet 0/3
FastEthernet0/3 is down, line protocol is down (err-disabled)
    Hardware is Fast Ethernet, address is 001e.147c.bd03 (bia 001e.147c.bd03)
    MTU 1500 bytes, BW 10000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

Note the message “err-disabled” next to “line protocol is down,” which means that the port was disabled by the BPDU guard feature.

**Step 4**

To make the FastEthernet 0/3 port operational on SW1, disable the STP BPDU guard feature. You also need to disable and enable the port.

**Step 5**

On SW1, use the `show interfaces FastEthernet 0/3` command to verify that the FastEthernet 0/3 port is up and operational.

```
SW1#show interfaces FastEthernet 0/3
FastEthernet0/3 is up, line protocol is up (connected)
    Hardware is Fast Ethernet, address is 001e.147c.bd03 (bia 001e.147c.bd03)
    MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```
Step 6

On SW1, use the no debug all command to disable all debugging.

```
SW1#no debug all
All possible debugging has been turned off
```

Step 7

Save the configurations on the switches SW1 and SW2.

Activity Verification

No additional verification is needed in this task.
Lab 1-3: Configuring EtherChannel

Activity Overview

Objectives

In this lab, you will become familiar with EtherChannel technology. When you have completed this activity, you will be able to meet these objectives:

- Configure EtherChannel
- Verify EtherChannel redundancy

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
**Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>channel-group channel_id mode active</code></td>
<td>Configures an interface or interfaces as EtherChannel bundle members using LACP in active mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface range interface_range</code></td>
<td>Enters interface range configuration mode.</td>
</tr>
<tr>
<td><code>show etherchannel port-channel</code></td>
<td>Displays port channel interface information.</td>
</tr>
<tr>
<td><code>show interfaces interface</code></td>
<td>Displays interface status and statistics.</td>
</tr>
<tr>
<td><code>show spanning-tree vlan vlan_id</code></td>
<td>Verifies spanning tree configuration for a VLAN.</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>

**Job Aids**

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.
The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. A trunk is configured on each of the two links between switches SW1 and SW2. SW1 and the Branch router are connected by a single trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing
As the figure shows, OSPF is set up as the routing protocol on both routers.

Task 1: Configure EtherChannel
In this task, you will first verify that STP blocked one of the ports between the switches. Then you will configure an EtherChannel bundle between the SW1 and SW2 switches to use both available interfaces to increase bandwidth and provide redundancy between the switches.

Activity Procedure
Complete the following steps:
Step 1

On SW2, verify the spanning-tree configuration for VLAN 10. Your output should look like this example:

```plaintext
SW2# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID  Priority    24586
  Address     001e.147c.6f00
  Cost        19
  Port        3 (FastEthernet0/3)
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
  Address     001e.145e.4980
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec

  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/3               Root FWD 19        128.3    P2p
  Fa0/4               Altn BLK 19        128.4    P2p
```

You should see that FastEthernet0/3 is in the forwarding state and FastEthernet0/4 is in the blocking state. Thus, only one link between the switches is in a forwarding state, because of STP. In the next step, you will bundle both interfaces into an EtherChannel to use both interfaces to increase bandwidth and provide redundancy.

Step 2

On SW1, configure FastEthernet0/3 and FastEthernet0/4 interfaces as EtherChannel members. Use 1 as the port channel identifier and configure LACP in the active mode.

Step 3

On SW2, configure the FastEthernet0/3 and FastEthernet0/4 interfaces as EtherChannel members. Use 1 as the port channel identifier and configure LACP in the active mode.

Activity Verification

You have completed this task when you attain these results:
Step 1

On SW2, verify the spanning-tree configuration for VLAN 10.

```
SW2# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority  24586
  Address    001e.147c.6f00
  Cost       12
  Port       64  (Port-channel1)
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority 32778 (priority 32768 sys-id-ext 10)
  Address    001e.145e.4980
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time 300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Po1                 Root FWD 12        128.64   P2p
```

Before you had ports FastEthernet 0/3 and 0/4 listed, now there is one single interface, Port-channel 1, that bundled the two interfaces.

Step 2

On SW1, verify the state of the port channel interface:

```
SW1# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
<output omitted>
```

Step 3

On SW2, verify the state of the port channel interface:

```
SW2# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
<output omitted>
```
Step 4

On SW1, display the port channel interface information:

```
SW1#show etherchannel port-channel
  Channel-group listing:
  ----------------------
  Group: 1
  -------------
  Port-channels in the group:
  ---------------------------
  Port-channel: Po1    (Primary Aggregator)
  ------------
  Age of the Port-channel   = 0d:00h:29m:43s
  Logical slot/port   = 2/1          Number of ports = 2
  HotStandBy port = null
  Port state          = Port-channel Ag-Inuse
  Protocol            =   LACP
  Port security       = Disabled
  Ports in the Port-channel:
  Index   Load   Port     EC state        No of bits
  +------------------+-----------
  0     00     Fa0/3    Active             0
  0     00     Fa0/4    Active             0
  Time since last port bundled: 0d:00h:29m:39s    Fa0/4
```

Step 5

On SW2, display the port channel interface information:

```
SW2#show etherchannel port-channel
  Channel-group listing:
  ----------------------
  Group: 1
  -------------
  Port-channels in the group:
  ---------------------------
  Port-channel: Po1    (Primary Aggregator)
  ------------
  Age of the Port-channel   = 0d:00h:31m:06s
  Logical slot/port   = 2/1          Number of ports = 2
  HotStandBy port = null
  Port state          = Port-channel Ag-Inuse
  Protocol            =   LACP
  Port security       = Disabled
  Ports in the Port-channel:
  Index   Load   Port     EC state        No of bits
  +------------------+-----------
  0     00     Fa0/3    Active             0
  0     00     Fa0/4    Active             0
  Time since last port bundled: 0d:00h:30m:41s    Fa0/4
```
Step 6

On SW1, verify the spanning tree configuration for VLAN 10. You should see that the EtherChannel interface appears as a single interface to STP.

```
SW1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
  Address     001e.145e.4980
  Cost        12
  Port        64 (Port-channel1)
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
  Address     001e.147c.6f00
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/1               Desg FWD 19       128.1    P2p
  Fa0/13              Desg FWD 19       128.13   P2p
  Po1                 Root FWD 12       128.64   P2p
```

Task 2: Verify EtherChannel Redundancy

In this task, you will verify EtherChannel redundancy by shutting down one of the ports in the EtherChannel bundle. You will observe the connectivity between the PCs while shutting down the port.

Activity Procedure

Complete the following steps:

Step 1

Access PC1. Open a command prompt and trigger a continuous ping to PC2 at 10.1.20.100. Leave the command prompt open.

```
c:\>ping 10.1.20.100 -t
Pinging 10.1.20.100 with 32 bytes of data:
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=9ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
<output omitted>
```

Step 2

Access SW1.
**Step 3**

Shut down the FastEthernet0/3 interface. Return to the command prompt on the PC1 and observe the pings.

Were any packets lost when the interface was shut down?

---

**Step 4**

On SW1, display the port channel interface information.

```bash
SW1#show etherchannel port-channel
Channel-group listing:
----------------------
Group: 1

Port-channels in the group:
---------------------------
Port-channel: Po1     (Primary Aggregator)
--------------
Age of the Port-channel   = 0d:00h:01m:47s
Logical slot/port   = 2/1           Number of ports = 1
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
----------------------------------------------
0     00     Fa0/4    Active             0

Time since last port bundled: 0d:00h:01m:11s    Fa0/3
Time since last port Un-bundled: 0d:00h:00m:17s    Fa0/3
```

You should see that only one interface is in the bundle. You should also see how long ago the interface was removed from the EtherChannel bundle.

**Step 5**

Bring the FastEthernet0/3 interface back up.
**Step 6**

On SW1, display the port channel interface information.

```plaintext
SW1#show etherchannel port-channel
     Channel-group listing:
     ----------------------
Group: 1
-------
     Port-channels in the group:
     ---------------------------
Port-channel: Po1   (Primary Aggregator)
-------
Age of the Port-channel   = 0d:00h:10m:21s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
--------------------------
0     00     Fa0/3    Active             0
0     00     Fa0/4    Active             0
--- Time since last port bundled: 0d:00h:00m:05s    Fa0/3
--- Time since last port Un-bundled: 0d:00h:08m:51s    Fa0/3
```

You should see that both interfaces are in the bundle. You should also see how long ago the interface was added back into the EtherChannel bundle.

**Step 7**

Return to PC1 and interrupt the continuous ping using the Ctrl-C combination.

**Step 8**

Save the configurations on the switches SW1 and SW2.

**Activity Verification**

No additional verification is needed in this task.
Lab 2-1: Troubleshooting IP Connectivity

Activity Overview

Objectives

In this activity, you will explore various trouble tickets related to IP connectivity, identify the problems, and correct them. After completing this activity, you will be able to meet these objectives:

- Troubleshoot the default route
- Troubleshoot an ACL problem
- Troubleshoot the default gateway
- Troubleshoot name resolution

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need assistance with configuration or verification of Cisco IOS commands during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>ip access-list extended ACL-name</td>
<td>Configures extended access list and enters extended access list configuration mode.</td>
</tr>
<tr>
<td>ip route network mask next-hop</td>
<td>Configures IP static route.</td>
</tr>
<tr>
<td>permit protocol source destination eq port</td>
<td>Adds permit statement into extended access list.</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>Verifies IP connectivity.</td>
</tr>
<tr>
<td>show interfaces interface</td>
<td>Displays interface status and statistics.</td>
</tr>
<tr>
<td>show ip access-lists</td>
<td>Displays IP access lists.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays interface IP setup.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays IP routing table.</td>
</tr>
<tr>
<td>telnet ip_address [tcp_port]</td>
<td>Uses Telnet to connect to the IP address—with an optional TCP port, it opens Telnet to a specified TCP port.</td>
</tr>
<tr>
<td>traceroute ip_address</td>
<td>Traces IP address.</td>
</tr>
</tbody>
</table>

Refer to this list if you need assistance with configuration or verification of Windows commands during the lab activity.

### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd directory</td>
<td>Changes directory in the command prompt</td>
</tr>
<tr>
<td>ipconfig</td>
<td>Displays interface adapter IP settings</td>
</tr>
<tr>
<td>notepad file</td>
<td>Lunches Microsoft Notepad application and opens specified file</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>Verifies IP connectivity</td>
</tr>
<tr>
<td>tracert ip_address</td>
<td>Traces IP address</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>Device</td>
<td>Hardware</td>
<td>Operating System</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Device</td>
<td>Interface</td>
<td>IP Address/Subnet Mask</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel and a trunk is configured on it. SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.

**IP Routing**

As the figure shows, OSPF is set up as the routing protocol on both routers.
Task 1: Troubleshoot the Default Route

You have been informed that the user in VLAN 10 cannot establish Telnet or HTTP to the server. As a network engineer, you have to troubleshoot and correct the problem. You will run your tests from the switch where users connect. The senior network engineer has confirmed that the problem is not between the SW1 switch and the Branch router. You also found out that the name server should be resolved into IP address 172.16.1.100.

Interface Serial 0/0/0 on the Branch router is shut down and will stay shut down throughout this lab. Branch should only have connectivity to the HQ router through the GigabitEthernet0/1 interface.

Activity Procedure

Complete the following steps:

Step 1

On SW1, verify that you can ping the IP address of the server (172.16.1.100).

```
SW1#ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

The ping is not successful. From the output, you can see that a destination is unreachable and an error PDU is received.

The table below lists the possible output characters from the ping facility:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point indicates the receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period indicates that the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench (destination too busy).</td>
</tr>
<tr>
<td>M</td>
<td>Could not fragment.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime is exceeded.</td>
</tr>
</tbody>
</table>
**Step 2**

On SW1, do a trace to the IP address of the server (172.16.1.100).

```
SW1#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to Server (172.16.1.100)
  1 10.1.1.1   0 msec 8 msec 0 msec
  2 10.1.1.1 !H  *  !H
```

From the `traceroute` command output, you can see that the host is unreachable and the last hop that answers is from IP 10.1.1.1. This means that there is a possible problem on the router with IP address 10.1.1.1.

From the network diagram, you find out that IP address 10.1.1.1 is on the Branch router. You will continue troubleshooting on the Branch router.

The table lists the characters that can appear in the `traceroute` command output.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nn msec</td>
<td>For each node, the round-trip time in milliseconds for the specified number of probes</td>
</tr>
<tr>
<td>*</td>
<td>The probe timed out</td>
</tr>
<tr>
<td>A</td>
<td>Administratively prohibited (for example, an access list)</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench (destination too busy)</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable</td>
</tr>
<tr>
<td>T</td>
<td>Timeout</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type</td>
</tr>
</tbody>
</table>
Step 3

On the Branch router, verify that interface GigabitEthernet0/1, which connects to the Internet, is operational.

```
Branch# show interfaces GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 5475.d08e.9ad9 (bia 5475.d08e.9ad9)
  Description: Link to HQ
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  <output omitted>
```

The interface is fully operational.

Step 4

On the Branch router, verify that there is a route to the server (172.16.1.100). There should be a static route configured on the Branch router.

```
Branch# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
       Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
    C    10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
    L    10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
    C    10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
    L    10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
    C    10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
    L    10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
  209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
    C    209.165.201.0/27 is directly connected, GigabitEthernet0/1
    L    209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

The Branch router has no specific route to the server. Moreover, there is no default route configured.
**Step 5**

On the Branch router, configure the default route with the next-hop IP address **209.165.201.2**.

Verify the routing table once again.

```
Branch#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 209.165.201.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.201.2
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
  C      10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
  L      10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
  C      10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
  L      10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
  C      10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
  L      10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
  C    209.165.201.0/27 is directly connected, GigabitEthernet0/1
  L    209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

The configured default route should appear as a static route, and the gateway of last resort should be shown in the routing table of the Branch router.

**Activity Verification**

You have completed this task when you attain this result:

**Step 1**

On SW1, verify that you can ping the IP address of the server (172.16.1.100).

```
SW1#ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```

The ping is successful.

**Task 2: Troubleshoot an ACL**

In this task, you will continue troubleshooting by checking whether the user in VLAN 10 is able to reach the server via Telnet and HTTP. The user on PC1 should only be allowed HTTP, Telnet, traceroute, and ping traffic types to and from the server at 172.16.1.100.
Activity Procedure
Complete the following steps:

Step 1
On SW1, use Telnet and try to connect to 172.16.1.100 on ports 23 (Telnet) and 80 (HTTP).

```
SW1#telnet 172.16.1.100 23
Trying 172.16.1.100, 80 ...
% Destination unreachable; gateway or host down
SW1#telnet 172.16.1.100 80
Trying 172.16.1.100, 80 ...
% Destination unreachable; gateway or host down
```

There is no connectivity between SW1 and the server at 172.16.1.100 through ports 23 and 80.

Step 2
On SW1, trace to the IP address of the server (172.16.1.100).

```
SW1#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to Server (172.16.1.100)
  1 10.1.1.1 0 msec 8 msec 0 msec
    2 10.1.1.1 !A * !A
```

From the `traceroute` output, you can see that packets with IP address 10.1.1.1 are administratively prohibited by the router. There may be an ACL that prohibits Telnet and HTTP as well. You will continue troubleshooting on the Branch router.

Step 3
On the Branch router, examine the interfaces to see if any ACLs are used.

```
Branch#show ip interface | include GigabitEthernet|access list
GigabitEthernet0/0 is up, line protocol is up
  Outgoing access list is not set
  Inbound access list is not set
GigabitEthernet0/0.1 is up, line protocol is up
  Outgoing access list is not set
  Inbound access list is not set
GigabitEthernet0/0.10 is up, line protocol is up
  Outgoing access list is not set
  Inbound access list is not set
GigabitEthernet0/0.20 is up, line protocol is up
  Outgoing access list is not set
  Inbound access list is not set
GigabitEthernet0/1 is up, line protocol is up
  Outgoing access list is Outbound-ACL
  Inbound access list is not set
```

Notice that there is an ACL, Outbound-ACL, set as outgoing on the GigabitEthernet0/1 interface.
**Step 4**

On the Branch router, examine the Outbound-ACL ACL.

```console
Branch#show ip access-lists Outbound-ACL
Extended IP access list Outbound-ACL
  10 permit icmp any any
  20 permit tcp any any eq ftp
  30 permit tcp any any eq ftp-data
```

The ACL that is displayed is permitting all ICMP traffic, but from TCP, only ports FTP and FTP-DATA are permitted. All other protocols and ports are denied. To allow users to access the server via Telnet and HTTP, you need to adjust the ACL entries on the Branch router.

**Step 5**

On the Branch router, adjust Outbound-ACL to permit Telnet (23) and HTTP (80) ports in TCP.

**Step 6**

From SW1, verify the establishment of Telnet and HTTP sessions to the server (172.16.1.100).

```console
SW1#telnet 172.16.1.100
Trying 172.16.1.100 ... Open
HQ>exit
[Connection to 172.16.1.100 closed by foreign host]
SW1#

SW1#telnet 172.16.1.100 80
Trying 172.16.1.100, 80 ... Open
exit
```

Telnet connection to standard port 23 is successful, as well as Telnet connection to HTTP port 80 (indicated by the "... Open" response). Now it is very likely that the user in VLAN 10 will be able to reach the server via both protocols.
Step 7

Issue a `traceroute` command from SW1 to 172.16.1.100. Response should still not be successful.

Which configuration step is missing to have a successful `traceroute` response?

```
SW1# traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to 172.16.1.100
  1 10.1.1.1 0 msec 8 msec 0 msec
  2 10.1.1.1 !A * !A
```

Activity Verification
No additional verification is needed in this task.

Task 3: Troubleshoot the Default Gateway and Name Resolution Settings

In this task, you will troubleshoot the default gateway and name resolution setup on PC1, which is connected to VLAN 10.

From the network diagram, you learned that the default gateway for VLAN 10 is 10.1.10.1. Additionally, the senior network engineer has confirmed that no DNS server is set in the domain. Users will need to set local name resolution mapping on their PCs to be able to connect to the server without specifying an IP address.

Activity Procedure
Complete the following steps:

Step 1
On PC1, open the command prompt and verify that a ping to the server is `not` successful.

```
C:\> ping Server
Ping request could not find host Server. Please check the name and try again.
C:\>
```

PC1 cannot resolve the name server into IP address 172.16.1.100.
Step 2

On PC1, use the command prompt and browse to the C:\Windows\System32\drivers\etc directory. Open the Hosts file with the Notepad application.

C:\> cd C:\Windows\System32\drivers\etc
C:\Windows\System32\drivers\etc> notepad hosts

The Notepad application opens the Hosts file.

Step 3

On the PC1 Hosts file, enter the mapping of the IP address 172.16.1.100 to the name server.

172.16.1.100 Server

Save the Hosts file as shown.

PC1 now has a local DNS entry to resolve the name server into IP address 172.16.1.100.
**Step 4**

On PC1, from the command prompt, use the `tracert` command to locate the problem.

```
C:\Windows\System32\drivers\etc>tracert Server
Tracing route to Server [172.16.1.100]
over a maximum of 30 hops:
    1 Windows7 [10.1.10.100] reports: Destination host unreachable.
Trace complete.
C:\Windows\System32\drivers\etc>
```

From the output, you can see that PC1 is not able to find the destination. It may be a problem in the local route on PC1.

**Step 5**

On PC1, use the `ipconfig` command to verify that the default gateway is correctly set.

```
C:\Windows\System32\drivers\etc>ipconfig
Windows IP Configuration
Ethernet adapter LAB:
    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::dc6d:98e9:82b7:d637%13
    IPv4 Address. . . . . . . . . . . : 10.1.10.100
    Subnet Mask . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . : 10.1.10.10
<output omitted>
```

The default gateway is not correctly set. The default gateway IP address should be 10.1.10.1.
**Step 6**

On PC1, change the default gateway from 10.1.10.10 to 10.1.10.1 on the Ethernet adapter that connects to SW1.

To change the default gateway on PC1, right-click to the Network icon in the Task menu and choose the **Open Network and Sharing Center** option.

In the Network and Sharing Center window, choose **Change Adapter Settings** from the left menu.

Right-click the LAN adapter and choose **Properties**.

The LAN Properties window opens. Choose **Internet Protocol version 4 (TCP/IPv4)** and click **Properties**.
Change the default gateway from 10.1.10.10 to 10.1.10.1 and click **OK**.
Click **OK** in the Properties window. You have changed the default gateway on PC1.

**Step 7**

Save the changes you made on the Branch router.

**Activity Verification**

You have completed this task when you attain this result:
**Step 1**

On PC1, open the command prompt and verify that the ping to the server is successful.

```
C:\Windows\System32\drivers\etc>ping Server
Pinging Server [172.16.1.100] with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=2ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Windows\System32\drivers\etc>
```

The ping to the server should be successful.

**Step 2**

On PC1, use the PuTTY application and establish a Telnet connection to the server.

![PuTTY Configuration](image)

Establishment of a Telnet session to the server should be successful.
Step 3

Access PC1. Open Internet Explorer and try to connect to the server. If you are prompted for credentials, enter ccna as the username and cisco as the password.

You should be successful in establishing the HTTP session.
Lab 3-1: Implementing EIGRP

Activity Overview

Objectives

In this activity, you will configure EIGRP and investigate EIGRP neighbor events. After completing this activity, you will be able to meet these objectives:

- Verify network connectivity
- Configure and verify basic EIGRP
- Investigate EIGRP neighbor events
- Remove OSPF routing

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug eigrp neighbors</code></td>
<td>Debugs neighbor events.</td>
</tr>
<tr>
<td><code>network network [wildcard_mask]</code></td>
<td>Enables the routing protocol on the interfaces that match the specified network. Using the wildcard mask, you can further narrow the networks that you want to advertise.</td>
</tr>
<tr>
<td><code>[no] router eigrp autonomous-system</code></td>
<td>Disables and enables the EIGRP routing process.</td>
</tr>
<tr>
<td><code>[no] router ospf area area_number</code></td>
<td>Disables and enables the OSPF routing process.</td>
</tr>
<tr>
<td><code>show ip eigrp interfaces</code></td>
<td>Show interfaces that are enabled for the EIGRP process.</td>
</tr>
<tr>
<td><code>show ip eigrp neighbors</code></td>
<td>Show EIGRP neighbors.</td>
</tr>
<tr>
<td><code>show ip eigrp topology</code></td>
<td>Show the EIGRP topology table.</td>
</tr>
<tr>
<td><code>show ip protocols</code></td>
<td>Displays values about routing protocols and routing protocol timer information that is associated with the router.</td>
</tr>
<tr>
<td><code>show ip route [destination_network]</code></td>
<td>Displays the routing table. You can specify the destination network to investigate which route is being used for routing for this specific network.</td>
</tr>
<tr>
<td><code>undebug all</code></td>
<td>Turns off all debugging.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

### Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.
The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
**IP Routing**

The figure shows that OSPF is set up as the routing protocol on both routers.

**Task 1: Verify Connectivity to Remote Network**

In this task, you will verify connectivity from PC1 to the server in the 172.16.1.0/24 network. Note that the server is simulated by a loopback interface on the HQ router.
**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, bring up the Serial 0/0/0 interface.

**Step 2**

Issue a **ping** command from PC1 to the server with an IP address of 172.16.1.100. The ping should be successful.

```
C:\Users\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data;
Reply from 172.16.1.100: bytes=32 time<44ms TTL=128
Reply from 172.16.1.100: bytes=32 time<82ms TTL=128
Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round-trip times in milliseconds:
    Minimum = 36ms, Maximum = 82ms, Average = 49ms
```

**Step 3**

Investigate the routing table of the Branch router. Identify the route entry that points toward the 172.16.1.0/24 network.

```
Branch>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
       C  10.1.1.0/24 is directly connected, GigabitEthernet0/0
       L  10.1.1.1/32 is directly connected, GigabitEthernet0/0
       C  10.1.10.0/24 is directly connected, GigabitEthernet0/0.1
       L  10.1.10.1/32 is directly connected, GigabitEthernet0/0.1
       C  10.1.20.0/24 is directly connected, GigabitEthernet0/0.2
       L  10.1.20.1/32 is directly connected, GigabitEthernet0/0.2
172.16.0.0/24 is subnetted, 1 subnets
O  172.16.1.100 [110/65] via 192.168.1.2, 00:14:47, Serial0/0/0
  192.168.1.2/32 is variably subnetted, 2 subnets, 2 masks
     C  192.168.1.10/24 is directly connected, Serial0/0/0
     L  192.168.1.1/32 is directly connected, Serial0/0/0
  209.165.201.0/27 is subnetted, 1 subnets
     O  209.165.201.0 [110/65] via 192.168.1.2, 00:14:47, Serial0/0/0
```

Was this route manually put in the router by the administrator?
Activity Verification
No additional verification is needed in this task.

Task 2: Configure and Verify EIGRP
In this task, you will configure and verify EIGRP on the Branch router. The HQ router is already configured with EIGRP.

Activity Procedure
Complete the following steps:

Step 1
Enable the EIGRP routing process on the Branch router. Use an EIGRP AS number of 1.

Step 2
Configure EIGRP so that the interface toward the LAN (GigabitEthernet0/0 subinterfaces) and the interface toward the WAN (Serial0/0/0) are running EIGRP.
Activity Verification

Step 1

On the Branch router, issue the `show ip protocols` command, verify that the EIGRP process is turned on, and that networks 192.168.1.0 and 10.0.0.0 are being routed.

```
Branch#show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  10.1.1.0 0.0.0.255 area 0
  10.1.10.0 0.0.0.255 area 0
  10.1.20.0 0.0.0.255 area 0
  192.168.1.0 0.0.0.255 area 0
Routing Information Sources:
  Gateway         Distance      Last Update
  1.1.1.1              110      00:00:33
Distance: (default is 110)
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 209.165.201.1
  Topology: 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
  Maximum path: 4
  Maximum hopcount 100
  Maximum metric variance 1
  Automatic Summarization: disabled
  Maximum path: 4
Routing for Networks:
  10.1.1.0/24
  10.1.10.0/24
  10.1.20.0/24
  192.168.1.0/24
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.1.2           90      00:00:12
Distance: internal 90 external 170
```
**Step 2**

On the Branch router, investigate the routing table. Verify that the route to network 172.16.1.0, acquired through EIGRP, is present.

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

        Dec 24 11:24:05.623: %SYS-5-CONFIG_I: Configured from console by console
        + - replicated route, % - next hop override
        Gateway of last resort is 209.165.201.2 to network 0.0.0.0
        S*    0.0.0.0/0 [1/0] via 209.165.201.2
            10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
        C      10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
        L      10.1.1.0/24 is directly connected, GigabitEthernet0/0.10
        L      10.1.1.0/24 is directly connected, GigabitEthernet0/0.20
        172.16.0.0/24 is subnetted, 1 subnets
        D      172.16.1.0 [90/2297856] via 192.168.1.2, 00:00:46, Serial0/0/0
            192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
        C      192.168.1.0/24 is directly connected, Serial10/0/0
        L      192.168.1.0/24 is directly connected, Serial10/0/0
        O      192.168.2.0/24 [110/1064] via 192.168.1.2, 00:12:24, Serial10/0/0
            209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
        C      209.165.201.0/27 is directly connected, GigabitEthernet0/1
        L      209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

**Step 3**

On the Branch router, issue the **show ip eigrp interfaces** command to verify that the Serial0/0/0, GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20 interfaces are participating in the EIGRP routing process.

```
Branch#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)

Interface Peers Un/Reliable Xmit Queue PeerQ Mean Pacing Time Multicast Pending Routes
G10/0.1 0 0/0 0/0 0 0/0 0 0
G10/0.10 0 0/0 0/0 0 0/0 0 0
G10/0.20 0 0/0 0/0 0 0/0 0 0
Se0/0/0.0 1 0/0 0/0 1289 0/16 6420 0
```
Step 4

On the Branch router, verify that you have an EIGRP neighbor.

```
Branch#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
  (sec)         (ms)       Cnt Num
0   192.168.1.2             Se0/0/0           11 00:00:12   48   288  0  4
```

Step 5

Issue the `show ip route 172.16.1.0` command on the Branch router. Notice that the route to the 172.16.1.0/24 network is now routed by EIGRP because EIGRP (AD = 90) is more trustworthy than OSPF (AD = 110).

```
Branch#show ip route 172.16.1.0
Routing entry for 172.16.1.0/24
Known via "eigrp 1", distance 90, metric 2297856, type internal
Redistributing via eigrp 1
Last update from 192.168.1.2 on Serial0/0/0, 00:10:24 ago
Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:10:24 ago, via Serial0/0/0
    Route metric is 2297856, traffic share count is 1
    Total delay is 25000 microsec, minimum bandwidth is 1544 Kb
    Reliability 255/255, minimum MTU 1500 B
    Loading 1/255, Hops 1
```

Step 6

Investigate the EIGRP topology table on the Branch router. Identify the FD and reported distance to the 172.16.1.0/24 network. In the following example output, the FD to 172.16.1.0/24 is 2,297,856: the HQ reported distance of 128,256 plus the Branch cost of 2,169,600.

```
Branch#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status
P 192.168.1.0/24, 1 successors, FD is 2169856
   via Connected, Serial10/0/0
P 172.16.1.0/24, 1 successors, FD is 2297856
   via 192.168.1.2 (2297856/128256), Serial10/0/0
P 10.1.10.0/24, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0.1
P 10.1.20.0/24, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0.2
P 10.1.1.0/24, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0
```
Task 3: Investigate Neighbor Events

In this task, you will debug EIGRP. This will help you know what to look for when you need to troubleshoot EIGRP issues.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, display the EIGRP neighbor events with the `debug eigrp neighbors` command.

Step 2

On the Branch router, shut down the Serial0/0/0 interface. Observe the output of the `debug` command, telling you which EIGRP neighbor was lost.

```
Sep 20 07:58:55.135: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.2 (Serial0/0/0) is down: interface down
Sep 20 07:58:55.135: Going down: Peer 192.168.1.2 total=0 stub 0, iidb-stub=0 iid-all=0
Sep 20 07:58:55.139: EIGRP: BFD client initialized
Sep 20 07:58:55.139: EIGRP(0:1):[bfd_reg] state:2 iidb:Se0/0/0 peer:192.168.1.2
Sep 20 07:58:55.139: EIGRP: Handle deallocation failure [0]
Sep 20 07:58:55.139: EIGRP: Neighbor 192.168.1.2 went down on Serial0/0/0
Sep 20 07:58:57.131: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively down
Sep 20 07:58:58.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
```

Step 3

Wait 10 seconds and then enable the Serial0/0/0 interface. Observe the output, informing you that an EIGRP adjacency was established.

```
Sep 20 08:04:21.691: %SYS-5-CONFIG_I: Configured from console by console
Sep 20 08:04:22.671: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.2 (Serial0/0/0) is down: peer restarted
Sep 20 08:04:22.671: Going down: Peer 192.168.1.2 total=0 stub 0, iidb-stub=0 iid-all=0
Sep 20 08:04:22.671: EIGRP(0:1):[bfd_reg] state:2 iidb:Se0/0/0 peer:192.168.1.2
Sep 20 08:04:22.671: EIGRP: Handle deallocation failure [0]
Sep 20 08:04:22.671: EIGRP: Neighbor 192.168.1.2 went down on Serial0/0/0
Sep 20 08:04:24.659: EIGRP: Neighbor(192.168.1.2) not yet found
Sep 20 08:04:27.199: EIGRP: New peer 192.168.1.2
Sep 20 08:04:27.199: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.2 (Serial0/0/0) is up: new adjacency
```
Step 4

Turn off debugging on the Branch router:

```
Branch#undebug all
```

Activity Verification
No additional verification is needed in this task.

Task 4: Disable OSPF Routing Process
In this task, you will disable the OSPF routing process, therefore leaving EIGRP alone to route.

Activity Procedure
Complete the following steps:
**Step 1**

Issue the `show ip protocols` command and identify the message groups for OSPF and EIGRP.

```
Branch#show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router ID 10.1.1.1
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4
    Routing for Networks:
        10.1.1.0 0.0.0.255 area 0
        10.1.10.0 0.0.0.255 area 0
        10.1.20.0 0.0.0.255 area 0
        192.168.1.0 0.0.0.255 area 0
    Routing Information Sources:
        Gateway Distance Last Update
        1.1.1.1 110 00:16:03
    Distance: (default is 110)
Routing Protocol is "eigrp 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Default networks flagged in outgoing updates
    Default networks accepted from incoming updates
    EIGRP-IPv4 Protocol for AS(1)
        Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
        NSF-aware route hold timer is 240
        Router-ID: 209.165.201.1
        Topology : 0 (base)
            Active Timer: 3 min
            Distance: internal 90 external 170
        Maximum path: 4
        Maximum hopcount 100
        Maximum metric variance 1
        Automatic Summarization: disabled
    Routing for Networks:
        10.1.1.0/24
        10.1.10.0/24
        10.1.20.0/24
        192.168.1.0
    Routing Information Sources:
        Gateway Distance Last Update
        192.168.1.2 90 00:04:27
    Distance: internal 90 external 170
```

**Step 2**

Disable the OSPF routing process on the Branch router.

By doing this, you are finishing the migration from OSPF to EIGRP.
Step 3

Issue the `show ip protocols` command and verify that there is no more OSPF message group. Only EIGRP remains.

Branch#`show ip protocols`

```
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(1)
   Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
   NSF-aware route hold timer is 240
   Router-ID: 209.165.201.1
   Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1
   Automatic Summarization: disabled
   Maximum path: 4
Routing for Networks:
   10.1.1.0/24
   10.1.10.0/24
   10.1.20.0/24
   192.168.1.0
Routing Information Sources:
   Gateway         Distance      Last Update
       192.168.1.2           90      00:04:27
Distance: internal 90 external 170
```

Step 4

Save the changes that you made to the configuration on the Branch router.

Activity Verification

You have completed this task when you attain this result:
**Step 1**

Issue a **ping** command from PC1 to the server with an IP address of 172.16.1.100 to verify that connectivity is still there after you dismantled OSPF. The ping should be successful.

C:\Users\Administrator>**ping 172.16.1.100**
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time<44ms TTL=128
Reply from 172.16.1.100: bytes=32 time<82ms TTL=128
Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 36ms, Maximum = 82ms, Average = 49ms
Lab 3-2: Troubleshooting EIGRP

Activity Overview

Objectives

In this activity, you will troubleshoot connectivity problems that are related to EIGRP. After completing this activity, you will be able to meet these objectives:

- Troubleshoot EIGRP neighbors
- Troubleshoot routing table issues

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Copies the device running configuration file to the startup configuration</td>
</tr>
<tr>
<td>network network wildcard_mask</td>
<td>Enables the routing protocol on the interfaces that match the specified</td>
</tr>
<tr>
<td></td>
<td>network. Using the wildcard mask, you can further narrow the networks that</td>
</tr>
<tr>
<td></td>
<td>you want to advertise.</td>
</tr>
<tr>
<td>[no] passive interface interface</td>
<td>Disables and enables the passive interface for the EIGRP routing process</td>
</tr>
<tr>
<td>router eigrp autonomous-system</td>
<td>Enables EIGRP</td>
</tr>
<tr>
<td>show ip eigrp interfaces</td>
<td>Show interfaces that are enabled for the EIGRP process</td>
</tr>
<tr>
<td>show ip eigrp neighbors</td>
<td>Show EIGRP neighbors</td>
</tr>
<tr>
<td>show ip eigrp topology</td>
<td>Show the EIGRP topology table</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays IP-specific information of an interface</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays values about routing protocols and routing protocol timer</td>
</tr>
<tr>
<td></td>
<td>information that are associated with the router</td>
</tr>
<tr>
<td>show ip route [destination_network]</td>
<td>Displays the routing table. You can specify the destination network to</td>
</tr>
<tr>
<td></td>
<td>investigate which route is being used for routing for this specific network.</td>
</tr>
</tbody>
</table>

Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.
The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel and a trunk is configured on it. SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
**Trunk and VLAN Setup**

**IP Routing**

EIGRP is running in AS 1 between the HQ and Branch routers. The figure illustrates the EIGRP setup.

**Task 1: Troubleshoot Basic Connectivity**

In this task, you will follow the instructions to troubleshoot connectivity issues in your network.

**Activity Procedure**

Complete the following steps:
**Step 1**

You receive reports that PC1 is unable to ping the server at 172.16.1.100.

When you receive reports like these, always make sure that the reports are accurate. From PC1, ping the server 172.16.1.100. The ping should *not* be successful.

```
C:\Users\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
  Reply from 10.1.10.1: Destination host unreachable.
  Reply from 10.1.10.1: Destination host unreachable.
  Reply from 10.1.10.1: Destination host unreachable.
  Reply from 10.1.10.1: Destination host unreachable.
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

**Step 2**

From PC1, ping its default gateway. The ping is successful. This tells you that the first hop is OK and the problem lies somewhere further in the network.

```
C:\Users\Administrator>ping 10.1.10.1
Pinging 10.1.10.1 with 32 bytes of data:
  Reply from 10.1.10.1: bytes=32 time<2ms TTL=128
  Reply from 10.1.10.1: bytes=32 time<1ms TTL=128
  Reply from 10.1.10.1: bytes=32 time<1ms TTL=128
  Reply from 10.1.10.1: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

**Step 3**

From the Branch router, ping the HQ router. The ping should not be successful.

Therefore, the connectivity problem is between the Branch and HQ routers.

```
Branch#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
       ....
Success rate is 0 percent (0/5)
```
**Step 4**

On the Branch router, investigate if the interface toward the HQ router is operational.

```
Branch#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         10.1.1.1        YES manual up                    up
GigabitEthernet0/0.1       10.1.10.1       YES manual up                    up
GigabitEthernet0/0.2       10.1.20.1       YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                192.168.1.1     YES manual administratively down down
```

Why is the interface not operational?

**Step 5**

Correct the issue that you identified in the previous step.

**Step 6**

Notice that the Cisco IOS system informs you that the Serial0/0/0 interface is now operational.

```
Sep 21 08:38:38.859: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
Sep 21 08:38:39.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

**Step 7**

You can now repeat the connectivity test from PC1 to the server at 172.16.1.100. The ping is still not successful.

```
C:\Users\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
  Reply from 10.1.10.1: Destination host unreachable,
  Reply from 10.1.10.1: Destination host unreachable,
  Reply from 10.1.10.1: Destination host unreachable,
  Reply from 10.1.10.1: Destination host unreachable.
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```
Step 8

Investigate if the Branch router has a path to the 172.16.1.0/24 network. Your output should be similar to output shown. There is no path to the remote network at 172.16.1.0/24.

```
Branch#show ip route
Codes:  L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
     o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
     + - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
  C   10.1.1.0/24 is directly connected, GigabitEthernet0/0
  L   10.1.1.1/32 is directly connected, GigabitEthernet0/0
  C   10.1.10.0/24 is directly connected, GigabitEthernet0/0.1
  L   10.1.10.1/32 is directly connected, GigabitEthernet0/0.1
  C   10.1.20.0/24 is directly connected, GigabitEthernet0/0.2
  L   10.1.20.1/32 is directly connected, GigabitEthernet0/0.2
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
  C   192.168.1.0/24 is directly connected, Serial0/0/0
  L   192.168.1.1/32 is directly connected, Serial0/0/0
```

Proceed to the next task, where you will continue with your troubleshooting.

Activity Verification
No additional verification is needed in this task.

Task 2: Troubleshooting EIGRP Neighbors
In this task, you will troubleshoot EIGRP neighbor issues.

Activity Procedure
Complete the following steps:

Step 1

Investigate if routers in your pod are EIGRP neighbors.

```
Branch#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
```

What are the possible causes of routers not establishing neighbor adjacency?
**Step 2**

Investigate the possible causes of missing neighbor adjacencies as you identified them in the previous step. Use the `telnet` command from the Branch router to access the HQ router.

Why are the two routers not becoming neighbors?

---

Branch#`show ip protocols`

*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates

EIGRP-IPv4 Protocol for AS(1)
 Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 NSF-aware route hold timer is 240
 Router-ID: 10.1.20.1
 Topology: 0 (base)
 Active Timer: 3 min
 Distance: internal 90 external 170
 Maximum path: 4
 Maximum hopcount 100
 Maximum metric variance 1
 Automatic Summarization: disabled
 Maximum path: 4

Routing for Networks:
  192.168.1.0
Passive Interface(s):
  Serial0/0/0

Routing Information Sources:

  Gateway         Distance      Last Update
  Distance: internal 90 external 170

Branch#`telnet 192.168.1.2`

Trying 192.168.1.2 ... Open

HQ#`show ip protocols`

*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4

Routing for Networks:
  172.16.1.0 0.0.0.255 area 0
  192.168.1.0 0.0.0.255 area 0
  192.168.2.0 0.0.0.255 area 0
  209.165.201.0 0.0.0.31 area 0

Routing Information Sources:

  Gateway         Distance      Last Update
  Distance: (default is 110)

Routing Protocol is "eigrp 1"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Step 3
Correct the issue that you identified in the previous step.

Step 4
Notice that you were informed of a new EIGRP adjacency.

Activity Verification
No additional verification is needed in this task.

Task 3: Troubleshooting Routing Table Issues
In this task, you will troubleshoot routing table issues.

Activity Procedure
Complete the following steps:
Step 1

You can now repeat the connectivity test from PC1 to the HQ router. The ping is still not successful.

What are the possible causes of this lack of connectivity?
Step 2

Check if the HQ router is advertising the 172.16.1.0/24 network.

Does the Branch router know the route to the 172.16.1.0/24 network?

What would be your next step in troubleshooting connectivity?

```
HQ# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.255 area 0
    192.168.2.0 0.0.0.255 area 0
    209.165.201.0 0.0.0.31 area 0
  Routing Information Sources:
    Gateway Distance Last Update
    Distance: (default is 110)
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 172.16.1.100
    Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
    Automatic Summarization: disabled
    Maximum path: 4
    Routing for Networks:
      172.16.0.0
      192.168.1.0
  Routing Information Sources:
    Gateway Distance Last Update
    Distance: internal 90 external 170
Branch# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0
C 10.1.10.0/24 is directly connected, GigabitEthernet0/0.1
L 10.1.10.1/32 is directly connected, GigabitEthernet0/0.1
C 10.1.20.0/24 is directly connected, GigabitEthernet0/0.2
L 10.1.20.1/32 is directly connected, GigabitEthernet0/0.2
172.16.0.0/24 is subnetted, 1 subnets
D 172.16.1.0 [90/2297856] via 192.168.1.2, 00:02:05, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Serial0/0/0
L 192.168.1.1/32 is directly connected, Serial0/0/0

Step 3

Issue the show ip protocols command on the Branch router and identify the issue that is causing the lack of connectivity.

Branch#show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(1)
   Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
   NSF-aware route hold timer is 240
   Router-ID: 10.1.20.1
   Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1
   Automatic Summarization: disabled
   Maximum path: 4
Routing for Networks:
   192.168.1.0
   Routing Information Sources:
      Gateway         Distance      Last Update
      192.168.1.2     90       00:03:06
      Distance: internal 90 external 170

The Branch router is not routing for networks 10.1.1.0/24, 10.1.10.0/24, and 10.1.20.0/24. There are network commands that are missing in the configuration.
Step 4
Correct the issue that you identified in the previous step.

Step 5
Issue a ping command from PC1 to the server with an IP address of 172.16.1.100. The ping should be successful.

```
C:\Users\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
  Reply from 172.16.1.100: bytes=32 time<44ms TTL=128
  Reply from 172.16.1.100: bytes=32 time<82ms TTL=128
  Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
  Reply from 172.16.1.100: bytes=32 time<36ms TTL=128
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
         Minimum = 36ms, Maximum = 82ms, Average = 49ms
```

Step 6
Save the changes that you made to the configuration on the Branch router.

Activity Verification
No additional verification is needed in this task.
Lab 3-3: Implementing EIGRP for IPv6

Activity Overview

Objectives

In this activity, you will configure and verify EIGRP for IPv6. After completing this lab activity, you will be able to meet this objective:

- Enable IPv6 routing and configure an IPv6 address on an interface
- Enable EIGRP for IPv6

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration or verification of Cisco IOS command assistance during the lab activity.
Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>ipv6 address ipv6_address/mask</td>
<td>Sets an IPv6 address for an interface and the subnet mask.</td>
</tr>
<tr>
<td>ipv6 eigrp as_number</td>
<td>Configures EIGRP for IPv6 on an interface.</td>
</tr>
<tr>
<td>ipv6 router eigrp as_number</td>
<td>Creates and enters the IPv6 EIGRP router submode.</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enables IPv6 unicast routing.</td>
</tr>
<tr>
<td>no shutdown</td>
<td>EIGRP for IPv6 has a shutdown feature. The routing process should be in no shutdown mode in order to start running.</td>
</tr>
<tr>
<td>ping destination_address</td>
<td>Pings the specified address (IPv4 or IPv6).</td>
</tr>
<tr>
<td>show ipv6 eigrp interfaces</td>
<td>Displays IPv6 EIGRP interfaces.</td>
</tr>
<tr>
<td>show ipv6 eigrp neighbors</td>
<td>Displays IPv6 EIGRP neighbors.</td>
</tr>
<tr>
<td>show ipv6 eigrp topology</td>
<td>Displays the IPv6 EIGRP topology table.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the interface IPv6 setup.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays the IP routing table.</td>
</tr>
</tbody>
</table>

Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>HQ</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN1)</td>
<td>2001:db8 :0A01:100::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN10)</td>
<td>2001:db8 :0A01:A00::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN20)</td>
<td>2001:db8 :0A01:1400::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8 :D1A5:C900::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>2001:db8 :C0A8:100::1/64</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8 :D1A5:C900::2/64</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0</td>
<td>2001:db8 :C0A8:100::2/64</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>2001:db8 :AC10:100::64/64</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically.</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically.</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel and a trunk is configured on it. SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing

Your pod has an HQ router configured with EIGRP for IPv6.

Task 1: Enable IPv6 on the Interfaces

In this task, you will enable IPv6 routing and configure an IPv6 address on the interface.

IPv6 is already correctly configured on the HQ router, so you will only configure the Branch side.
**Activity Procedure**
Complete the following steps:

**Step 1**

**Step 2**
On the Branch router, configure the IPv6 address on the serial interface connected to the HQ router. Also, configure IPv6 addresses on subinterfaces GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20.

Use the IPv6 address as shown on the visual objective of this exercise. The subnet mask should be /64.

**Activity Verification**
You have completed this task when you attain these results:

**Step 1**
On the Branch router, verify that IPv6 is enabled. Verify that the global IPv6 unicast address is correctly configured on Serial0/0/0, GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20.

```
Branch# show ipv6 interface
GigabitEthernet0/0.1 is up, line protocol is up
   IPv6 is enabled, link-local address is FE80::FE99:47FF:FEE5:2700
   No Virtual link-local address(es):
   Global unicast address(es):
       2001:DB8:A01:100::1, subnet is 2001:DB8:A01:100::/64
       <output omitted>
GigabitEthernet0/0.10 is up, line protocol is up
   IPv6 is enabled, link-local address is FE80::FE99:47FF:FEE5:2700
   No Virtual link-local address(es):
   Global unicast address(es):
       2001:DB8:A01:A00::1, subnet is 2001:DB8:A01:A00::/64
       <output omitted>
GigabitEthernet0/0.20 is up, line protocol is up
   IPv6 is enabled, link-local address is FE80::FE99:47FF:FEE5:2700
   No Virtual link-local address(es):
   Global unicast address(es):
       2001:DB8:A01:1400::1, subnet is 2001:DB8:A01:1400::/64
       <output omitted>
Serial0/0/0 is up, line protocol is up
   IPv6 is enabled, link-local address is FE80::FE99:47FF:FEE5:2700
   No Virtual link-local address(es):
   Description: Link to HQ
   Global unicast address(es):
       2001:DB8:C0A8:100::1, subnet is 2001:DB8:C0A8:100::/64
       <output omitted>
```

**Task 2: Enable IPv6 EIGRP**
In this task, you will enable EIGRP for IPv6.

The HQ router is already correctly configured with EIGRP for IPv6.
Activity Procedure
Complete the following steps:

Step 1

Step 2
On the Branch router, configure IPv6 EIGRP routing on Serial0/0/0, GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20.

Activity Verification
You have completed this task when you attain these results:

Step 1
On the Branch router, verify on which interfaces that IPv6 EIGRP is enabled:

```
Branch# show ip eigrp interfaces
EIGRP-IPv6 Interfaces for AS(1)
Interface Peers Un/Reliable PeerQ Un/Reliable Mean Pacing Time Multicast Pending Routes
Se0/0/0 1 0/0 0/0 0/0 686 0/0 0/16 3400 0
Gi0/0.1 0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
Gi0/0.10 0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
Gi0/0.20 0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
```

IPv6 EIGRP is enabled on the first serial interface.

Step 2
On the Branch router, verify which IPv6 EIGRP neighbors are seen by the router:

```
Branch# show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq Cnt Num
0 Link-local address: Se0/0/0 12 00:27:05 61 366 0 2
FE80::21E:7AFF:FEA3:5F30
```

The IPv6 EIGRP neighbor is specified with a link-local address.
Step 3

On the Branch router, verify which routes are in the IPv6 EIGRP topology:

```
Branch#show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(1)/ID(209.165.201.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 2001:DB8:A01:100::/64, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0.1
P 2001:DB8:A01:1400::/64, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0.20
P 2001:DB8:C0A8:100::/64, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 2001:DB8:A01:A00::/64, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0.10
P 2001:DB8:AC10:100::/64, 1 successors, FD is 2297856
   via FE80::FE99:47FF:FEE5:2670 (2297856/128256), Serial10/0/0
```

The topology table holds successor routes to different destination networks. In your network, there are no feasible successor routes.

Step 4

On the Branch router, verify which IPv6 routes are learned via IPv6 EIGRP:

```
Branch#show ipv6 route eigrp
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
   U - Per-user Static route, M - MIPv6
   I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
   O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
   ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
   D - EIGRP, EX - EIGRP external
D 2001:DB8:AC10:100::/64 [90/2297856]
   via FE80::21E:7AFF:FEA3:5F30, Serial10/0/0
```

There is one EIGRP route present in the IPv6 routing table.
**Step 5**

Go to PC1 and use the `ipconfig` command to verify that it has a global unicast IPv6 address configured.

Stateless address configuration is a feature that is unique to IPv6. It means that the client picks its own address based on the prefix being advertised on its connected interface. All Cisco devices have the ability to participate in stateless autoconfiguration.

---

**Step 6**

On PC1, issue a `ping` command to the server at 2001:db8:ac10:100::64. This end-to-end connectivity test should be successful.
Lab 4-1: Configuring Multiarea OSPF

Activity Overview

Objectives

In this activity, you will remove the EIGRP routing protocol and replace it with multiarea OSPF. After completing this activity, you will be able to meet these objectives:

- Configure multiarea OSPF
- Verify multiarea OSPF configuration

Visual Objective

The figure illustrates what you will accomplish in this activity.
Visual Objective for Lab 4-1: Configuring Multiarea OSPF

Detailed Visual Objective

Required Resources
No additional resources are required for this lab.

Command List
The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>ip address ip_address mask</td>
<td>Configures the IP address on an interface.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>network network wildcard_mask area area_id</td>
<td>Enables the OSPF routing protocol for the specified area on the interfaces that match the specified network.</td>
</tr>
<tr>
<td>[no] router eigrp autonomous-system</td>
<td>Disables or enables the EIGRP routing process.</td>
</tr>
<tr>
<td>router ospf process_id</td>
<td>Enables the OSPF routing process.</td>
</tr>
<tr>
<td>show ip ospf interfaces brief</td>
<td>Shows interfaces that are enabled for the OSPF routing process.</td>
</tr>
<tr>
<td>show ip ospf neighbors</td>
<td>Shows OSPF neighbors.</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays the routing protocol status and routing protocol timer information that is associated with the router.</td>
</tr>
<tr>
<td>show ip route [ospf]</td>
<td>Displays the routing table.</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>Uses Telnet to connect to the specified host.</td>
</tr>
</tbody>
</table>

Job Aids

These job aids are available to help you complete the lab activity.

Pod Information

Each pod has two switches, two routers, and two PCs. The server is simulated on the Headquarters router by the IP address that is assigned to the loopback interface.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter s</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

![Topology and IP Addressing](image)

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>
**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.

![Trunk and VLAN Setup](image)

**IP Routing**

EIGRP is running in AS 1 between the HQ and Branch routers. The figure illustrates the EIGRP setup.

![IP Routing](image)
**Task 1: Configure Multiarea OSPF**

In this task, you will first remove EIGRP (with the AS of 1) and then configure multiarea OSPF on the Branch router. You will configure the LAN interfaces for OSPF Area 1 and the WAN interface for OSPF Area 0. The Headquarters router has been preconfigured.

**Activity Procedure**

Complete the following steps:

**Step 1**

Access the Branch router.

**Step 2**

Remove the EIGRP routing process from the Branch router. Recall that EIGRP has a lower administrative distance than OSPF. Without removing EIGRP, OSPF routes would not be considered when installing routes into the routing table.

**Step 3**

Configure the Loopback10 interface on the Branch router. Assign the 10.100.100.100/32 IP address to the interface. This IP address will serve as router ID for OSPF.

**Step 4**

Create the OSPF routing process on the Branch router. Use 1 as the process ID number.

**Step 5**

Enable OSPF for Area 0 on the WAN interface (Serial0/0/0).

**Step 6**

Enable OSPF for Area 1 on the LAN interfaces (GigabitEthernet0/0 subinterfaces) and on the Loopback10 interface.

**Activity Verification**

You have completed this task when you attain this result.
Step 1

Verify OSPF process status:

```
Branch#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.100.100.100
It is an area border router
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  10.1.1.0 0.0.0.255 area 1
  10.1.10.0 0.0.0.255 area 1
  10.1.20.0 0.0.0.255 area 1
  10.100.100.100 0.0.0.0 area 1
  192.168.1.0 0.0.0.255 area 0
Reference bandwidth unit is 100 mbps
Routing Information Sources:
  Gateway         Distance      Last Update
  1.1.1.1          110      00:00:53
Distance: (default is 110)
```

You should see the OSPF router ID set to the IP address of the Loopback10 interface. You should also see that OSPF is enabled on the WAN interface for Area 0 and on the LAN and Loopback interfaces for Area 1.

Task 2: Verify Multiarea OSPF

In this task, you will verify multiarea OSPF configuration and operations.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, verify OSPF adjacencies:

```
Branch#show ip ospf neighbor
Neighbor ID Pri State       Dead Time Address     Interface
  1.1.1.1  0 FULL/ - 00:00:33 192.168.1.2 Serial0/0/0
```

You should see the Headquarters router as a neighbor. The Headquarters router ID is 1.1.1.1. The neighbors should be in FULL state.
Step 2

On the Branch router, investigate which interfaces are enabled for OSPF:

```
Branch# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/0      1     0               192.168.1.1/24     64    P2P   1/1
Lo10         1     1               10.100.100.100/32  1     LOOP 0/0
Gi0/0.20     1     1               10.1.20.1/24       1     DR    0/0
Gi0/0.10     1     1               10.1.10.1/24       1     DR    0/0
Gi0/0.1      1     1               10.1.1.1/24        1     DR    0/0
```

Step 3

On the Branch router, verify OSPF routes in the routing table:

```
Branch# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, p - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 1 subnets
O       172.16.1.0 [110/65] via 192.168.1.2, 00:00:04, Serial0/0/0
```

You should see the 172.16.1.0/24 network in the routing table. Is the network seen as an interarea or intra-area route? Why?

Step 4

From the Branch router, use Telnet to connect to the Headquarters router:

```
Branch# telnet 192.168.1.2
Trying 192.168.1.2 ... Open
HQ#
```
**Step 5**

On the Headquarters router, verify OSPF routes in the routing table:

```
HQ# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA  10.1.1.0/24 [110/65] via 192.168.1.1, 00:06:41, Serial0/0/0
O IA  10.1.10.0/24 [110/65] via 192.168.1.1, 00:07:36, Serial0/0/0
O IA  10.1.20.0/24 [110/65] via 192.168.1.1, 00:07:36, Serial0/0/0
O IA  10.100.100.100/32 [110/65] via 192.168.1.1, 00:20:57, Serial0/0/0
```

You should see the LAN networks in the routing table. Are the LAN networks seen as an interarea or intra-area route? Why?

**Step 6**

Access PC1:

**Step 7**

Open a command prompt on PC1. Ping the server at 172.16.1.100. The ping should be successful:

```
C:\Windows\system32> ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=37ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
          Minimum = 36ms, Maximum = 37ms, Average = 36ms
```

**Step 8**

Save the changes that you made to the configuration on the Branch router:

**Activity Verification**

No additional verification is needed in this task.
Lab 4-2: Troubleshooting Multiarea OSPF

Activity Overview

Objectives

In this lab, you will be presented with two multiarea OSPF troubleshooting tickets. After this lab activity, you will be able to meet these objectives:

- Troubleshoot OSPF neighbor issues
- Troubleshoot OSPF routing table issues

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>debug ip ospf adj</td>
<td>Enables debugging of OSPF adjacency events.</td>
</tr>
<tr>
<td>network network wildcard_mask area area_id</td>
<td>Enables the OSPF routing protocol for the specified area on the interfaces that match the specified network.</td>
</tr>
<tr>
<td>[no] passive-interface interface</td>
<td>Disables the interface as a passive interface.</td>
</tr>
<tr>
<td>ping ip_address source interface</td>
<td>Pings an IP address from the specified interface.</td>
</tr>
<tr>
<td>router ospf process_id</td>
<td>Enables the OSPF routing process.</td>
</tr>
<tr>
<td>show ip interface interface</td>
<td>Displays the interface status and other IP-related information.</td>
</tr>
<tr>
<td>show ip ospf interfaces</td>
<td>Shows OSPF-related information on interfaces.</td>
</tr>
<tr>
<td>show ip ospf neighbors</td>
<td>Shows OSPF neighbors.</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays routing protocol status and routing protocol timer information that are associated with the router.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the routing table.</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>Uses Telnet to connect to the specified host.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

### Pod Information

Each pod has two switches, two routers, and two PCs. The server is simulated on the Headquarters router by the IP address that is assigned to the loopback interface.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Branch</td>
<td>Tunnel0</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>HQ</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>HQ</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>HQ</td>
<td>Tunnel0</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>
Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
Task 1: Troubleshoot OSPF Neighbor Issues

You have been informed that users behind the Branch router cannot communicate with the server in the central location. As a junior network engineer, you have to troubleshoot and correct the problem. A senior network engineer has confirmed that the problem is in an OSPF adjacency between the Headquarters and Branch routers.

**Activity Procedure**

Complete the following steps:

**Step 1**

Access the Branch router.
**Step 2**

From the Branch router, ping the server at 172.16.1.100. Use GigabitEthernet0/0.10 as the source interface:

```
Branch# ping 172.16.1.100 source GigabitEthernet0/0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
Packet sent with a source address of 10.1.10.1
.....
Success rate is 0 percent (0/5)
```

The ping should not be successful. This indicates a problem in connectivity between users behind the Branch router and the server in the central location.

**Step 3**

Examine the routing table on the Branch router. Verify if you received the 172.16.1.0/24 route from the Headquarters router:

```
Branch# show ip route 172.16.1.0
% Network not in table
```

You should see no route on the 172.16.1.0/24 network in the routing table.

**Step 4**

Verify OSPF neighbors:

```
Branch# show ip ospf neighbor
Branch#
```

You should see no OSPF neighbors on the Branch router.

**Step 5**

Verify if the interface connecting the Branch router to the Headquarters router is enabled on the Branch router. Use the visual objective to determine the interface:

```
Branch# show ip interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
<output omitted>
```

Is the Serial0/0/0 interface enabled on the Branch router?
Step 6

Verify if OSPF is enabled on the Serial 0/0/0 interface of the Branch router:

Branch# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
   Outgoing update filter list for all interfaces is not set
   Incoming update filter list for all interfaces is not set
   Router ID 10.100.100.100
   It is an area border router
   Number of areas in this router is 2. 2 normal 0 stub 0 nssa
   Maximum path: 4
Routing for Networks:
   10.1.1.0 0.0.0.255 area 1
   10.1.10.0 0.0.0.255 area 1
   10.1.20.0 0.0.0.255 area 1
   10.100.100.100 0.0.0.0 area 1
   192.168.1.0 0.0.0.255 area 0
   <output omitted>

For which OSPF area is the interface enabled?
Step 7

Verify if the Serial0/0/0 interface is configured as a passive interface:

```
Branch# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.100.100.100
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.0 0.0.0.255 area 1
    10.1.10.0 0.0.0.255 area 1
    10.1.20.0 0.0.0.255 area 1
    10.100.100.100 0.0.0.0 area 1
    192.168.1.0 0.0.0.255 area 0
  Passive Interface(s):
    Embedded-Service-Engine0/0
    GigabitEthernet0/0
    GigabitEthernet0/1
    GigabitEthernet0/2
    GigabitEthernet0/3
    Loopback10
    Serial0/0/0

<output omitted>
```

Is the Serial0/0/0 interface configured as a passive interface? Why are adjacencies not established over passive interfaces?

Step 8

Correct the problem by configuring the Serial0/0/0 interface as a nonpassive interface.
Step 9

Verify if the Serial0/0/0 interface is configured as an OSPF nonpassive interface:

Branch# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.100.100.100
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  10.1.1.0 0.0.0.255 area 1
  10.1.10.0 0.0.0.255 area 1
  10.1.20.0 0.0.0.255 area 1
  10.100.100.100 0.0.0.0 area 1
  192.168.1.0 0.0.0.255 area 0
Passive Interface(s):
  Embedded-Service-Engine0/0
  GigabitEthernet0/0
  GigabitEthernet0/1
  GigabitEthernet0/2
  GigabitEthernet0/3
  Loopback10
<output omitted>

Serial0/0/0 should no longer be configured as a passive interface.

Step 10

Verify if the Branch router established OSPF adjacency with the Headquarters router after you corrected the problem:

Branch# show ip ospf neighbor
Branch#

You should still see no OSPF neighbors on the Branch router. Proceed with troubleshooting the OSPF adjacency.
**Step 11**
Enable debugging of OSPF adjacencies using the `debug ip ospf adj` command and observe the output in the console:

```
Branch# debug ip ospf adj
OSPF adjacency debugging is on
Branch#
Oct 30 09:02:28.471: OSPF-1 ADJ  S0/0/0: Rcv pkt from 192.168.1.2, area 0.0.0.0, mismatched area 0.0.0.1 in the header
```

You should see routers trying to exchange hello packets, but the OSPF area is mismatched and therefore they can not become neighbors. Because the Branch router is configured for a correct OSPF area, the Headquarters router is probably configured for an incorrect OSPF area.

**Step 12**
Disable debugging of OSPF adjacencies using the `no debug ip ospf adj` command.

```
Branch# no debug ip ospf adj
OSPF adjacency debugging is off
```

**Step 13**
Correct the problem by configuring the Serial0/0/0 interface for OSPF Area 0 on the Headquarters router.

**Step 14**
Exit the Telnet session. Verify if the Branch router established an OSPF adjacency with the Headquarters router after you corrected the problem.

```
HQ# exit
[Connection to 192.168.1.2 closed by foreign host]
Branch# show ip ospf neighbors
Neighbor ID      Pri  State          Dead Time  Address       Interface
1.1.1.1          0    FULL/ -        00:00:32  192.168.1.2    Serial0/0/0
```

You should see that the OSPF adjacency was established this time. You successfully corrected the OSPF neighbor issues.

**Activity Verification**
No additional verification is needed in this task.
Task 2: Troubleshoot OSPF Routing Table Issues

Although you corrected the previous trouble ticket, the users still complain about connectivity to the server. You must troubleshoot further and correct the connectivity problem. The senior network engineer still insists that the problem is with a misconfigured OSPF routing protocol.

Activity Procedure

Complete the following steps:

**Step 1**

Examine the routing table on the Branch router again. Verify if you received the 172.16.1.0/24 route from the Headquarters router this time.

```
Branch# show ip route 172.16.1.0
% Network not in table
```

You should still see no route on the 172.16.1.0/24 network in the routing table. It looks like there is a routing table issue on the Headquarters or Branch router that is preventing the Headquarters router from sending a routing update or preventing the Branch router from receiving it.

**Step 2**

Use Telnet to connect to the Headquarters router. Verify if the Headquarters router correctly advertises the 172.16.1.0/24 network:

```
Branch# telnet 192.168.1.2
Trying 192.168.1.2 ... Open
HQ# show ip protocols
<output omitted>
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.1.100
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.255 area 0
    209.165.201.0 0.0.0.31 area 0
<output omitted>
```

Is the Headquarters router correctly advertising the 172.16.1.0/24 network?

**Step 3**

Correct the issue by configuring the Headquarters router to advertise the 172.16.1.0/24 network.
**Step 4**

Save the changes that you made on the Headquarters router.

Exit the Telnet session.

Save the changes that you made on the Branch router.

**Activity Verification**

You have completed this task when you attain these results:

**Step 1**

On the Branch router, examine the routing table. Verify if you received the 172.16.1.0/24 route from the Headquarters router this time.

```
Branch# show ip route 172.16.1.0
Routing entry for 172.16.1.0/24
  Known via "ospf 1", distance 110, metric 66, type intra area
  Last update from 192.168.1.2 on Serial0/0/0, 00:02:28 ago
  Routing Descriptor Blocks:
    * 192.168.1.2, from 172.16.1.100, 00:02:28 ago, via Serial0/0/0
      Route metric is 66, traffic share count is 1
```

**Step 2**

From the Branch router, ping the server at 172.16.1.100. Use GigabitEthernet0/0.10 as a source interface:

```
Branch# ping 172.16.1.100 source GigabitEthernet0/0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
Packet sent with a source address of 10.1.10.1
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The ping should be successful. This indicates that you successfully corrected the routing table issue and restored the connectivity between users behind the Branch router and the server in the central location.
Lab 4-3: Configuring OSPF for IPv6

Activity Overview

Objectives

In this lab, you will remove EIGRP for IPv6 and replace it with the OSPFv3 routing protocol. After this lab activity, you will be able to meet these objectives:

- Configure basic OSPF in an IPv6 network
- Verify the OSPFv3 configuration

Visual Objective

The figure illustrates what you will accomplish in this activity.
Visual Objective for Lab 4-3: Configuring OSPF for IPv6

Required Resources
No additional resources are required for this lab.

Command List
The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration or verification Cisco IOS command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>interface interface</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>ipv6 ospf process-id area area-id</strong></td>
<td>Configures OSPFv3 on an interface.</td>
</tr>
<tr>
<td><strong>ipv6 router eigrp as_number</strong></td>
<td>Enters the IPv6 EIGRP router submode.</td>
</tr>
<tr>
<td><strong>ipv6 router ospf process-id</strong></td>
<td>Creates and enters the OSPFv3 router submode.</td>
</tr>
<tr>
<td><strong>ping destination_address</strong></td>
<td>Pings the specified address (IPv4 or IPv6).</td>
</tr>
<tr>
<td><strong>router-id router-id</strong></td>
<td>Sets the OSPFv3 router ID.</td>
</tr>
<tr>
<td><strong>show ipv6 interface</strong></td>
<td>Displays the interface IPv6 setup.</td>
</tr>
<tr>
<td><strong>show ipv6 ospf</strong></td>
<td>Displays general information about OSPFv3 routing processes.</td>
</tr>
<tr>
<td><strong>show ipv6 ospf interface brief</strong></td>
<td>Displays interfaces that are enabled for the OSPFv3 process.</td>
</tr>
<tr>
<td><strong>show ipv6 ospf neighbor</strong></td>
<td>Lists OSPFv3 neighbors.</td>
</tr>
<tr>
<td><strong>show ipv6 route</strong></td>
<td>Displays the IP routing table.</td>
</tr>
<tr>
<td><strong>shutdown route</strong></td>
<td>Disables EIGRP for IPv6.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

### Pod Information

Each pod has two switches, two routers, and two PCs. The server is simulated on the Headquarters router by the IP address that is assigned to the loopback interface.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>2001:db8:0a01:100::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>2001:db8:0a01:a00::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>2001:db8:0a01:1400::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8:d1a5:c900::1/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>2001:db8:c0a8:100::1/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8:d1a5:c900::2/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>2001:db8:c0a8:100::2/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>2001:db8:ac10:100::64/64</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically</td>
</tr>
</tbody>
</table>

Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing

As the figure shows at the beginning of this lab, your pod has the Headquarters and Branch routers configured with EIGRP for IPv6.

Task 1: Enable OSPFv3

In this task, you will configure and verify OSPFv3.

The Headquarters router is already correctly configured with OSPFv3.
Activity Procedure

Complete the following steps:

Step 1

On the Branch router, configure the OSPFv3 routing process with process ID 1. The router must have router ID 2.2.2.2.

Step 2

On the Branch router, disable the IPv6 EIGRP routing protocol. EIGRP is configured with AS 1.

Step 3

On the Branch router, verify that interfaces Serial0/0/0, GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20 all have IPv6 addresses that are configured:

```
Branch# show ipv6 interface brief
Em0/0                  [administratively down/down]
         unassigned
GigabitEthernet0/0     [up/up]
         unassigned
GigabitEthernet0/0.1   [up/up]
         FE80::FE99:47FF:FE5:2709
         2001:DB8:A01:A00::1
GigabitEthernet0/0.10  [up/up]
         FE80::FE99:47FF:FE5:2709
         2001:DB8:A01:A00::1
GigabitEthernet0/0.20  [up/up]
         FE80::FE99:47FF:FE5:2709
         2001:DB8:A01:A100::1
GigabitEthernet0/1     [administratively down/down]
         unassigned
Serial0/0/0             [up/up]
         FE80::FE99:47FF:FE5:2709
         2001:DB8:C0A8:100::1
Loopback10             [up/up]
         unassigned
```

Step 4

On the Branch router, enable OSPFv3 in Area 0 on interface Serial0/0/0. Enable OSPFv3 in Area 1 on interfaces GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20. Use process ID number 1.

Step 5

Save the changes that you made to the configuration on the Branch router.

Activity Verification

You have completed this task when you attain these results:
**Step 1**

On the Branch router, verify on which interfaces that OSPFv3 is enabled:

```
Branch# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0/0      1     0               6          64    P2P   1/1
Gi0/0.20     1     1               14         1     DR    0/0
Gi0/0.10     1     1               13         1     DR    0/0
Gi0/0.1      1     1               12         1     DR    0/0
```

**Step 2**

On the Branch router, verify that Headquarters is the neighbor. The Headquarters router ID is 1.1.1.1. The state should be "FULL":

```
Branch# show ipv6 ospf neighbor

OSPFv3 Router with ID (10.100.100.100) (Process ID 1)
Neighbor ID     Pri State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:31    6               Serial0/0/0
```
Step 3

On the Branch router, verify general OSPFv3 information:

```
Branch# show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border router
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0000000
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled

Area BACKBONE(0)
  Number of interfaces in this area is 1
  SPF algorithm executed 5 times
  Number of LSA 9. Checksum Sum 0x0479E4
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

Area 1
  Number of interfaces in this area is 3
  SPF algorithm executed 3 times
  Number of LSA 7. Checksum Sum 0x03EFD4
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

The Branch router has router ID 2.2.2.2. It has OSPFv3 configured in Areas 0 (backbone) and 1.

Step 4

On the Branch router, verify which IPv6 routes are learned via OSPFv3:

```
Branch# show ipv6 route ospf
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
         B - BGP, H - Home Agent, MR - Mobile Router, R - RIP
         I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
         D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
         O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
         ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O  2001:DB8::AC10:100::64/128 [110/64] via FE80::21E:7AFF:FEA3:5F30, Serial0/0/0
```
**Step 5**

Go to PC1 and verify that it has a global unicast IPv6 address that is configured using the `ipconfig` command.

Stateless address configuration is a unique feature only to IPv6. It means that clients pick their own address based on the prefix being advertised on their connected interface. All Cisco devices have the ability to participate in stateless autoconfiguration.

![ipconfig_output](image1)

**Step 6**

On PC1, issue a ping to the server at 2001:db8:ac10:100::64. This end-to-end connectivity test should be successful.

![Ping_output](image2)
Lab 5-1: Configuring and Troubleshooting a Serial Connection

Activity Overview

Objectives

In this activity, you will first identify connectivity issues due to misconfigured PPP encapsulation and correct them. In the second part, you will change the encapsulation from PPP to HDLC. After completing this activity, you will be able to meet these objectives:

- Troubleshoot PPP encapsulation
- Configure and verify HDLC encapsulation

Visual Objective

The figures illustrate what you will accomplish in this activity.
Visual Objective for Lab 5-1: Configuring and Troubleshooting a Serial Connection

Detailed Visual Objective

Required Resources
No additional resources are required for this lab.

Command List
The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration or verification Cisco IOS command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>debug ppp authentication</td>
<td>Enables PPP authentication debugging.</td>
</tr>
<tr>
<td>debug ppp negotiation</td>
<td>Enables PPP negotiation debugging.</td>
</tr>
<tr>
<td>disconnect line</td>
<td>Disconnects the Telnet session to the remote host.</td>
</tr>
<tr>
<td>encapsulation hdlc</td>
<td>Enables HDLC encapsulation on the serial interface.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>ping destination_address</td>
<td>Pings the specified IP address.</td>
</tr>
<tr>
<td>ppp authentication chap</td>
<td>Enables CHAP PPP authentication on the serial interface.</td>
</tr>
<tr>
<td>show interface interface</td>
<td>Displays interface setup and statistics.</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays a brief interface status.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td>no debug all</td>
<td>Disables all debugging.</td>
</tr>
<tr>
<td>[no] shutdown</td>
<td>Enables or disables an interface.</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>Connects via Telnet to the specified IP address.</td>
</tr>
<tr>
<td>username username password</td>
<td>Configures a user on the router.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

### Pod Information

Each pod has two switches, two routers, and two PCs. The server is simulated on the Headquarters router by the IP address that is assigned to the loopback interface.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter s</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.
Topologies and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
</tbody>
</table>
### Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing

EIGRP is running in AS 1 between the HQ and Branch routers. The figure illustrates the EIGRP setup.

Task 1: Troubleshoot PPP

In this task, you will troubleshoot PPP encapsulation on the serial link between the Branch and Headquarters routers.

The Branch and Headquarters routers are already configured with PPP encapsulation on the serial interface, but the link is not functional. You will troubleshoot and make changes on the Branch router only.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, verify that the first serial interface is operational.

```
Branch# show ip interface brief
Interface     IP-Address     OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0  unassigned      YES unset  up                    up
GigabitEthernet0/0.1 10.1.1.1        YES manual up                    up
GigabitEthernet0/0.10 10.1.10.1       YES manual up                    up
GigabitEthernet0/0.20 10.1.20.1       YES manual up                    up
GigabitEthernet0/1 209.165.201.1     YES manual administratively down down
Serial0/0/0 192.168.1.1     YES manual up                    down
Loopback10  10.100.100.100  YES manual up                    up
```

The status of the Serial 0/0/0 interface is up, but the protocol is down.
**Step 2**

On the Branch router, verify the encapsulation of the first serial interface.

```
Branch# show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is down
   Hardware is GT96K Serial
   Description: Link to HQ
   Internet address is 192.168.1.1/24
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation PPP, LCP Closed, loopback not set
   Keepalive set (10 sec)
   CRC checking enabled
   Last input 00:00:01, output 00:00:01, output hang never
   Last clearing of "show interface" counters 02:04:40
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: weighted fair
   Output queue: 0/1000/64/0 (size/max total/threshold/drops)
   Conversations 0/1/256 (active/max active/max total)
   Reserved Conversations 0/0 (allocated/max allocated)
   Available Bandwidth 1158 kilobits/sec
<output omitted>
```

Encapsulation on the Serial 0/0/0 interface is correctly set to PPP, but the status of the LCP will be either Closed, ACKsent or REQsent, but not Open.

**Step 3**

On the Branch router, determine the PPP authentication method that is used.

```
Branch# show running-config interface Serial 0/0/0
Building configuration...
Current configuration : 206 bytes
!
interface Serial0/0/0
   description Link to HQ
   ip address 192.168.1.1 255.255.255.0
   encapsulation ppp
   ipv6 address 2001:DB8::CA:8:100:1/64
   ipv6 eigrp 1
   ipv6 ospf 1 area 0
   ppp authentication pap
end
Branch#
```

On the Branch router, the PPP authentication method is PAP.
**Step 4**

On the Branch router, start the **debug ppp negotiation** command and observe the output.

Notice that one end of the serial connection is configured with PAP-type authentication (Branch) and the other side is configured with CHAP (Headquarters).

Turn off all debugging on the Branch router.

```
Branch# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch#
Dec  3 14:30:18.383: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 15
Dec  3 14:30:18.383: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)
Dec  3 14:30:18.383: Se0/0/0 LCP: MagicNumber 0x9967C432 (0x05069967C432)
Dec  3 14:30:18.383: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Branch#
Dec  3 14:30:18.387: Se0/0/0 LCP: O CONFREQ [ACKsent] id 16 len 14
Dec  3 14:30:18.387: Se0/0/0 LCP: AuthProto PAP (0x0304C023)
Dec  3 14:30:18.387: Se0/0/0 LCP: MagicNumber 0x995A9970 (0x0506995A9970)
Branch# no debug all

**Step 5**

On the Branch router, change the PPP authentication method on the Serial 0/0/0 interface from PAP to CHAP. In this way, the authentication types will match.

**Step 6**

On the Branch router, enable PPP authentication debugging using the **debug ppp authentication** command.

**Step 7**

The debug shows PPP authentication messages. Observe that authentication is not successful.

```
*Oct 24 11:53:29.731: Se0/0/0 PPP: Using default call direction
*Oct 24 11:53:29.731: Se0/0/0 PPP: Treating connection as a dedicated line
*Oct 24 11:53:29.731: Se0/0/0 PPP: Session handle[750000B1] Session id[177]
*Oct 24 11:53:29.771: Se0/0/0 CHAP: O CHALLENGE id 1 len 27 from "Branch"
*Oct 24 11:53:29.779: Se0/0/0 CHAP: I CHALLENGE id 1 len 23 from "HQ"
*Oct 24 11:53:29.779: Se0/0/0 PPP: Sent CHAP SENDAUTH Request
*Oct 24 11:53:29.783: Se0/0/0 PPP: Received SENDAUTH Response PASS
*Oct 24 11:53:29.783: Se0/0/0 CHAP: Using hostname from configured hostname
*Oct 24 11:53:29.783: Se0/0/0 CHAP: Using password from AAA
*Oct 24 11:53:29.783: Se0/0/0 CHAP: O RESPONSE id 1 len 27 from "Branch"
*Oct 24 11:53:29.791: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "HQ"
*Oct 24 11:53:29.791: Se0/0/0 PPP: Sent CHAP LOGIN Request
*Oct 24 11:53:29.795: Se0/0/0 PPP: Received LOGIN Response FAIL
*Oct 24 11:53:29.795: Se0/0/0 CHAP: O FAILURE id 1 len 25 msg is "Authentication failed"
```

**Step 8**

The Serial 0/0/0 interface CHAP password should be “cisco.” Examine the configuration on the Branch router.

```
Branch# show running-config | include username
username HQ password 0 Cisco
Branch#
```

Observe that the password for user Headquarters is incorrect. A capital letter is used.

**Step 9**

On the Branch router, change the password for user Headquarters to “cisco.”

**Step 10**

The debug shows PPP authentication messages. Observe that authentication is successful.

```
*Oct 24 12:00:11.283: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Oct 24 12:00:11.287: Se0/0/0 PPP: Using default call direction
*Oct 24 12:00:11.287: Se0/0/0 PPP: Treating connection as a dedicated line
*Oct 24 12:00:11.287: Se0/0/0 PPP: Session handle[DB00005F] Session id[351]
*Oct 24 12:00:11.339: Se0/0/0 CHAP: O CHALLENGE id 1 len 27 from "Branch"
*Oct 24 12:00:11.347: Se0/0/0 CHAP: I CHALLENGE id 1 len 23 from "HQ"
*Oct 24 12:00:11.347: Se0/0/0 PPP: Sent CHAP SENDAUTH Request
*Oct 24 12:00:11.347: Se0/0/0 PPP: Received SENDAUTH Response PASS
*Oct 24 12:00:11.347: Se0/0/0 CHAP: Using hostname from configured hostname
*Oct 24 12:00:11.347: Se0/0/0 CHAP: Using password from AAA
*Oct 24 12:00:11.347: Se0/0/0 CHAP: O RESPONSE id 1 len 27 from "Branch"
*Oct 24 12:00:11.359: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "HQ"
*Oct 24 12:00:11.359: Se0/0/0 PPP: Sent CHAP LOGIN Request
*Oct 24 12:00:11.363: Se0/0/0 PPP: Received LOGIN Response PASS
*Oct 24 12:00:11.367: Se0/0/0 CHAP: O SUCCESS id 1 len 4
*Oct 24 12:00:11.371: Se0/0/0 CHAP: I SUCCESS id 1 len 4
*Oct 24 12:00:11.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

**Step 11**

On the Branch router, disable debugging:

```
Branch# no debug all
All possible debugging has been turned off
Branch#
```

**Activity Verification**

You have completed this task when you attain this result:
Step 1
On the Branch router, you have pinged the Headquarters router (192.168.1.2). The ping should be successful.

```
Branch# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
Branch#
```

Task 2: Enable HDLC Encapsulation
In this task, you will configure and verify HDLC encapsulation on the serial interface.

Because you do not have console access to the Headquarters router, you will use Telnet to connect to the Headquarters router and change the serial interface encapsulation on the Headquarters router first. The serial link will go down, and you will lose the Telnet connection to the Headquarters router. Then you will change serial interface encapsulation on the Branch router, and the link should come up again.

Activity Procedure
Complete the following steps:

Step 1
From the Branch router, use Telnet to connect to the Headquarters router (192.168.1.2).

```
Branch# telnet 192.168.1.2
Trying 192.168.1.2 ... Open
HQ#
```

Step 2
On the Headquarters router, change the encapsulation on the Serial 0/0/0 interface to HDLC.

You will lose Telnet connectivity to the Headquarters router. Get back to the Branch router by pressing Ctrl-Shift-6 and then pressing x.

Step 3
On the Branch router, disconnect the Telnet session to the Headquarters router.

```
Branch# disconnect 1
Closing connection to 192.168.1.2 [confirm]
Branch#
```

Step 4
On the Branch router, change the encapsulation on the Serial 0/0/0 interface to HDLC.
**Step 5**

Save the changes you made on the Branch router.

Use Telnet to connect to the Headquarters router at 192.168.1.2 and save the changes that you made on the Headquarters router.

**Activity Verification**

You have completed this task when you attain this result:

**Step 1**

On the Branch router, you have verified the serial interface encapsulation.

```
Branch# show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
   Hardware is GT96K Serial
   Description: Link to HQ
   Internet address is 192.168.1.1/24
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation HDLC, loopback not set
   Keepalive set (10 sec)
   CRC checking enabled
   Last input 00:00:00, output 00:00:00, output hang never
   Last clearing of "show interface" counters 00:07:47
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: weighted fair
   Output queue: 0/1000/64/0 (size/max total/threshold/drops)
      Conversations 0/1/256 (active/max active/max total)
      Reserved Conversations 0/0 (allocated/max allocated)
   Available Bandwidth 1158 kilobits/sec
<output omitted>
```

The Serial 0/0/0 interface is up, and the encapsulation is HDLC.
Lab 5-2: Establishing a Frame Relay WAN

Activity Overview

Objectives

In this activity, you will configure basic Frame Relay. After completing this activity, you will be able to meet these objectives:

- Configure and verify basic Frame Relay
- Configure and verify Frame Relay subinterfaces
- Remove the Frame Relay configuration

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

No additional resources are required for this lab.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>encapsulation frame-relay</code></td>
<td>Sets encapsulation on an interface to Frame Relay.</td>
</tr>
<tr>
<td><code>encapsulation hdlc</code></td>
<td>Sets encapsulation on an interface to HDLC.</td>
</tr>
<tr>
<td><code>frame-relay interface-dlci dlci</code></td>
<td>Assigns a DLCI to an interface or subinterface.</td>
</tr>
<tr>
<td><code>ip address ip_address mask</code></td>
<td>Configures an IP address on an interface.</td>
</tr>
<tr>
<td><code>interface interface</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface.subinterface point-to-point</code></td>
<td>Creates a subinterface and enters subinterface configuration mode.</td>
</tr>
<tr>
<td><code>ping ip_address</code></td>
<td>Pings the specified IP address.</td>
</tr>
<tr>
<td><code>show frame-relay lmi</code></td>
<td>Displays LMI statistics.</td>
</tr>
<tr>
<td><code>show frame-relay pvc</code></td>
<td>Displays PVC statistics.</td>
</tr>
<tr>
<td><code>show frame-relay map</code></td>
<td>Displays Frame Relay mappings.</td>
</tr>
<tr>
<td><code>show ip ospf interfaces interface</code></td>
<td>Shows OSPF-related information on interfaces.</td>
</tr>
<tr>
<td><code>show ip ospf neighbors</code></td>
<td>Shows OSPF neighbors.</td>
</tr>
<tr>
<td><code>show interfaces interface</code></td>
<td>Displays interface status and counters.</td>
</tr>
<tr>
<td><code>telnet ip_address</code></td>
<td>Connects to a specified host with Telnet.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

### Pod Information

Each pod has two switches, two routers, and two PCs. The server is simulated on the Headquarters router by the IP address that is assigned to the loopback interface.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter s</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.
Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>Device</td>
<td>Interface</td>
<td>IP Address/Subnet Mask</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

**Trunk and VLAN Setup**

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
IP Routing

EIGRP is running in AS 1 between the HQ and Branch routers. The figure illustrates the EIGRP setup.

Task 1: Configure and Verify Basic Frame Relay

In this task, you will configure and verify basic Frame Relay on the Serial0/0/0 interface of the Branch router. The router will use LMI and Inverse ARP to learn available DLCIs and the mapping between a DLCI and remote IP address.

**Note**

In an actual scenario, you would have a Frame Relay network with Frame Relay switches between the Branch and Headquarters routers. In this lab environment, the Headquarters router acts as both a Frame Relay switch and a router.

**Activity Procedure**

Complete the following steps:

**Step 1**

Access the Branch router.

**Step 2**

Bring up the GigabitEthernet0/1 interface on the Branch router.

You need this connection so you do not get cut off when you are configuring the serial interface on the Headquarters router.
**Step 3**

From the Branch router, use Telnet to connect to the Headquarters router at 209.165.201.2.

```
Branch# telnet 209.165.201.2
Trying 209.165.201.2 ... Open
HQ#
```

**Step 4**

Copy or type the following configuration to the Headquarters router: You must be in global configuration mode when you paste in the following configuration.

```
frame-relay switching
!
interface Serial0/0/0
encapsulation frame-relay
frame-relay map ip 192.168.1.1 120
frame-relay interface-dlci 120
frame-relay intf-type dce
```

By doing this, you configured the Headquarters router to function as a Frame Relay switch. A Frame Relay switch would normally be a device within the service provider cloud. You do not need to know these commands but do need to understand how to set up a router to communicate with the Frame Relay switch.

**Step 5**

Exit the Telnet session.

```
HQ# exit
[Connection to 209.165.201.2 closed by foreign host]
Branch#
```

**Step 6**

On the Branch router, enable Frame Relay encapsulation on the Serial0/0/0 interface. You should see that the interface went up.

```
Nov 8 10:13:00.298: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

**Activity Verification**

You have completed this task when you attain these results:
**Step 1**

You have verified the status of the Serial0/0/0 interface. You should see that the interface is up and encapsulation is set to Frame Relay.

```
Branch# show interfaces Serial0/0/0
Serial0/0/0 is up, line protocol is up
   Hardware is WIC MBRD Serial
   Internet address is 192.168.1.1/24
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation FRAME-RELAY, loopback not set
   Keepalive set (10 sec)
   LMI enq sent 61, LMI stat recvd 62, LMI upd recvd 0, DTE LMI up
   LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
   LMI DLCI 1023 LMI type is CISCO frame relay DTE
```

**Step 2**

You have displayed LMI statistics. You should see that a number of LMI messages are being exchanged between the routers.

```
Branch# show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
   Invalid Unnumbered info 0     Invalid Prot Disc 0
   Invalid dummy Call Ref 0      Invalid Msg Type 0
   Invalid Status Message 0     Invalid Lock Shift 0
   Invalid Information ID 0      Invalid Report IE Len 0
   Invalid Report Request 0     Invalid Keep IE Len 0
   Num Status Enq. Sent 67      Num Status msgs Rcvd 68
   Num Update Status Rcvd 0     Num Status Timeouts 0
   Last Full Status Req 00:00:13 Last Full Status Rcvd 00:00:13
```

**Step 3**

You have displayed PVC statistics. You should see that one PVC is active on the Serial0/0/0 interface.

```
Branch# show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
   Active     Inactive      Deleted       Static
   Local          1            0            0            0
   Switched       0            0            0            0
   Unused         0            0            0            0
   DLCI = 120, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0
<output omitted>
```

What is the local DLCI number?
**Step 4**

You have displayed Frame Relay mappings. You should see dynamic mapping between the local DLCI and the IP address of the Headquarters router, which was learned through Inverse ARP.

```
Branch# show frame-relay map
Serial0/0/0 (up): ip 192.168.1.2 dlci 120 (0x78, 0x1C80), dynamic,
                   broadcast,
                   CISCO, status defined, active
```

Write down the mapping between the remote IP address and the local DLCI.

---

**Step 5**

From the Branch router, you have pinged the Headquarters router at 192.168.1.2. The ping should be successful.

```
Branch# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

---

**Task 2: Configure and Verify Frame Relay Subinterfaces**

In this task, you will configure a point-to-point subinterface on the Branch router. Because the router uses LMI and Inverse ARP to obtain DLCI information and the mapping between a DLCI and a remote IP address, you will also be required to map a DLCI to the configured subinterface.

**Activity Procedure**

Complete the following steps:

**Step 1**

Access the Branch router.

**Step 2**

On the Branch router, remove the IP address from the Serial0/0/0 interface.
**Step 3**

On the Branch router, create a point-to-point subinterface on the Serial0/0/0 interface. Use 120 as the subinterface identifier. Assign the previously removed IP address (192.168.1.1) to the subinterface.

**Step 4**

Verify the Frame Relay mappings and LMI statistics. No Frame Relay mappings should be seen. However, you should see that the counter of sent and received LMI messages is being incremented.

```
Branch# show frame-relay map
Branch# show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0     Invalid Prot Disc 0
  Invalid dummy Call Ref 0      Invalid Msg Type 0
  Invalid Status Message 0      Invalid Lock Shift 0
  Invalid Information ID 0      Invalid Report IE Len 0
  Invalid Report Request 0      Invalid Keep IE Len 0
  Num Status Enq. Sent 563      Num Status msgs Rcvd 564
  Num Update Status Rcvd 0      Num Status Timeouts 0
  Last Full Status Req 00:00:53 Last Full Status Rcvd 00:00:53
```

Why are no Frame Relay mappings being learned, although LMI is operational?

---

**Step 5**

On the Branch router, assign DLCI 120 to subinterface Serial0/0/0.120.

**Note**

Note that manual assignment of DLCIs to subinterfaces is not needed when you use static Frame Relay mappings.

**Activity Verification**

You have completed this task when you attain these results:
**Step 1**

You have verified the status of the Serial0/0/0.120 subinterface. You should see that the subinterface is up.

```
Branch# show interfaces Serial0/0/0.120
Serial0/0/0.120 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
<output omitted>
```

**Step 2**

You have displayed PVC statistics. You should see that one PVC is active on the Serial0/0/0.120 subinterface.

```
Branch# show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
  Active     Inactive      Deleted       Static
  Local          1            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
DLCI = 120, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.120
<output omitted>
```

Notice that the local DLCI number is 120.

**Step 3**

You have displayed Frame Relay mappings. You should see dynamic mapping between the local DLCI and the IP address of the Headquarters router.

```
Branch# show frame-relay map
Serial0/0/0.120 (up): point-to-point dlci, dlci 120(0x78,0x1C80), broadcast
  status defined, active
```

**Step 4**

From the Branch router, you have pinged the Headquarters router at 192.168.1.2. The ping should be successful.

```
Branch# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```
Task 3: Remove Frame Relay Configuration

In this task, you will remove the configured subinterface from the Branch router and remove Frame Relay encapsulation from both routers.

**Activity Procedure**

Complete the following steps:

**Step 1**
Access the Branch router.

**Step 2**
On the Branch router, remove the previously configured subinterface.

**Step 3**
On the Branch router, enable HDLC encapsulation on the Serial0/0/0 interface.

**Step 4**
On the Branch router, assign IP address 192.168.1.1 to the Serial0/0/0 interface.

**Step 5**
From the Branch router, use Telnet to connect to the Headquarters router at 209.165.201.2.

```
Branch# telnet 209.165.201.2
Trying 209.165.201.2 ... Open
HQ#
```

**Step 6**
On the Headquarters router, enable HDLC encapsulation on the Serial0/0/0 interface.

**Step 7**
Save the configuration on the Headquarters router.

Exit the Telnet session.

Save the configuration on the Branch router.

**Activity Verification**

You have completed this task when you attain these results:
**Step 1**

You have verified the status of the Serial0/0/0 subinterface on the Branch router. You should see that the interface is up and encapsulation is set to HDLC.

```
Branch# show interfaces Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: Link to HQ
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
<output omitted>
```

**Step 2**

From the Branch router, you have pinged the Headquarters router at 192.168.1.2. The ping should be successful.

```
Branch# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```
Lab 5-3: Establishing a GRE Tunnel

Activity Overview

Objectives

In this activity, you will implement a GRE tunnel. After completing this activity, you will be able to meet these objectives:

- Configure and verify a GRE tunnel
- Configure and verify OSPF over a GRE tunnel

Visual Objective

The figure illustrates what you will accomplish in this activity.
Visual Objective for Lab 5-3: Establishing a GRE Tunnel

Required Resources
No additional resources are required for this lab.

Command List
The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration or verification Cisco IOS command assistance during the lab activity.
## Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>ip address ip_address subnet_mask</td>
<td>Sets an IP address on the interface.</td>
</tr>
<tr>
<td>network network wildcard_mask area area_id</td>
<td>Enables the OSPF routing protocol for a specified area on the interfaces that match the specified network.</td>
</tr>
<tr>
<td>[no] passive-interface interface</td>
<td>Disables sending routing updates on the interface. To re-enable the sending of routing updates, use the no form of this command.</td>
</tr>
<tr>
<td>ping destination_address</td>
<td>Pings the specified IP address.</td>
</tr>
<tr>
<td>router ospf process_id</td>
<td>Enables the OSPF routing process.</td>
</tr>
<tr>
<td>show interface interface</td>
<td>Displays interface setup and statistics.</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays a brief interface status.</td>
</tr>
<tr>
<td>show ip ospf neighbors</td>
<td>Shows OSPF neighbors.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the routing table.</td>
</tr>
<tr>
<td>[no] shutdown</td>
<td>Enables or disables the interface.</td>
</tr>
<tr>
<td>tunnel source ip_address</td>
<td>Specifies the tunnel source IP address in interface tunnel configuration mode.</td>
</tr>
<tr>
<td>tunnel destination ip_address</td>
<td>Specifies the tunnel destination IP address in interface tunnel configuration mode.</td>
</tr>
</tbody>
</table>

## Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access the equipment in this lab.
### Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
</tbody>
</table>
### Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>
IP Routing

The Headquarters router has interfaces Serial0/0/0 and Loopback0 in OSPF Area 0. The Branch router has only the interface Serial0/0/0 enabled in Area 0. All of the interfaces on the Branch router toward the LAN are enabled for OSPF Area 1. The Headquarters router ID is 1.1.1.1.

---

Task 1: Configure and Verify a GRE Tunnel

In this task, you will configure a GRE tunnel between the Branch and Headquarters routers over an Internet link. The Headquarters router is preconfigured for a GRE tunnel, so you will configure only the Branch router.

Activity Procedure

Complete the following steps:

**Step 1**

On the Branch router, create a GRE tunnel with these parameters:

- **Tunnel source:** Interface GigabitEthernet 0/1 on the Branch router
- **Tunnel destination:** Interface GigabitEthernet 0/1 on the Headquarters router
- **IP address:** 192.168.2.1/24

*Note*  
The GRE tunnel mode is the default tunnel interface mode of Cisco IOS Software.
Step 2

A GRE tunnel was preconfigured by your colleague on the Headquarters router, but he left the tunnel interface shut down.

Use Telnet to connect to the Headquarters router and enable interface Tunnel 0.

Activity Verification

You have completed this task when you attain this result:

Step 1

On the Branch router, you have verified that the GRE tunnel is up and that the tunnel mode is set to GRE.

```
Branch# show interface tunnel 0
Tunnel0 is up, line protocol is up
   Hardware is Tunnel
   Internet address is 192.168.2.1/24
   MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation TUNNEL, loopback not set
   Keepalive not set
   Tunnel source 209.165.201.1, destination 209.165.201.2
   Tunnel protocol/transport GRE/IP
```

Task 2: Configure and Verify OSPF over a GRE Tunnel

In this task, you will configure OSPF over a GRE tunnel. The WAN link between the Branch and Headquarters routers is configured, so you will add a GRE tunnel to the OSPF process. OSPF over a GRE tunnel is preconfigured on the Headquarters router, so you will configure it only on the Branch router.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, configure OSPF to exchange routes over the GRE tunnel. The Headquarters router already has a network statement including the Tunnel 0 interface into the Area 0 OSPF process.

Do not forget to add the Tunnel 0 interface as an OSPF nonpassive interface.

Note

OSPF over GRE is preconfigured on the Headquarters router.
**Step 2**

Verify that an OSPF adjacency has been established over the GRE tunnel.

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>0</td>
<td>FULL/</td>
<td>00:00:32</td>
<td>192.168.2.2</td>
<td>Tunnel0</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>0</td>
<td>FULL/</td>
<td>00:00:31</td>
<td>192.168.1.2</td>
<td>Serial0/0/0</td>
</tr>
</tbody>
</table>

You should see the Headquarters router as a neighbor over two interfaces. One of them should be the GRE tunnel interface. The neighbors should be in the full state.

**Step 3**

Verify the current routing table on the Branch router.

```
Branch# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       *i - IS-IS inter area, * - candidate default, U - per-user static route
       O - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 209.165.201.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.201.2
       10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
       C  10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
       L  10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
       C  10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
       L  10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
       C  10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
       L  10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
       C  10.100.100.32/32 is directly connected, Loopback10
       172.16.0.0/24 is subnetted, 1 subnets
       O  172.16.1.0 [110/65] via 192.168.1.2, 00:07:42, Serial0/0/0
          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
          C  192.168.1.0/24 is directly connected, Serial0/0/0
          L  192.168.1.1/32 is directly connected, Serial0/0/0
          192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
          C  192.168.2.0/24 is directly connected, Tunnel10
          L  192.168.2.1/32 is directly connected, Tunnel10
       209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
       C  209.165.201.0/27 is directly connected, GigabitEthernet0/1
       L  209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

You should see that OSPF chooses the path over the serial link as the best path toward the server.

**Step 4**

On the Branch router, disable interface Serial 0/0/0.
By shutting down the interface, you are simulating the failure of this interface.

**Step 5**

Verify the current routing table on the Branch router.

```
Branch# show ip route
 Codes:  L - local,  C - connected,  S - static,  R - RIP,  M - mobile,  B - BGP
       D - EIGRP,  EX - EIGRP external,  O - OSPF,  IA - OSPF inter area
       N1 - OSPF NSSA external type 1,  N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,  E2 - OSPF external type 2
       i - IS-IS,  su - IS-IS summary,  L1 - IS-IS level-1,  L2 - IS-IS level-2
       ia - IS-IS inter area,  * - candidate default,  U - per-user static route
       o - ODR,  P - periodic downloaded static route,  H - NHRP,  l - LISP
       + - replicated route,  % - next hop override
Gateway of last resort is 209.165.201.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.201.2
10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
 C    10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
 L    10.1.1.0/32 is directly connected, GigabitEthernet0/0.1
 C    10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
 L    10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
 C    10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
 L    10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
 C    10.100.100.100/32 is directly connected, Loopback10
172.16.0.0/24 is subnetted, 1 subnets
 O   172.16.1.0 [110/1001] via 192.168.2.2, 00:00:06, Tunnel0
 O   192.168.1.0/24 [110/1064] via 192.168.2.2, 00:00:06, Tunnel10
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
 C   192.168.2.0/24 is directly connected, Tunnel0
 L   192.168.2.1/32 is directly connected, Tunnel0
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
 C   209.165.201.0/27 is directly connected, GigabitEthernet0/1
 L   209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

You should see that OSPF chooses the path over the GRE tunnel as the best path toward the server.

**Step 6**

Ping the server from the Branch router.

```
Branch# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

You should see that this attempt is successful.
**Step 7**

Verify that traffic enters the GRE tunnel.

```
Branch# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
    Hardware is Tunnel
    Internet address is 192.168.2.1/24
    MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation TUNNEL, loopback not set
    Keepalive not set
    Tunnel source 209.165.201.1, destination 209.165.201.2
    Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
    Tunnel TTL 255, Fast tunneling enabled
    Tunnel transport MTU 1476 bytes
    Tunnel transmit bandwidth 8000 (kbps)
    Tunnel receive bandwidth 8000 (kbps)
    Last input 00:00:05, output 00:00:01, output hang never
    Last clearing of "show interface" counters 00:33:03
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/0 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    217 packets input, 22588 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    117 packets output, 12380 bytes, 0 underruns
```

You should see that the input and output counters increase for the GRE tunnel interface.

**Step 8**

On the Branch router, enable the Serial 0/0/0 interface.

**Step 9**

Use Telnet to connect to the Headquarters router at 192.168.1.2.

Save the configuration on the Headquarters router.

Exit the Telnet session.

Save the configuration on the Branch router.
Activity Verification
Verification is part of the activity procedure.
Lab 6-1: SNMP and Syslog
Basic Configuration

Activity Overview

Objectives

In this activity, you will configure the Branch router as an SNMP and syslog client. After completing this activity, you will be able to meet these objectives:

- Configure the SNMP client
- Configure the syslog client

Visual Objective

The figure illustrates what you will accomplish in this activity.
Visual Objective for Lab 6-1: SNMP and Syslog Basic Configuration

Required Resources

PC1 has the HillSoft MIB browser and Kiwi Syslog Daemon installed. You will need both of them to complete this lab.
Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] shutdown</td>
<td>Enables or disables the interface</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enters interface configuration mode</td>
</tr>
<tr>
<td>logging ip-address</td>
<td>Identifies a syslog server host to receive logging messages</td>
</tr>
<tr>
<td>logging trap severity</td>
<td>Limits the syslog messages that are sent to the syslog server based on severity</td>
</tr>
<tr>
<td>snmp-server community string [ro</td>
<td>rw]</td>
</tr>
<tr>
<td>snmp-server contact contact_name</td>
<td>Sets the system contact string</td>
</tr>
<tr>
<td>snmp-server location location</td>
<td>Sets the system location string</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of syslog and the contents of the standard syslog buffer</td>
</tr>
</tbody>
</table>

Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

There are no console or enable passwords that are set for the routers and switches in the initial lab setup. The table shows the usernames and passwords that are used to access PC1 and PC2.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address or Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Branch</td>
<td>Tunnel0</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Tunnel0</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>
Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates trunk and VLAN setup.
IP Routing

The Headquarters router has interfaces Serial 0/0/0, Tunnel 0, and Loopback0 (which simulates a remote server in your pod) in OSPF Area 0. The Branch router has interfaces Serial 0/0/0 and Tunnel 0 that are enabled in OSPF Area 0. All of the interfaces toward the LAN are enabled for OSPF Area 1.

---

Task 1: Configure Router for SNMP Access

In this task, you will configure a community access string to permit SNMP access to the router.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, define the community access string "Cisco" with read-write privileges.

**Step 2**

On the Branch router, set the SNMP system contact string to "Joe Summer" and SNMP system location string to "San Jose."
Step 3
On PC1, run HillSoft MIB Browser. Click Tools >SNMP Entities and fill in the required fields to be able to retrieve SNMP data from the Branch router.

![SNMP Entities](image)

Step 4
In the MIB tree view, navigate to iso->org->dod->internet->mgmt->mib-2->system.

Activity Verification
You have completed this task when you attain this result:
**Step 1**

Choose sysContact SNMP OID, choose GET as the SNMP method, and click the green button.

You should see that value for this OID is "Joe Summer."

**Step 2**

Repeat the same procedure for other OIDs (sysUpTime, sysName, sysLocation, and so on).

**Task 2: Configure Router for Syslog**

In this task, you will configure the Branch router to send syslog messages to the syslog server, which is installed on PC1.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, configure PC1 as the syslog server host that receives syslog messages.

**Step 2**

On the Branch router, specify that syslog messages with all severity levels are sent to the syslog server.
**Step 3**

Run Kiwi Syslog Daemon, which is installed on PC1.

**Step 4**

On the Branch router, disable the Serial0/0/0 interface.

---

**Note**

By doing this, you will initiate the generation of syslog messages.

---

**Step 5**

After observing syslog messages on the Kiwi Syslog server, enable the Serial0/0/0 interface on the Branch router.

**Step 6**

Save the changes that you made on the Branch router.

```
Branch# copy running-config startup-config
```

**Activity Verification**

You have completed this task when you attain these results:

**Step 1**

Observe the syslog messages that are received on the Kiwi Syslog server.

You should see the syslog message of the Serial0/0/0 interface going down and the message of OSPF state going from FULL to DOWN.
Step 2

On the Branch router, display the state of syslog and the contents of the standard system logging buffer.

```
Branch# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
  Console logging: level debugging, 27 messages logged, xml disabled, filtering disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
  Buffer logging: level debugging, 50 messages logged, xml disabled, filtering disabled
  Exception Logging: size (4096 bytes)
  Count and timestamp logging messages: disabled
  Persistent logging: disabled
  Trap logging: level debugging, 53 message lines logged
    Logging to 10.1.10.100 (udp port 514, audit disabled, link up),
    23 message lines logged, 0 message lines rate-limited, 0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
  Logging Source-Interface: VRF Name:
```

You should see that the syslog logging level is debugging and the syslog messages are sent to the server with IP address 10.1.10.100.
Lab 6-2: Analyzing NetFlow Data

Activity Overview

Objectives

In this activity, you will look at outputs from a NetFlow analyzer and answer questions about them. After completing this activity, you will be able to meet this objective:

- Analyze data that is captured by the NetFlow Collector

Visual Objective

There is no visual objective for this lab.

Required Resources

No additional resources are required for this lab.

Command List

There are no commands that are needed for completing this lab.

Job Aids

There are no job aids that are needed for completing this lab.

Task 1: Analyze NetFlow Data

In this task, you analyze and interpret NetFlow data that is obtained in the NetFlow analyzer.

Activity Procedure

Complete the following steps:
Step 1

Which application is responsible for generating the most traffic in your network according to the following pie chart?

The pie chart provides a view of the applications that are responsible for the most traffic passing through the viewed node or interface over the selected period of time. The table along with the pie chart provides the following information:

- The application name with its assigned port number
- The amount of data, in both bytes and packets, flowing to the selected application through the viewed node
• The percentage of all traffic through the viewed node that can be attributed to use of the listed application

Answer: _________________________________________________
Step 2

Which is the most bandwidth-consuming conversation that is conducted over your monitored network?

The pie chart provides a list of the most bandwidth-consuming conversations that are conducted over your monitored network. Conversations are listed with the amount of data that is transferred in the conversation, in both bytes and packets. The table along with the pie chart provides the following information:

- The application name
- The amount of data, in both bytes and packets, flowing in the selected conversation through the viewed node or interface
- The percentage of all traffic through the viewed node or interface

Answer: _________________________________________________
Step 3

Which receiver consumes the most bandwidth over your monitored network?

The pie chart provides a list of the receivers consuming the bandwidth over your monitored network. Receivers are listed with the amount of data that is transferred, in both bytes and packets, and the name or IP address of the receiving endpoint. The table along with the pie chart provides the following information:

- The application name
- The amount of data, in both bytes and packets, that is routed through the viewed node that is received by the listed endpoint over the specified period of time
- The percentage of all traffic that is routed through the viewed node that is received by the listed endpoint over the specified period of time

Answer: _________________________________________________

<table>
<thead>
<tr>
<th>HOSTNAME</th>
<th>INGRESSBYTES</th>
<th>EGRESSBYTES</th>
<th>INGRESSPACKETS</th>
<th>EGRESSPACKETS</th>
<th>PERCENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>hmsrussdev</td>
<td>3.4 Mbytes</td>
<td>14.9 Mbytes</td>
<td>7.51 k</td>
<td>32.81 k</td>
<td>25.73%</td>
</tr>
<tr>
<td>hmcoby</td>
<td>2.6 Mbytes</td>
<td>12.7 Mbytes</td>
<td>5.15 k</td>
<td>23.5 k</td>
<td>21.48%</td>
</tr>
<tr>
<td>KJOHNSTONXIP</td>
<td>1.8 Mbytes</td>
<td>11.0 Mbytes</td>
<td>4.05 k</td>
<td>20.33 k</td>
<td>18.05%</td>
</tr>
<tr>
<td>TMEYERLT</td>
<td>936.8 kbytes</td>
<td>6.3 Mbytes</td>
<td>2.03 k</td>
<td>11.4 k</td>
<td>10.26%</td>
</tr>
<tr>
<td>PMCCARTHY</td>
<td>756.9 kbytes</td>
<td>4.6 Mbytes</td>
<td>1.49 k</td>
<td>8.34 k</td>
<td>7.54%</td>
</tr>
<tr>
<td>MJENKINSDer</td>
<td>4.3 Mbytes</td>
<td>0 bytes</td>
<td>9.11 k</td>
<td>0</td>
<td>6.03%</td>
</tr>
<tr>
<td>hhoevelktp</td>
<td>712.9 kbytes</td>
<td>1.9 Mbytes</td>
<td>2.17 k</td>
<td>4.71 k</td>
<td>3.68%</td>
</tr>
<tr>
<td>ABARNESWks</td>
<td>1.9 Mbytes</td>
<td>0 bytes</td>
<td>4.24 k</td>
<td>0</td>
<td>2.72%</td>
</tr>
<tr>
<td>EVOOD</td>
<td>1.8 Mbytes</td>
<td>0 bytes</td>
<td>3.81 k</td>
<td>0</td>
<td>2.52%</td>
</tr>
<tr>
<td>mbishopwks</td>
<td>653.0 kbytes</td>
<td>767.1 kbytes</td>
<td>1.94 k</td>
<td>2.47 k</td>
<td>2%</td>
</tr>
</tbody>
</table>
Step 4

Which transmitter consumes the most bandwidth over your monitored network?

The pie chart provides a list of the transmitters consuming the bandwidth over your monitored network. Transmitters are listed with the amount of data that is transferred, in both bytes and packets. The table along with the pie chart provides the following information:

- The application name
- The amount of data, in both bytes and packets, that is routed through the viewed node that is received by the listed endpoint over the specified period of time
- The percentage of all traffic that is routed through the viewed node that is received by the listed endpoint over the specified period of time

Answer: ____________________________
Step 5
Which IP address group is responsible for the most traffic on your network?

The pie chart provides a view of the IP address groups that are responsible for the most traffic on your network. With NetFlow, you can create IP groups that are based on IP addresses and/or a combination of port and protocol. IP grouping is useful in tracking departmental bandwidth utilization, calculating bandwidth costs, and ensuring appropriate usage of network bandwidth. The table along with the pie chart provides the following information:

- The IP address group range or the name of this IP range
- The amount of data, in both bytes and packets, through the viewed node that is traceable to the listed IP address group over the selected period of time
- The percentage of all traffic over the viewed node that is traceable to the listed IP address group

Answer: ____________________________

Activity Verification
No additional verification is needed in this task.
Lab 6-3: Managing Cisco Devices and Licensing

Activity Overview

Objectives

In this lab, you will do a password recovery, manage Cisco IOS image and configuration files, and verify licensing. After completing this activity, you will be able to meet these objectives:

- Perform a password recovery on a router
- Back up a Cisco IOS image
- Manage a configuration file
- Verify licensing

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources

PC1 must have Cisco TFTP server software.

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Activates configuration mode from the terminal.</td>
</tr>
<tr>
<td><strong>config-register</strong> value</td>
<td>Sets the configuration register in privileged mode.</td>
</tr>
<tr>
<td><strong>confr</strong> value</td>
<td>Sets the configuration register in the ROM monitor mode.</td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td>Saves the running configuration into the startup configuration.</td>
</tr>
<tr>
<td><strong>copy running-config tftp:</strong></td>
<td>Copies running configuration to the TFTP server.</td>
</tr>
<tr>
<td><strong>copy startup-config running-config</strong></td>
<td>Brings and merges startup configuration into running configuration.</td>
</tr>
<tr>
<td><strong>copy tftp: running-config</strong></td>
<td>Copies the configuration on the TFTP server to the running configuration.</td>
</tr>
<tr>
<td><strong>disable</strong></td>
<td>Exits privilege EXEC mode.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Activates privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.</td>
</tr>
<tr>
<td><strong>enable secret</strong> password</td>
<td>Configures the enable password in MD5-encrypted form.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits the router console.</td>
</tr>
<tr>
<td><strong>hostname hostname</strong></td>
<td>Sets the system name, which forms part of the prompt.</td>
</tr>
<tr>
<td><strong>ping ip_address</strong></td>
<td>Pings a destination IP address.</td>
</tr>
<tr>
<td><strong>reload</strong></td>
<td>Restarts the switch and reloads the Cisco IOS operating system and configuration.</td>
</tr>
<tr>
<td><strong>reset</strong></td>
<td>Resets the router from the ROM monitor mode.</td>
</tr>
<tr>
<td><strong>show ip interfaces brief</strong></td>
<td>Displays a brief summary of the IP information and status of an interface.</td>
</tr>
<tr>
<td><strong>show license</strong></td>
<td>Displays information about the Cisco IOS Software license.</td>
</tr>
<tr>
<td><strong>show version</strong></td>
<td>Displays information about the currently loaded software along with hardware and device information.</td>
</tr>
</tbody>
</table>

### Job Aids

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>Headquarter s</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M4</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>
There are no console or enable passwords that are set for the routers and switches in the initial lab setup. The table shows the usernames and passwords that are used to access PC1 and PC2.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Topology and IP Addressing**

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that are used in this lab setup.

The table shows the interface identification and IP addresses that are used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Branch</td>
<td>Tunnel0</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
</tbody>
</table>
### Device Configuration

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters</td>
<td>Tunnel0</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>

### Trunk and VLAN Setup

Three VLANs are configured on the switches. VLAN 1 is used for switch management, VLAN 10 is used to connect PC1, and VLAN 20 is used to connect PC2. The two links between SW1 and SW2 are bonded into an EtherChannel, and a trunk is configured on it. The SW1 switch and the Branch router are connected by a trunk link. The figure illustrates the trunk and VLAN setup.
**IP Routing**

The Headquarters router has interfaces Serial 0/0/0, Tunnel 0, and Loopback0 (which simulates a remote server in your pod) in OSPF Area 0. The Branch router has interfaces Serial 0/0/0 and Tunnel 0 that are enabled in OSPF Area 0. All of the interfaces toward the LAN are enabled for OSPF Area 1.

---

**Task 1: Lab Setup**

In this Lab Setup task, you will load a configuration to the Branch router to create a trouble ticket. You will resolve these tickets in the next tasks.

**Activity Procedure**

Complete the following steps:

**Step 1**

Access the Branch router.

**Step 2**

Overwrite the running configuration with the file that is located in the router flash memory called INIT_Managing_and_Licensing_Branch.cfg.

```bash
Branch# configure replace flash: INIT_Managing_and_Licensing_Branch.cfg
```

**Activity Verification**

No additional verification is needed in this task.
Task 2: Router Password Recovery
You are unable to access the Branch router because the enable password is misconfigured. In this task, you will do a password recovery on the Branch router.

Activity Procedure
Complete the following steps:

Step 1
Connect with the console to the Branch router and try to access privileged mode.

Branch con0 is now available
Press RETURN to get started.
Branch>
Branch> enable
Password: cisco
Password:

You will see the user mode prompt and will be unable to access privileged mode because you do not have the correct enable password.

Step 2
On the Branch router, do a password recovery to get to the privileged mode.

Step 3
After completing the password recovery process, all of the interfaces on the router will be in the administratively shutdown state.

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded-Service-Engine0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0.1</td>
<td>10.1.1.1</td>
<td>YES TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0.10</td>
<td>10.1.10.1</td>
<td>YES TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0.20</td>
<td>10.1.20.1</td>
<td>YES TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1</td>
<td>YES TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>192.168.1.1</td>
<td>YES TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Loopback10</td>
<td>10.100.100.100</td>
<td>YES TFTP</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel0</td>
<td>192.168.2.1</td>
<td>YES TFTP</td>
<td>up</td>
<td>down</td>
</tr>
</tbody>
</table>

Bring up interfaces Serial0/0/0, GigabitEthernet0/0, and GigabitEthernet0/1.
**Activity Verification**

**Step 1**

On the Branch router, exit from privileged mode and try to get back with the password "cisco":

```
Branch# disable
Branch> enable
Password: cisco
Branch#
```

You should be able to access privileged mode of the Branch router.

**Step 2**

On the Branch router, verify the value of the configuration register:

```
Branch# show version | include register
Configuration register is 0x2142 (will be 0x2102 at next reload)
```

The configuration register will be 0x2102 at the next reload.

**Step 3**

Verify that the status of interfaces Serial0/0/0, GigabitEthernet0/0.1, GigabitEthernet0/0.10, and GigabitEthernet0/0.20 is up/up.

```
Branch# sh ip interfaces brief
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded-Service-Engine0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
</tr>
<tr>
<td>GigabitEthernet0/0.1</td>
<td>10.1.1.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>GigabitEthernet0/0.10</td>
<td>10.1.10.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>GigabitEthernet0/0.20</td>
<td>10.1.20.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>192.168.1.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Loopback10</td>
<td>10.100.100.100</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel10</td>
<td>192.168.2.1</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
</tbody>
</table>
```

**Task 3: Backing up an IOS Image**

In this task, you will copy a Cisco IOS image from the Branch router to the TFTP server that is installed on PC1.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, confirm the presence of the Cisco IOS image on the Flash.
**Step 2**

Verify connectivity from the Branch router to PC1. You should have connectivity between the two devices.

```
Branch# ping 10.1.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

**Step 3**

On the PC1 desktop, create new folder named TFTP.

Run Cisco TFTP server software on PC1. Click the **Options > Server Root** directory and set the root directory of the TFTP server to the folder that you just created.

![TFTP Server](image)

**Step 4**

On the Branch router, enter the sequence of commands that will back up the Cisco IOS image to the TFTP server.

**Activity Verification**

You have completed this task when you attain this result:
Step 1

Verify that the Cisco IOS image was copied to C:\TFTP on PC1.

You should see the image file in TFTP folder.

Task 4: Manage a Configuration File

In this task, you will copy a configuration file from the Branch router to the TFTP server on PC1. You will open the configuration file and change it on PC1 and apply the configuration back to the Branch router.

Activity Procedure

Complete the following steps:

Step 1

Copy the running configuration of the Branch router to the TFTP server on PC1.
**Step 2**

On PC1, open the transferred file C:\TFTP\branch-config using WordPad and change the hostname to Branch-changedconfiguration. Close and save the file.

![Image of WordPad with hostname change](image)

**Step 3**

Copy the changed configuration from the TFTP server on PC1 to the running configuration of the Branch router.

When copying from the TFTP server into the running configuration of the Branch router, will the new configuration overwrite the old one?

**Step 4**

Verify that the hostname of the router is changed.

```
Branch-changedconfiguration#
```

**Step 5**

Change the hostname of the Branch router back to Branch.
Step 6
Save the changes that you made on the Branch router.

Activity Verification
Verification is part of the Activity Procedure.

Task 5: Verify Licensing
In this task, you will verify which technology package licenses are installed on the Branch router.

Activity Procedure
Complete the following steps:

Step 1
Verify which technology package licenses or feature licenses are installed on the Branch router.
Which technology package license is installed and which license type is this?

Activity Verification
Verification is part of the Activity Procedure.
Lab S-2: ICND2 Superlab

Activity Overview

Objectives

In this lab, you will reinforce your knowledge that you acquired through this course. You will be presented with a mix of configuration and troubleshooting tasks:

- Secure a router and configure inter-VLAN routing
- Configure basic settings, VLANs, and trunks on a switch
- Configure EtherChannel
- Configure port security
- Configure SSH on a router
- Configure a DHCP server
- Configure stateless autoconfiguration
- Configure PPP encapsulation
- Configure dynamic routing protocol
- Troubleshoot an IP access control list

Visual Objective

The figure illustrates what you will accomplish in this activity.
Required Resources
No additional resources are required for this lab.

Command List
The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list acl_id permit network</td>
<td>Creates a numbered access list entry.</td>
</tr>
<tr>
<td>banner login # text #</td>
<td>Sets the login banner.</td>
</tr>
<tr>
<td>channel-group group_id mode mode</td>
<td>Assigns and configures an EtherChannel interface to an EtherChannel group. Mode active enables LACP unconditionally. Mode auto places a port into a passive negotiating state in which the port responds to PAgP packets that it receives but does not initiate PAgP packet negotiation.</td>
</tr>
<tr>
<td>config-register value</td>
<td>Sets the configuration register in privileged mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Activates configuration mode from the terminal.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves running configuration into startup configuration.</td>
</tr>
<tr>
<td>copy startup-config running-config</td>
<td>Brings and merges startup configuration into running configuration.</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Generates the RSA crypto key pair.</td>
</tr>
<tr>
<td>default-router default_ip</td>
<td>Assigns the default gateway to the DHCP pool.</td>
</tr>
<tr>
<td>delete name</td>
<td>Deletes a file from Flash memory.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>deny ip</td>
<td>tcp</td>
</tr>
<tr>
<td>disable</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Activates privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.</td>
</tr>
<tr>
<td>enable secret password</td>
<td>Configures the enable password in MD5-encrypted form.</td>
</tr>
<tr>
<td>encapsulation dot1Q vlan</td>
<td>Sets the encapsulation type and VLAN on a subinterface on a router.</td>
</tr>
<tr>
<td>encapsulation ppp</td>
<td>Sets PPP encapsulation on a serial interface on a router.</td>
</tr>
<tr>
<td>erase startup-configuration</td>
<td>Erases the startup configuration that is stored in nonvolatile memory.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the router console.</td>
</tr>
<tr>
<td>hostname hostname</td>
<td>Sets the system name, which forms part of the prompt.</td>
</tr>
<tr>
<td>interface [range] interface</td>
<td>Enters interface configuration mode. With the range keyword, enters the interface range.</td>
</tr>
<tr>
<td>interface [range] interface.subinterface</td>
<td>Enters subinterface configuration mode. With the range keyword, enters the subinterface range.</td>
</tr>
<tr>
<td>ip access-group acl_name in</td>
<td>out</td>
</tr>
<tr>
<td>ip access-list extended acl_name</td>
<td>Creates an extended, named access list.</td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td>Sets the IP address and mask on an interface.</td>
</tr>
<tr>
<td>ip dhcp excluded-address first_ip last_ip</td>
<td>Defines which IP addresses are excluded from DHCP allocation.</td>
</tr>
<tr>
<td>ip dhcp pool pool_name</td>
<td>Creates and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td>ip domain-name domain</td>
<td>Sets a domain name.</td>
</tr>
<tr>
<td>ip nat inside</td>
<td>Configures an interface as NAT inside.</td>
</tr>
<tr>
<td>ip nat inside source list acl_id interface overload</td>
<td>Configures dynamic NAT with PAT.</td>
</tr>
<tr>
<td>ip nat outside</td>
<td>Configures an interface as NAT outside.</td>
</tr>
<tr>
<td>ip route network mask next_hop_ip_address</td>
<td>Configures a static route (including a default route).</td>
</tr>
<tr>
<td>ip ssh version 2</td>
<td>Enables SSH version 2.</td>
</tr>
<tr>
<td>ipv6 address ipv6-address/prefix_length</td>
<td>Sets the IPv6 address and prefix length on an interface.</td>
</tr>
<tr>
<td>ipv6 ospf process_id area area_id</td>
<td>Enables an interface for OSPFv3 in an area.</td>
</tr>
<tr>
<td>ipv6 router ospf process_id</td>
<td>Creates the OSPFv3 process.</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enables IPv6 routing on a router.</td>
</tr>
<tr>
<td>lease days hours minutes</td>
<td>Assigns a lease value to the DHCP pool.</td>
</tr>
<tr>
<td>line console 0</td>
<td>Enters line console configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>line vty start_line end_line</td>
<td>Enters virtual lines configuration mode.</td>
</tr>
<tr>
<td>logging synchronous</td>
<td>Causes all router status messages to be displayed on a new line.</td>
</tr>
<tr>
<td>login</td>
<td>Enables verification of a password on a line.</td>
</tr>
<tr>
<td>login local</td>
<td>Enables verification of a username and password on a line.</td>
</tr>
<tr>
<td>network network subnet_mask</td>
<td>Assigns a network to the DHCP pool.</td>
</tr>
<tr>
<td>network network wildcard_mask area area_id</td>
<td>Configures a router to advertise a network through OSPF.</td>
</tr>
<tr>
<td>password password</td>
<td>Sets a password on an line.</td>
</tr>
<tr>
<td>permit ip</td>
<td>tcp</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>Pings a destination IP address.</td>
</tr>
<tr>
<td>reload</td>
<td>Restarts the switch and reloads the Cisco IOS operating system and configuration.</td>
</tr>
<tr>
<td>router ospf process_id</td>
<td>Creates the OSPF process.</td>
</tr>
<tr>
<td>show etherchannel summary</td>
<td>Displays EtherChannel port members and negotiation protocol.</td>
</tr>
<tr>
<td>show interfaces interface</td>
<td>Displays the status of an interface.</td>
</tr>
<tr>
<td>show interfaces interface switchport</td>
<td>Displays the switchport status of a port.</td>
</tr>
<tr>
<td>show interfaces interface trunk</td>
<td>Displays the trunking status of a port.</td>
</tr>
<tr>
<td>show ip access-lists</td>
<td>Displays configured access lists and hit counts.</td>
</tr>
<tr>
<td>show ip dhcp binding</td>
<td>Displays DHCP bindings on the router acting as a DHCP server.</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays the brief status of interfaces and their IP addresses.</td>
</tr>
<tr>
<td>show ip nat translations</td>
<td>Displays the NAT translation table.</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Displays OSPF settings on a router.</td>
</tr>
<tr>
<td>show ip ospf neighbors</td>
<td>Displays OSPF neighbors.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the routing table.</td>
</tr>
<tr>
<td>show ipv6 interface interface</td>
<td>Displays IPv6 settings and status on an interface.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Displays the IPv6 neighbor discovery table.</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>Displays OSPFv3 settings on a router.</td>
</tr>
<tr>
<td>show ipv6 ospf neighbors</td>
<td>Displays OSPFv3 neighbors.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays the IPv6 routing table.</td>
</tr>
<tr>
<td>show mac address-table</td>
<td>Displays the MAC address table on a switch.</td>
</tr>
<tr>
<td>show port-security interface interface</td>
<td>Displays port security information on an interface.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the current configuration on the Cisco IOS router or switch.</td>
</tr>
<tr>
<td>show spanning-tree vlan vlan</td>
<td>Displays VLAN spanning-tree status.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>show users</td>
<td>Displays users that are currently logged into a router.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays hardware, software setup, and configure register on the router.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down an interface. Use the no version of the command to enable the interface.</td>
</tr>
<tr>
<td>switchport access vlan vlan</td>
<td>Specifies an access VLAN on a switchport.</td>
</tr>
<tr>
<td>switchport mode access</td>
<td>trunk</td>
</tr>
<tr>
<td>switchport port-security</td>
<td>Enables port security on a switchport.</td>
</tr>
<tr>
<td>switchport port-security mac-address mac_address</td>
<td>Manually defines MAC addresses that are allowed on a switchport when port security is enabled.</td>
</tr>
<tr>
<td>switchport port-security maximum number</td>
<td>Specifies the maximum number of MAC address that can be seen on a port when port security is enabled.</td>
</tr>
<tr>
<td>switchport port-security violation protect</td>
<td>Configures the port security violation to protect.</td>
</tr>
<tr>
<td>switchport trunk allowed vlan vlans</td>
<td>Specifies allowed VLANs on a trunk link.</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>Uses Telnet to connect to a destination IP address.</td>
</tr>
<tr>
<td>transport input ssh telnet</td>
<td>Allows Telnet and SSH on virtual lines.</td>
</tr>
<tr>
<td>username username password password</td>
<td>Creates a user account in the local user database.</td>
</tr>
<tr>
<td>vlan vlan_id</td>
<td>Creates a VLAN on a switch.</td>
</tr>
</tbody>
</table>

**Job Aids**

These job aids are available to help you complete the lab activity.

The table shows the hardware that is used in the lab and the operating system that is running on the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>Headquarter s</td>
<td>Cisco 2901 Integrated Services Router</td>
<td>c2900-universalk9-mz.SPA.152-4.M1</td>
</tr>
<tr>
<td>SW1</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanbasek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>SW2</td>
<td>Catalyst 2960 Series Switch</td>
<td>c2960-lanlitek9-mz.150-1.SE3</td>
</tr>
<tr>
<td>PC1</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>PC2</td>
<td>Any PC</td>
<td>Microsoft Windows 7</td>
</tr>
</tbody>
</table>

The table shows the usernames and passwords that are used to access PC1 and PC2.

<table>
<thead>
<tr>
<th>Device</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>PC2</td>
<td>Administrator</td>
<td>admin</td>
</tr>
</tbody>
</table>
Topology and IP Addressing

Devices are connected with Ethernet and serial connections. The figure illustrates the interface identification and IP addresses that will be used in this lab.

The table shows the interface identification and IP addresses that will be used in this lab setup.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>10.1.20.1/24</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.1/27</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Branch</td>
<td>Loopback10</td>
<td>10.100.100.100/32</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>209.165.201.2/27</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>172.16.1.100/24</td>
</tr>
<tr>
<td>SW1</td>
<td>VLAN 1</td>
<td>10.1.1.11/24</td>
</tr>
<tr>
<td>SW2</td>
<td>VLAN 1</td>
<td>10.1.1.12/24</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.10.100/24</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>10.1.20.100/24</td>
</tr>
</tbody>
</table>
IPv6 Addressing

The figure illustrates IPv6 addresses that will be used in this lab.

The table shows the interface identification and IPv6 addresses that will be used in this lab.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.1 (VLAN 1)</td>
<td>2001:db8:0a01:100::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.10 (VLAN 10)</td>
<td>2001:db8:0a01:a00::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/0.20 (VLAN 20)</td>
<td>2001:db8:0a01:1400::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8:d1a5:c900::1/64</td>
</tr>
<tr>
<td>Branch</td>
<td>Serial0/0/0</td>
<td>2001:db8:c0a8:100::1/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>GigabitEthernet0/1</td>
<td>2001:db8:d1a5:c900::2/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Serial0/0/0</td>
<td>2001:db8:c0a8:100::2/64</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Loopback0</td>
<td>2001:db8:ac10:100::64/64</td>
</tr>
<tr>
<td>PC1</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically</td>
</tr>
<tr>
<td>PC2</td>
<td>Ethernet adapter local area connection</td>
<td>IP address is acquired dynamically</td>
</tr>
</tbody>
</table>

Task 1: Secure Router and Configure Inter-VLAN Routing

In this task, you will secure administrative access to the Branch router and configure subinterfaces for VLANs 1, 10, and 20.

The Headquarters router was already configured by your colleague.
Activity Procedure
Complete the following steps:

Step 1
On the Branch router, protect privileged mode access with the password "cisco."

Step 2
Secure console access to the Branch router by enabling the password on the console line. Use "cisco" as the password.
Also, add the logging synchronous command to the console line so that all router status messages are displayed on a new line.

Step 3
Secure Telnet access to the router by enabling the password on virtual lines. Use "cisco" as the password.

Step 4
On the Branch router, configure the following login banner:

+----------------------------------------+
|                                        |
|         CCNA 2 Branch router            |
|                                        |
+----------------------------------------+

Step 5
Enable the GigabitEthernet0/0 interface on the Branch router. Create three subinterfaces and configure them with the following parameters:

<table>
<thead>
<tr>
<th>Subinterface Identifier</th>
<th>VLAN Identifier</th>
<th>IP Address/Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0.1</td>
<td>1 (native)</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>GigabitEthernet0/0.10</td>
<td>10</td>
<td>10.1.10.1/24</td>
</tr>
<tr>
<td>GigabitEthernet0/0.20</td>
<td>20</td>
<td>10.1.20.1/24</td>
</tr>
</tbody>
</table>

Activity Verification
You have completed this task when you attain these results:
**Step 1**

Exit the Branch router console and enter back into privileged mode:

```
Branch# exit
Branch con0 is now available
Press RETURN to get started.
```

You should see a login banner when entering the Branch router console. You will then need to enter the console password "cisco" and privilege password "cisco" to get back into privileged mode.

**Step 2**

On the Branch router, verify the state of configured subinterfaces:

```
Branch# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  up                    up
GigabitEthernet0/0.1       10.1.1.1        YES manual up                    up
GigabitEthernet0/0.10      10.1.10.1       YES manual up                    up
GigabitEthernet0/0.20      10.1.20.1       YES manual up                    up
<output omitted>
```

You should see that the subinterfaces are configured with IP addresses and are operational.

**Task 2: Configure Basic Settings, VLANs, and Trunks on Switch**

In this task, you will configure basic settings on the SW1 switch and secure administrative access to the switch. You will also configure VLANs and trunks on the switch and put PC1 into VLAN 10.

SW2 was preconfigured by your colleague.

**Activity Procedure**

Complete the following steps:

**Step 1**

The SW1 switch has no hostname configured. It is set to the default "Switch1." Change the hostname to "SW1."
**Step 2**
On the SW1 switch, enable the VLAN 1 interface and configure the VLAN 1 IP address. Use the job aids to determine the IP address.

**Step 3**
On the SW1 switch, configure encrypted enable password "cisco."

**Step 4**
On the SW1 switch, secure console access by configuring password "cisco."
Also, add **logging synchronous** to the console line so that all switch status messages are displayed on a new line.

**Step 5**
On the SW1 switch, create VLANs 10 and 20. SW2 already has these two VLANs configured.

**Step 6**
On the SW1 switch, configure a trunk on the FastEthernet0/3 and FastEthernet0/4 ports. Allow only VLANs 1, 10, and 20 on the trunk links.
SW2 already has both links toward SW1 that are configured as trunks.

**Step 7**
On SW1, configure the port connecting to PC1 (FastEthernet0/1) as an access port. Put the port into VLAN 10.

Interface FastEthernet 0/1 on SW2, which connects to PC2, is already configured as a member of VLAN 20.
**Step 8**  
Access PC1. Use "Administrator" as a username and "admin" as a password in order to log in. Set the following IP settings on the lab network adapter:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.100</td>
<td>255.255.255.0</td>
<td>10.1.10.1</td>
</tr>
</tbody>
</table>

**Step 9**  
On the SW1 switch, configure the FastEthernet 0/13 port as a trunk. Allow only VLANs 1, 10, and 20 on the trunk link. In this way, you will enable the switch to send traffic to or from all configured VLANs over the same port toward the Branch router.

**Activity Verification**  
You have completed this task when you attain these results:
**Step 1**

On the SW1 switch, verify the switchport status of the FastEthernet0/13 port:

```
SW1# show interfaces FastEthernet0/13 switchport
Name: Fa0/13
Switchport: Enabled
   Administrative Mode: trunk
   Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
```

You should see that the interface is in trunking mode.

**Step 2**

On the SW1 switch, verify the switchport status of the FastEthernet0/3 port:

```
SW1# show interfaces FastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
   Administrative Mode: trunk
   Operational Mode: trunk (suspended member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
```

You should see that the interface is in trunking mode.
Step 3

Verify the trunking status of the FastEthernet0/3 and FastEthernet0/4 ports on the SW1 switch:

```
SW1# show interfaces FastEthernet0/3 trunk
Port   Mode          Encapsulation    Status   Native vlan
Fa0/3  on            802.1q trunking 1
Port   Vlans allowed on trunk
Fa0/3  1,10,20
Port   Vlans allowed and active in management domain
Fa0/3  1,10,20
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/3  1,10,20
```

```
SW1# show interfaces FastEthernet0/4 trunk
Port   Mode          Encapsulation    Status   Native vlan
Fa0/4  on            802.1q trunking 1
Port   Vlans allowed on trunk
Fa0/4  1,10,20
Port   Vlans allowed and active in management domain
Fa0/4  1,10,20
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/4  1,10,20
```

You should see that both interfaces are in trunking mode, encapsulation is 802.1q, and VLANs 1, 10, and 20 are active.

Step 4

From PC1, ping the SW1 management IP address at 10.1.1.11.

```
C:\Windows\system32> ping 10.1.1.11
Pinging 10.1.1.11 with 32 bytes of data:
Request timed out.
Reply from 10.1.1.11: bytes=32 time=8ms TTL=254
Reply from 10.1.1.11: bytes=32 time=2ms TTL=254
Reply from 10.1.1.11: bytes=32 time=2ms TTL=254
Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
          Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

The ping should be successful.

Task 3: Troubleshoot EtherChannel

Two links between SW1 and SW2 are not successfully bundled into an EtherChannel port group. Your senior colleague says SW2 is correctly configured, but you have to make changes on SW1 to get EtherChannel working.

Activity Procedure

Complete the following steps:
Step 1

On switches SW1 and SW2, observe the VLAN 10 STP states:

```
SW1# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
  Address     001e.147c.bd00
  This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
  Address     001e.147c.bd00
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/1               Desg FWD 19        128.1    P2p
  Fa0/3               Desg FWD 19        128.3    P2p
  Fa0/4               Desg FWD 19        128.4    P2p
  Fa0/13              Desg FWD 19        128.13   P2p

SW2# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
  Address     001e.147c.bd00
  Cost        19
  Port        3 (FastEthernet0/3)
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
  Address     001e.147c.c880
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/3               Root FWD 19        128.3    P2p
  Fa0/4               Altn BLK 19        128.4    P2p
```

From the output, you can see that one port between SW1 and SW2 switches is in a blocking state. This indicates that both links are not utilized and that EtherChannel does not function.

Note that the blocking port may be on SW1 and not SW2. It depends on which switch was elected as the root bridge.
Step 2

On the SW1 and SW2 switches, observe the status of port-channel 1:

SW1# show interfaces Port-channel 1
Port-channel1 is down, line protocol is down (notconnect)
    Hardware is EtherChannel, address is 0000.0000.0000 (bia 0000.0000.0000)
    MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Auto-duplex, Auto-speed, link type is auto, media type is unknown
    input flow-control is off, output flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
    <output omitted>

SW2# show interfaces Port-channel 1
Port-channel1 is down, line protocol is down (notconnect)
    Hardware is EtherChannel, address is 0000.0000.0000 (bia 0000.0000.0000)
    MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Auto-duplex, Auto-speed, link type is auto, media type is unknown
    input flow-control is off, output flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
    <output omitted>

The EtherChannel between SW1 and SW2 is down.
Step 3

On the SW1 and SW2 switches, display the EtherChannel 1 details:

```
SW1# show etherchannel 1 detail
Group state = L2
Ports: 2  Maxports = 8
Port-channels: 1  Max Port-channels = 1
Protocol:  PAgP
Minimum Links: 0

Ports in the group:
-------------------
Port: Fa0/3
------------
Port state    = Up  Sngl-port-Bndl  Mstr  Not-in-Bndl
Channel group = 1  Mode = Automatic-Sl  Gcchange = 0
Port-channel  = null  GC = 0x00010001  Pseudo port-channel = Po1
Port index    = 0  Load = 0x00  Protocol = PAgP
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
      A - Device is in Auto mode.  P - Device learns on physical port.
      d - PAgP is down.
Timers:  H - Hello timer is running.  Q - Quit timer is running.
        S - Switching timer is running.  I - Interface timer is running.
Local information:  Hello Partner  PAgP Learning Group
Port Flags State Timers Interval Count Priority Method Ifindex
Fa0/3  A U2/S4  1s  0  128  Any  10003
Age of the port in the current state: 0d:00h:15m:01s

Port: Fa0/4
------------
Port state    = Up  Sngl-port-Bndl  Mstr  Not-in-Bndl
Channel group = 1  Mode = Automatic-Sl  Gcchange = 0
Port-channel  = null  GC = 0x00010001  Pseudo port-channel = Po1
Port index    = 0  Load = 0x00  Protocol = PAgP
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
      A - Device is in Auto mode.  P - Device learns on physical port.
      d - PAgP is down.
Timers:  H - Hello timer is running.  Q - Quit timer is running.
        S - Switching timer is running.  I - Interface timer is running.
Local information:  Hello Partner  PAgP Learning Group
Port Flags State Timers Interval Count Priority Method Ifindex
Fa0/4  A U2/S4  1s  0  128  Any  10004
Age of the port in the current state: 0d:00h:15m:01s

Port-channels in the group:
---------------------------
Port-channel: Po1
------------
Age of the Port-channel  = 0d:00h:15m:10s
Logical slot/port  = 2/1  Number of ports = 0
GC  = 0x00000000  HotStandBy port = null
Port state  = Port-channel Ag-Not-Inuse
Protocol = PAgP
Port security  = Disabled
```

```
SW2# show etherchannel 1 detail
Group state = L2
```
Ports: 2  Maxports = 16
Port-channels: 1 Max Port-channels = 16

**Protocol:** LACP

Minimum Links: 0

<table>
<thead>
<tr>
<th>Ports in the group:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------</td>
</tr>
</tbody>
</table>

**Port: Fa0/3**

---

Port state = Up Sngl-port-Bndl Mstr Not-in-Bndl

Channel group = 1  Mode = Passive  Gcchange = -

Port-channel = null  GC = -  Pseudo port-channel = Pol

Port index = 0  Load = 0x00  **Protocol = LACP**

Flags:  S - Device is sending Slow LACPDU  F - Device is sending fast LACPDU

A - Device is in active mode.  P - Device is in passive mode.

Local information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/3</td>
<td>SP</td>
<td>indep</td>
<td>Priority</td>
<td>Key Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>32768</td>
<td>0x1 0x1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0x104</td>
<td>0x7C</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:22m:27s

**Port: Fa0/4**

---

Port state = Up Sngl-port-Bndl Mstr Not-in-Bndl

Channel group = 1  Mode = Passive  Gcchange = -

Port-channel = null  GC = -  Pseudo port-channel = Pol

Port index = 0  Load = 0x00  **Protocol = LACP**

Flags:  S - Device is sending Slow LACPDU  F - Device is sending fast LACPDU

A - Device is in active mode.  P - Device is in passive mode.

Local information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/4</td>
<td>SP</td>
<td>indep</td>
<td>Priority</td>
<td>Key Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>32768</td>
<td>0x1 0x1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0x105</td>
<td>0x7C</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:22m:27s

**Port-channels in the group:**

---

**Port-channel: Po1**  (Primary Aggregator)

---

Age of the Port-channel = 0d:00h:22m:35s

Logical slot/port = 2/1  Number of ports = 0

HotStandBy port = null

Port state = Port-channel Ag-Not-Inuse

**Protocol** = LACP

Port security = Disabled

From the output, you can see that the SW1 switch is incorrectly configured, so use the PAgP link aggregation protocol instead of LACP. The SW2 switch is correctly configured with LACP.

**Step 4**

Reconfigure the SW1 switch to use LACP as a link aggregation protocol.

**Activity Verification**

You have completed this task when you attain these results:
Step 1

On the SW1 switch, display the EtherChannel 1 details:

```bash
SW1# show etherchannel 1 detail
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
Minimum Links: 0

Ports in the group:

-------------------
Port: Fa0/3
-------------------
Port state = Up Mstr Assoc In-Bndl
Channel group = 1 Mode = Active Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = LACP
Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs.
A - Device is in active mode. P - Device is in passive mode.
Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key Index</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/3</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x104</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/3</td>
<td>SP</td>
<td>32768</td>
<td>001e.147c.c880</td>
<td>19s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x104</td>
<td>0x3C</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:03m:57s

Port: Fa0/4

-------------------
Port state = Up Mstr Assoc In-Bndl
Channel group = 1 Mode = Active Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = LACP
Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs.
A - Device is in active mode. P - Device is in passive mode.
Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key Index</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/4</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x105</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/4</td>
<td>SP</td>
<td>32768</td>
<td>001e.147c.c880</td>
<td>18s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x105</td>
<td>0x3C</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:03m:57s

Port-channels in the group:

---------------------------
Port-channel: Po1 (Primary Aggregator)
---------------------------
Age of the Port-channel = 0d:00h:32m:44s
Logical slot/port = 2/1 Number of ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Port security = Disabled
Ports in the Port-channel:
Index Load Port EC state No of bits
```
The SW1 switch is now using LACP as a link aggregation protocol.

**Step 2**

On the SW1 and SW2 switches, observe the VLAN 10 STP states:

```
SW1# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
               Address     001e.147c.bd00
  This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID Priority    32778 (priority 32768 sys-id-ext 10)
               Address     001e.147c.bd00
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/1               Desg FWD 19        128.1    P2p
  Fa0/13              Desg FWD 19        128.13   P2p
  Po1                 Desg FWD 12        128.64   P2p

SW2# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
               Address     001e.147c.bd00
  Cost        12
  Port        64 (Port-channel1)
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID Priority    32778 (priority 32768 sys-id-ext 10)
               Address     001e.147c.c880
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Po1                 Root FWD 12        128.64   P2p
```

From the output, you can see that all ports between SW1 and SW2 switches are active. You will also see the Port-channel 1 interface present in the output.
Step 3

On the SW1 and SW2 switches, observe the status of Port-channel 1:

```
SW1# show interfaces Port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001e.147c.bd04 (bia 001e.147c.bd04)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa0/3 Fa0/4
<output omitted>

SW2# show interfaces Port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001e.147c.c883 (bia 001e.147c.c883)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa0/3 Fa0/4
<output omitted>
```

The EtherChannel between SW1 and SW2 is up. FastEthernet 0/3 and FastEthernet 0/4 are listed as members of Port-channel 1.

Task 4: Port Security (Trouble Ticket)

You received reports that connectivity between PC1 and PC2 is broken. In this task, you will resolve this connectivity issue.

Activity Procedure

Complete the following steps:
**Step 1**

Access PC2 by using username "Administrator" and password "admin." Ping the SW1 management IP address at 10.1.1.11.

```
C:\Windows\system32> ping 10.1.1.11
Pinging 10.1.1.11 with 32 bytes of data:
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Reply from 10.1.20.100: Destination host unreachable.
Ping statistics for 10.1.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The ping is not successful.

**Step 2**

On the SW2 switch, check the interface status.

```
SW2# show interfaces FastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 001e.147c.c881 (bia 001e.147c.c881)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

Interface FastEthernet 0/1 on the SW2 switch is in the error-disable state. This indicates that the interface is probably disabled due to a port security feature.

**Step 3**

On the SW2 switch, check the port security settings on the FastEthernet 0/1 interface.

```
SW2# show port-security interface FastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.2996.494d:20
Security Violation Count   : 1
```

The interface is disabled due to the port security feature.
Step 4

On the SW2 switch, reconfigure port security on the interface connecting to PC2 (FastEthernet0/1) in order to allow only PC2 to connect to the switch. Use the following port security parameters:

- Violation action: Protect
- Maximum MAC addresses: 1
- MAC address: PC2

Remember to disable and then enable port FastEthernet0/1 after you finish the port security configuration. This is needed to bring it out of the error-disable state.

Activity Verification

You have completed this task when you attain these results:

Step 1

From PC2, ping the SW1 management IP address at 10.1.1.11.

C:\Windows\system32> ping 10.1.1.11
Pinging 10.1.1.11 with 32 bytes of data:
Reply from 10.1.1.11: bytes=32 time=6ms TTL=254
Reply from 10.1.1.11: bytes=32 time=4ms TTL=254
Reply from 10.1.1.11: bytes=32 time=3ms TTL=254
Reply from 10.1.1.11: bytes=32 time=2ms TTL=254
Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms

The ping should be successful now.

Step 2

From PC2, ping PC1 (10.1.10.100).

C:\Windows\system32> ping 10.1.10.100
Pinging 10.1.10.100 with 32 bytes of data:
Reply from 10.1.10.100: bytes=32 time=7ms TTL=127
Reply from 10.1.10.100: bytes=32 time=1ms TTL=127
Reply from 10.1.10.100: bytes=32 time=1ms TTL=127
Reply from 10.1.10.100: bytes=32 time=1ms TTL=127
Ping statistics for 10.1.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms

The ping should be successful.
Task 5: Enable SSH Access on the Branch Router

A senior colleague instructed you to configure SSH on the Branch router. He added that Telnet should not be allowed.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, enable SSH version 2 remote access. Use 1024-bit RSA keys.

Only SSH should be allowed.

Step 2

Create a local user account on the Branch router that will be used to authenticate users accessing the router via SSH or Telnet. Use "ccna" as a username and "cisco" as the password. Configure the virtual lines for checking the username and password.

Activity Verification

You have completed this task when you attain these results:
**Step 1**

On PC1, start PuTTY by double-clicking the PuTTY icon on the desktop. Establish an SSH session to the Branch router at 10.1.10.1. Accept the router fingerprint when asked. Use "ccna" as the username and "cisco" as the password in order to log in. Enter privileged EXEC mode using the "cisco" password in order to verify if the enable password is correctly configured.

```
login as: ccna
+----------------------------------------+
|                                        |
|         CCNA 2 Branch router           |
|                                        |
+----------------------------------------+
Using keyboard-interactive authentication.
Password: cisco
Branch> enable
Password: cisco
Branch#
```

Establishment of the SSH session should be successful.

**Step 2**

Close the SSH session on PC1.
Task 6: Configure DHCP Server

A senior engineer instructed you to lessen the administrative overhead of assigning static IP addresses to hosts in VLAN 10. In this task, you will configure the Branch router to act as a DHCP server for VLAN 10. Until now, PC1 had a static IP address, but now PC1 will acquire the static IP address dynamically.

Activity Procedure
Complete the following steps:

Step 1
Configure the Branch router as a DHCP server for VLAN 10 with the following parameters:

- DHCP pool name: VLAN10
- DHCP network: 10.1.10.0/24
- Default router: 10.1.10.1
- Lease: 3 minutes
- Exclude IP addresses: 10.1.10.1-10.1.10.199 and 10.1.10.201-10.1.10.254

Step 2
Access PC1 by using username "Administrator" and password "admin" and change the IPv4 setting on the lab Ethernet adapter to acquire the IP setting dynamically.

Activity Verification
You have completed this task when you attain these results:
Step 1

Verify the IP configuration on PC1.

C:\Windows\system32> `ipconfig /all`
Windows IP Configuration
  Host Name . . . . . . . . . . . . : Windows7
  Primary Dns Suffix . . . . . . . :
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter LAB:
  Connection-specific DNS Suffix . :
  Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter #2
  Physical Address . . . . . . . . : 00-0C-29-36-69-78
  DHCP Enabled. . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . : Yes
  Link-local IPv6 Address . . . . : fe80::2ca7:950f:d859:9256%13(Preferred)
  IPv4 Address . . . . . . . . . : 10.1.10.200(Preferred)
  Subnet Mask . . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . . . : Wednesday, November 28, 2012 10:33:01 AM
  Lease Expires . . . . . . . . . : Wednesday, November 28, 2012 10:36:01 AM
  Default Gateway . . . . . . . . : 10.1.10.1
  DHCP Server . . . . . . . . . : 10.1.10.1
  DHCPv6 IAID . . . . . . . . . : 285215785
  DHCPv6 Client DUID. . . . . : 00-01-00-01-13-3B-A1-51-00-0C-29-87-5C-B5
  DNS Servers . . . . . . . . . : fec0:0:0:ffff::1%1
                               : fec0:0:0:ffff::2%1
                               : fec0:0:0:ffff::3%1
  NetBIOS over Tcpip. . . . . . : Disabled
<output omitted>

The IPv4 address on PC1 should be 10.1.10.200/24, and the default gateway should be 10.1.10.1.

Step 2

From PC1, ping PC2 (10.1.20.100).

C:\Windows\system32> `ping 10.1.20.100`
Pinging 10.1.20.100 with 32 bytes of data:
  Reply from 10.1.20.100: bytes=32 time=6ms TTL=127
  Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
  Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
  Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Ping statistics for 10.1.20.100:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 6ms, Average = 2ms

The ping should be successful.
**Step 3**

On the Branch router, display the DHCP bindings.

```
Branch# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address     Client-ID/    Lease expiration        Type
              Hardware address/    User name
10.1.1.200     0100.0c29.3669.78  Nov 28 2012 09:38 AM    Automatic
```

You should see one automatic binding to IP address 10.1.1.200.

**Task 7: Stateless Autoconfiguration on the PC**

The Headquarters router was preconfigured with IPv6 addresses and routing by your colleague. In this task, you will enable IPv6 on the Branch router and then verify that PC1 received an IPv6 address through the stateless autoconfiguration feature.

**Activity Procedure**

Complete the following steps:

**Step 1**

On the Branch router, enable IPv6 unicast routing.

**Step 2**

On the Branch router, configure IPv6 addresses on interfaces that are listed in the following table.

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6 Address/Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0.1</td>
<td>2001:DB8:0A01:100::1/64</td>
</tr>
<tr>
<td>GigabitEthernet0/0.10</td>
<td>2001:DB8:0A01:A00::1/64</td>
</tr>
<tr>
<td>GigabitEthernet0/0.20</td>
<td>2001:DB8:0A01:1400::1/64</td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>2001:DB8:D1A5:C900::1/64</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>2001:DB8:C0A8:100::1/64</td>
</tr>
</tbody>
</table>

**Activity Verification**

You have completed this task when you attain these results:
Step 1
Verify IPv6 configuration on PC1.

PC1 will set the IPv6 address automatically because stateless autoconfiguration is enabled by default.

Observe the IPv6 address on the lab Ethernet adapter on PC1.

C:\Windows\system32> ipconfig /all
Windows IP Configuration
  Host Name . . . . . . . . . . . . : Windows7
  Primary Dns Suffix . . . . . . . :
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . : No
  WINS Proxy Enabled. . . . . . . : No
Ethernet adapter LAB:
  Connection-specific DNS Suffix . :
  Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter #2
  Physical Address . . . . . . . . : 00-0C-29-36-69-78
  DHCP Enabled. . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . : Yes
  IPv6 Address. . . . . . . . . . : 2001:db8:a01:a00:2ca7:950f:d859:9256(Pref erred)
    Temporary IPv6 Address. . . . . : 2001:db8:a01:a00:6118:3007:18b4:1bb6(Pref erred)
    Link-local IPv6 Address . . . . : fe80::2ca7:950f:d859:9256%13(Preferred)
  IPv4 Address. . . . . . . . . . : 10.1.10.200(Preferred)
  Subnet Mask . . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . . . : Wednesday, November 28, 2012 10:33:01 AM
  Lease Expires . . . . . . . . . : Wednesday, November 28, 2012 11:15:01 AM
  Default Gateway . . . . . . . . : fe80::6e20:56ff:fe17:b148%13
    10.1.10.1
  DHCP Server . . . . . . . . . . : 10.1.10.1
  DNS Servers . . . . . . . . . . : fec0:0:0:ffff::1%1
    fec0:0:0:ffff::2%1
    fec0:0:0:ffff::3%1
  NetBIOS over Tcpip. . . . . . . : Disabled
<output omitted>

Step 2
From PC2, ping the PC1 IPv6 address that was learned from the previous step.

C:\Windows\system32> ping 2001:db8:a01:a00:2ca7:950f:d859:9256
Ping 2001:db8:a01:a00:2ca7:950f:d859:9256 with 32 bytes of data:
  Reply from 2001:db8:a01:a00:2ca7:950f:d859:9256: time=24ms
  Reply from 2001:db8:a01:a00:2ca7:950f:d859:9256: time=1ms
  Reply from 2001:db8:a01:a00:2ca7:950f:d859:9256: time=1ms
  Reply from 2001:db8:a01:a00:2ca7:950f:d859:9256: time=1ms
Ping statistics for 2001:db8:a01:a00:2ca7:950f:d859:9256:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 24ms, Average = 6ms

The ping should be successful.
Task 8: Configure PPP Encapsulation

In this task, you will configure PPP encapsulation on the serial link between the Branch and Headquarters routers.

The Headquarters router is already configured with PPP encapsulation on the serial interface.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, enable the first serial interface.

Step 2

On the Branch router, verify the status of the first serial interface.

```
Branch# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  up                    up
GigabitEthernet0/0.1       10.1.1.1        YES manual up                    up
GigabitEthernet0/0.10      10.1.10.1       YES manual up                    up
GigabitEthernet0/0.20      10.1.20.1       YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                unassigned      YES unset  up                    down
```

The status of the Serial 0/0/0 interface is up, but the protocol is down.

Step 3

On the Branch router, verify the encapsulation of the first serial interface.

```
Branch# show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is down
Hardware is WIC MBRD Serial
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:01, output 00:00:03, output hang never
Last clearing of "show interface" counters 00:58:05
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
<output omitted>
```

Encapsulation on the Serial 0/0/0 interface is HDLC, but it should be set to PPP.

Step 4

On the Branch router, change encapsulation on the first serial interface to the PPP and configure it with an IP address of 192.168.1.1/24.
Activity Verification
You have completed this task when you attain these results:

Step 1

On the Branch router, verify the status of the first serial interface.

```
Branch# show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
   Hardware is WIC MBRD Serial
   Internet address is 192.168.1.1/24
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

Encapsulation on the Serial 0/0/0 interface is PPP. The Serial 0/0/0 interface is operational.

Step 2

From the Branch router, ping the Headquarters router (192.168.1.2). The ping should be successful.

```
Branch# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

Task 9: Configure Dynamic Routing Protocol

Now that the Branch router has Layer 3 connectivity with the Headquarters router, you are instructed to configure single-area OSPF on the Branch router in order to exchange routing information with the Headquarters router. The Headquarters router has been preconfigured with OSPF by your colleague.

Activity Procedure

Complete the following steps:

Step 1

On the Branch router, create OSPF routing process 1 and enable OSPF routing in Area 0 for the following networks:

- 192.168.1.0/24
- 10.1.1.0/24
- 10.1.10.0/24
- 10.1.20.0/24

Activity Verification

You have completed this task when you attain these results:
Step 1
Verify OSPF neighbors on the Branch router.

```
Branch# show ip ospf neighbor
Neighbor ID   Pri   State   Dead Time   Address         Interface
1.1.1.1       0   FULL/ -   00:00:39    192.168.1.2     Serial0/0/0
```

You should see the Headquarters router as the OSPF neighbor in FULL state.

Step 2
Issue the `show ip ospf` command and verify that four interfaces are configured in OSPF Area 0.

```
Branch# show ip ospf
Routing Process "ospf 1" with ID 192.168.1.1
Start time: 13:04:36.668, Time elapsed: 00:29:30.400
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFvs 10000 msecs
Maximum wait time between two consecutive SPFvs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
   Number of interfaces in this area is 4
   Area has no authentication
   SPF algorithm last executed 00:28:50.972 ago
   SPF algorithm executed 3 times
   Area ranges are
   Number of LSA 2. Checksum Sum 0x00D78C
   Number of opaque link LSA 0. Checksum Sum 0x000000
   Number of DCbitless LSA 0
   Number of indication LSA 0
   Number of DoNotAge LSA 0
   Flood list length 0
```
Step 3

Verify the routing table on the Branch router.

Branch# show ip route
Codes:  L - local,  C - connected,  S - static,  R - RIP,  M - mobile,  B - BGP
       D - EIGRP,  EX - EIGRP external,  O - OSPF,  IA - OSPF inter area
       N1 - OSPF NSSA external type 1,  N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,  E2 - OSPF external type 2
       i - IS-IS,  su - IS-IS summary,  L1 - IS-IS level-1,  L2 - IS-IS level-2
       ia - IS-IS inter area,  * - candidate default,  U - per-user static route
       o - ODR,  P - periodic downloaded static route,  H - NHRP,  l - LISP
       + - replicated route,  % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
   C        10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
   L        10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
   L        10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C        10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
   L        10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
172.16.0.0/24 is subnetted, 1 subnets
   O        172.16.1.0 [110/65] via 192.168.1.2, 00:01:29, Serial0/0/0
       192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
   C        192.168.1.1/24 is directly connected, Serial1/0/0
   L        192.168.1.1/32 is directly connected, Serial1/0/0
   C        192.168.1.2/32 is directly connected, Serial1/0/0
       209.165.201.0/27 is subnetted, 1 subnets
   O        209.165.201.0 [110/65] via 192.168.1.2, 00:01:29, Serial1/0/0

You should see the 172.16.1.0/24 network as an OSPF route. The network should be accessible over the Serial0/0/0 interface.

Task 10: Configure the OSPFv3 Routing Protocol

In this task, you will enable the OSPFv3 routing protocol to route for IPv6 between the Branch and Headquarters routers. The Headquarters router has already been preconfigured by OSPFv3 by your colleague.

Activity Procedure
Complete the following steps:
**Step 1**

On the Branch router, enable the following interfaces for OSPFv3 in Area 0. Use OSPFv3 process ID 1:

- Serial0/0/0
- GigabitEthernet0/0.1
- GigabitEthernet0/0.10
- GigabitEthernet0/0.20

You should see that the OSPFv3 adjacency went up immediately after you enabled OSPFv3 on the Serial0/0/0 interface:

```
Nov 29 09:24:20.975: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

**Activity Verification**

You have completed this task when you attain these results:

**Step 1**

Verify the OSPFv3 neighbors on the Branch router.

```
Branch# show ipv6 ospf neighbor
OSPFv3 Router with ID (192.168.1.1) (Process ID 1)

Neighbor ID    Pri State  Dead Time Interface ID Interface
1.1.1.1         0 FULL/  - 00:00:35       6 Serial0/0/0
```

You should see the Headquarters router as the OSPFv3 neighbor.
Step 2

Issue the `show ipv6 ospf` command and verify that four interfaces are configured in OSPFv3 Area 0.

```console
Branch# show ipv6 ospf
Routing Process "ospfv3 1" with ID 192.168.1.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF 10000 msecs
Maximum wait time between two consecutive SPF 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
   Area BACKBONE(0)
      Number of interfaces in this area is 4
      SPF algorithm executed 5 times
      Number of LSA 9. Checksum Sum 0x056DE6
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
<output omitted>
```

You should see that OSPFv3 is enabled for four interfaces in Area 0.
Step 3

Verify the IPv6 routing table on the Branch router.

```plaintext
Branch# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
    B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
    IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
    ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:DB8:A01:100::/64 [0/0]
    via GigabitEthernet0/0.1, directly connected
L   2001:DB8:A01:100::1/128 [0/0]
    via GigabitEthernet0/0.1, receive
C   2001:DB8:A01:A00::/64 [0/0]
    via GigabitEthernet0/0.10, directly connected
L   2001:DB8:A01:A00::1/128 [0/0]
    via GigabitEthernet0/0.10, receive
C   2001:DB8:A01:1400::/64 [0/0]
    via GigabitEthernet0/0.20, directly connected
L   2001:DB8:A01:1400::1/128 [0/0]
    via GigabitEthernet0/0.20, receive
O   2001:DB8:AC10:100::64/128 [110/64]
    via FE80::FE99:47FF:FEDE:B4B8, Serial0/0/0
C   2001:DB8:C0A8:100::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:C0A8:100::1/128 [0/0]
    via Serial0/0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
```

You should see the 2001:DB8:AC10:100::/64 network that is learned through OSPF and with the Headquarters router as the next hop. This is the network where the server is located.

Step 4

Access PC1 and open a command prompt. Ping the server at 2001:db8:ac10:100::64.

```plaintext
C:\Windows\system32> ping 2001:db8:ac10:100::64
Pinging 2001:db8:ac10:100::64 with 32 bytes of data:
Reply from 2001:db8:ac10:100::64: time=62ms
Reply from 2001:db8:ac10:100::64: time=50ms
Reply from 2001:db8:ac10:100::64: time=46ms
Reply from 2001:db8:ac10:100::64: time=46ms
Ping statistics for 2001:db8:ac10:100::64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 62ms, Average = 51ms
```

The ping should be successful.
Task 11: Troubleshoot the IP Access Control List (Trouble Ticket)

While there is connectivity between the two sites, the user using PC2 is reporting that he is unable to ping the server at 172.16.1.100. In this task, you are required to resolve this issue.

Activity Procedure

Complete the following steps:

Step 1

First check whether PC2 is really not able to ping server IP address 172.16.1.100.

The ping should fail. Find the solution to this issue.

Activity Verification

You have completed this task when you attain this result:

Step 1

From PC2, ping the server IP address at 172.16.1.100.

C:\Windows\system32> ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=38ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Reply from 172.16.1.100: bytes=32 time=36ms TTL=254
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 38ms, Average = 36ms

The ping should be successful.
Lab Answer Keys

Lab S-1: Review

Task 1: Configure Basic Settings, VLANs, Trunks, and Port Security on Switches

**Step 1**

Enter the following commands on the SW1 switch:

```
SW1>enable
SW1#erase startup-config
SW1#delete vlan.dat
SW1#reload
```

Enter the following commands on the SW2 switch:

```
SW2>enable
SW2#write erase
SW2#delete vlan.dat
SW2#reload
```

**Step 2**

Enter the following commands on the SW1 switch:

```
Switch#configure terminal
Switch(config)#hostname SW1
```

Enter the following commands on the SW2 switch:
Switch#configure terminal
Switch(config)#hostname SW2

**Step 3**

Enter the following commands on the SW1 switch:

```
SW1(config-if)#interface vlan 1
SW1(config-if)#ip address 10.1.1.11 255.255.255.0
SW1(config-if)#no shutdown
```

Enter the following commands on the SW2 switch:

```
SW2(config-if)#interface vlan 1
SW2(config-if)#ip address 10.1.1.12 255.255.255.0
SW2(config-if)#no shutdown
```

**Step 4**

Enter the following command on the SW1 switch:

```
SW1(config)#enable secret cisco
```

Enter the following command on the SW2 switch:

```
SW2(config)#enable secret cisco
```

**Step 5**

Enter the following commands on the SW1 switch:

```
SW1(config)#line console 0
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#logging synchronous
```

Enter the following commands on the SW2 switch:

```
SW2(config)#line console 0
SW2(config-line)#password cisco
SW2(config-line)#login
SW2(config-line)#logging synchronous
```

**Step 6**

Enter the following commands on the SW1 switch:
Enter the following commands on the SW1 switch:

```
SW1(config)#configure terminal
SW1(config)#username ccna password cisco
SW1(config)#line vty 0 ?
   <1-15>  Last Line number
   <cr>
SW1(config)#line vty 0 15
SW1(config-line)#login local
```

**Step 7**

Enter the following commands on the SW2 switch:

```
SW2(config)#configure terminal
SW2(config)#username ccna password cisco
SW2(config)#line vty 0 ?
   <1-15>  Last Line number
   <cr>
SW2(config)#line vty 0 15
SW2(config-line)#login local
```

**Step 8**

Enter the following commands on the SW1 switch:
SW1(config)#vlan 10
SW1(config)#vlan 20

Enter the following commands on the SW2 switch:

SW2(config)#vlan 10
SW2(config)#vlan 20

**Step 9**

Enter the following commands on the SW1 switch:

SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 1,10,20
SW1(config)#
SW1(config)#interface FastEthernet0/4
SW1(config-if)#shutdown

Enter the following commands on the SW2 switch:

SW2(config)#interface FastEthernet0/3
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 1,10,20
SW2(config)#
SW2(config)#interface FastEthernet0/4
SW2(config-if)#shutdown

**Step 10**

Enter the following commands on the SW1 switch:

SW1(config)#interface FastEthernet0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10

**Step 11**

Enter the following commands on the SW2 switch:

SW2(config)#interface FastEthernet0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20

**Step 18**

Enter the following commands on the SW1 switch:
**Task 2: Configure Inter-VLAN Routing**

**Step 1**

Enter the following commands on the Branch router:

```
Branch>enable
Branch#erase startup-config
Branch#reload
```

**Step 2**

Enter the following commands on the Branch router:

```
Router#configure terminal
Router(config)#hostname Branch
```

**Step 3**

Enter the following command on the Branch router:

```
Branch(config)#enable secret cisco
```
**Step 4**

Enter the following commands on the Branch router:

```
Branch(config)#line console 0
Branch(config-line)#password cisco
Branch(config-line)#login
Branch(config-line)#logging synchronous
```

**Step 5**

Enter the following commands on the Branch router:

```
Branch(config)#line vty 0 1114
Branch(config-line)#password cisco
Branch(config-line)#login
```

**Step 6**

Enter the following commands on the Branch router:

```
Branch(config)#interface GigabitEthernet0/0
Branch(config-if)#no shutdown
Branch(config)#
Branch(config-if)#interface GigabitEthernet0/0.1
Branch(config-subif)#encapsulation dot1Q 1 native
Branch(config-subif)#ip address 10.1.1.1 255.255.255.0
Branch(config)#
Branch(config-subif)#interface GigabitEthernet0/0.10
Branch(config-subif)#encapsulation dot1Q 10
Branch(config-subif)#ip address 10.1.10.1 255.255.255.0
Branch(config)#
Branch(config-subif)#interface GigabitEthernet0/0.20
Branch(config-subif)#encapsulation dot1Q 20
Branch(config-subif)#ip address 10.1.20.1 255.255.255.0
```

**Step 7**

Enter the following commands on the SW1 switch:

```
SW1#configure terminal
SW1(config)#interface FastEthernet0/13
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 1,10,20
```
Step 8

Enter the following command on the SW1 switch:

```
SW1(config)#ip default-gateway 10.1.1.1
```

Enter the following command on the SW2 switch:

```
SW2(config)#ip default-gateway 10.1.1.1
```

Task 3: Configure Internet Connectivity

Step 1

Enter the following commands on the Branch router:

```
Branch#configure terminal
Branch(config)#interface GigabitEthernet0/1
Branch(config-if)#ip address 209.165.201.1 255.255.255.224
Branch(config-if)#description Link to HQ
Branch(config-if)#no shutdown
```

Step 2

Enter the following commands on the Branch router:

```
Branch(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

Step 3

Enter the following commands on the Branch router:

```
Branch(config)#access-list 1 permit 10.1.10.0 0.0.0.255
Branch(config)#access-list 1 permit 10.1.20.0 0.0.0.255
```

Step 4

Enter the following commands on the Branch router:
Task 4: Configure WAN Connectivity and a Dynamic Routing Protocol

Step 1
Enter the following commands on the Branch router:

```
Branch(config)#configure terminal
Branch(config)#interface Serial0/0/0
Branch(config-if)#ip address 192.168.1.1 255.255.255.0
Branch(config-if)#description Link to HQ
Branch(config-if)#no shutdown
```

Step 2
Enter the following commands on the Branch router:

```
Branch(config)#router ospf 1
Branch(config-router)#network 192.168.1.0 0.0.0.255 area 0
Branch(config-router)#network 10.1.1.0 0.0.0.255 area 0
Branch(config-router)#network 10.1.10.0 0.0.0.255 area 0
Branch(config-router)#network 10.1.20.0 0.0.0.255 area 0
```

Step 7
Enter this command on the Branch router:

```
Branch#copy running-config startup-config
```

Enter this command on the SW1 switch:

```
SW1#copy running-config startup-config
```

Enter this command on the SW2 switch:

```
SW2#copy running-config startup-config
```
Lab 1-1: Troubleshooting VLANs and Trunks

Task 1: Troubleshoot VLAN Connectivity

Step 5
The interface is in VLAN 10. However, the switch port is inactive, which means that VLAN 10 does not exist on the switch.

Step 7
Enter this command on the SW1 switch:

   SW1(config)#vlan 10

Task 2: Troubleshoot Trunk Connectivity Between the Switches

Step 7
The trunk has not established because both interfaces are configured for dynamic auto DTP mode. This combination does not establish a trunk.

Step 8
Enter these commands on the SW2 switch:

   SW2(config)#interface fastEthernet0/3
   SW2(config-if)#switchport mode trunk
   SW2(config-if)#switchport nonegotiate

Step 9
Enter these commands on the SW1 switch:

   SW1(config)#interface fastEthernet0/3
   SW1(config-if)#switchport mode trunk
   SW1(config-if)#switchport nonegotiate

Step 13
Enter these commands on the SW1 switch:
SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport trunk native vlan 1

**Step 14**

Enter these commands on the SW2 switch:

```
SW2(config)#interface FastEthernet0/3
SW2(config-if)#switchport trunk native vlan 1
```

**Step 16**

Enter this command on the SW1 switch:

```
SW1#copy running-config startup-config
```

Enter this command on the SW2 switch:

```
SW2#copy running-config startup-config
```

**Lab 1-2: Optimizing STP**

**Task 1: Verify STP Operation**

**Step 1**

Enter these commands on the SW1 switch:

```
SW1#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface FastEthernet 0/4
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport nonegotiate
SW1(config-if)#switchport trunk allowed vlan 1,10,20
SW1(config-if)#no shutdown
```

Enter these commands on the SW2 switch:

```
SW2#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#interface FastEthernet 0/4
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport nonegotiate
SW2(config-if)#switchport trunk allowed vlan 1,10,20
SW2(config-if)#no shutdown
```

**Task 2: Influence Root Bridge Selection**
Step 2
Enter this command on the SW2 switch:

```
SW2(config)#spanning-tree vlan 20 root primary
```

Step 5
Enter these commands on the SW1 switch:

```
SW1(config)#spanning-tree vlan 1 root primary
SW1(config)#spanning-tree vlan 10 root primary
```

Task 3: Implement STP PortFast

Step 1
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#shutdown
```

Step 3
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#no shutdown
```

Step 4
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#spanning-tree portfast
```

Step 5
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#shutdown
SW1(config-if)#no shutdown
```
Task 4: Implement STP BPDU Guard

Step 2
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/3
SW1(config-if)#spanning-tree bpduguard enable
```

Step 4
Enter these commands on the SW1 switch:

```
SW1(config)#interface FastEthernet 0/3
SW1(config)#no spanning-tree bpduguard enable
SW1(config)#shutdown
SW1(config)#no shutdown
```

Step 7
Enter this command on the SW1 switch:

```
SW1#copy running-config startup-config
```

Enter this command on the SW2 switch:

```
SW2#copy running-config startup-config
```

Lab 1-3: Configuring EtherChannel

Task 1: Configure EtherChannel

Step 2
Enter these commands on the SW1 switch:

```
SW1(config)#interface range fastEthernet 0/3 - 4
SW1(config-if-range)#channel-group 1 mode active
```

Step 3
Enter these commands on the SW2 switch:
Task 2: Verify EtherChannel Redundancy

Step 3
Enter these commands on the SW1 switch:

```
SW1(config)#interface fastEthernet0/3
SW1(config-if)#shutdown
```

No packets were lost during the interface shutdown.

Step 5
Enter these commands on the SW1 switch:

```
SW1(config)#interface fastEthernet0/3
SW1(config-if)#no shutdown
```

Step 8
Enter this command on the SW1 switch:

```
SW1#copy running-config startup-config
```

Enter this command on the SW2 switch:

```
SW2#copy running-config startup-config
```

Lab 2-1: Troubleshooting IP Connectivity

Task 1: Troubleshoot the Default Route

Step 5
Enter this command on the Branch router:

```
Branch(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

Task 2: Troubleshoot an ACL
**Step 5**

Enter these commands on the Branch router:

```
Branch(config)#ip access-list extended Outbound-ACL
Branch(config-ext-nacl)#permit tcp any any eq Telnet
Branch(config-ext-nacl)#permit tcp any any eq www
```

**Step 7**

To see a successful response from the `traceroute` command on SW1, allow UDP on the Branch router. The `traceroute` command is sending UDP packets with different TTL values. As a response to the original UDP packet, the ICMP packet is sent.

Because it was said that only HTTP and Telnet traffic should be allowed, access list permitting `traceroute` is not needed at this point.

**Task 3: Troubleshoot the Default Gateway and Name Resolution Settings**

**Step 7**

Enter this command on the Branch router.

```
Branch#copy running-config startup-config
```

**Lab 3-1: Implementing EIGRP**

**Task 1: Verify Connectivity to Remote Network**

**Step 1**

On the Branch router, enter the following sequence of commands:

```
Branch#configure terminal
Branch(config)#interface Serial 0/0/0
Branch(config-if)#no shutdown
```

**Step 3**

No, the route to the network of 172.16.1.0/24 is not a static route. The route was learned by the OSPF routing process.

**Task 2: Configure and Verify EIGRP**
**Step 1**

Enter this command sequence on the Branch router:

```
Branch>enable
Branch#configure terminal
Branch(config)#router eigrp 1
Branch(config-router)#
```

**Step 2**

Enter this command sequence on the Branch router:

```
Branch(config-router)#network 10.1.1.0 0.0.0.255
Branch(config-router)#network 10.1.10.0 0.0.0.255
Branch(config-router)#network 10.1.20.0 0.0.0.255
Branch(config-router)#network 192.168.1.0 0.0.0.255
```

**Task 3: Investigate Neighbor Events**

**Step 1**

Enter the following command on the Branch router:

```
Branch#debug eigrp neighbors
EIGRP Static Neighbor debugging is on
```

**Step 2**

Enter the following commands on the Branch router:

```
Branch#configure terminal
Branch(config)#interface S0/0/0
Branch(config-if)#shutdown
```

**Step 3**

Enter the following commands on the Branch router:

```
Branch#configure terminal
Branch(config)#interface S0/0/0
Branch(config-if)#no shutdown
```

**Task 4: Disable OSPF Routing Process**
**Step 2**

Enter this sequence of commands on the Branch router:

```
Branch#
Branch(config)#no router ospf 1
```

**Step 4**

Enter this command on the Branch router:

```
Branch#copy running-config startup-config
```

---

**Lab 3-2: Troubleshooting EIGRP**

**Task 1: Troubleshoot Basic Connectivity**

---

**Step 4**

The Serial0/0/0 interface that is connected to the HQ router is not operational because it is administratively shut down.

---

**Step 5**

Enter the following sequence of commands on the Branch router:

```
Branch#configure terminal
Branch(config)#interface s0/0/0
Branch(config-if)#no shutdown
Branch(config-if)#
```

---

**Task 2: Troubleshooting EIGRP Neighbors**

---

**Step 1**

Some possible causes of routers not being EIGRP neighbors are mismatched EIGRP numbers, the network on the link between routers is not being advertised, or there is an interface that is configured as passive.

---

**Step 2**

The AS numbers match and both routers are advertising the 192.168.1.0 network that is their WAN link, but the Branch router has the Serial0/0/0 interface configured as passive, therefore it is not sending or receiving EIGRP hello packets to the HQ router. Adjacency cannot be established without the hello packets.
Step 3

On the Branch router, enter the following sequence of commands:

```
Branch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#router eigrp 1
Branch(config-router)#no passive-interface serial 0/0/0
```

Task 3: Troubleshooting Routing Table Issues

Step 1

There might be a routing table issue. It might be that all necessary networks are not being advertised or that there is an ACL that is blocking advertisements.

Step 2

The HQ router is advertising the 172.16.1.0/24 network and the Branch router knows about this network. The next step should probably be to investigate if the Branch router is advertising the network to which PC1 belongs. This is why the ping output states "Request timed out." Branch knows how to get to the 172.16.1.0/24 network, but HQ does not know how to get back to PC1.

Step 4

Enter this sequence of commands on the Branch router:

```
Branch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#router eigrp 1
Branch(config-router)#network 10.1.1.0 0.0.0.255
Branch(config-router)#network 10.1.10.0 0.0.0.255
Branch(config-router)#network 10.1.20.0 0.0.0.255
```

Step 6

Enter this command on the Branch router:

```
Branch#copy running-config startup-config
```

Lab 3-3: Implementing EIGRP for IPv6

Task 1: Enable IPv6 on the Interfaces
**Step 1**

Enter this command on the Branch router:

```
Branch(config)#ipv6 unicast-routing
```

**Step 2**

Enter these commands on the Branch router:

```
Branch(config)#interface Serial0/0/0
Branch(config-if)#ipv6 address 2001:db8:C0A8:100::1/64
Branch(config-if)#exit
Branch(config)#interface GigabitEthernet0/0.1
Branch(config-subif)#ipv6 address 2001:db8:0a01:100::1/64
Branch(config-subif)#exit
Branch(config)#interface GigabitEthernet0/0.10
Branch(config-subif)#ipv6 address 2001:db8:0a01:a00::1/64
Branch(config-subif)#exit
Branch(config)#interface GigabitEthernet0/0.20
Branch(config-subif)#ipv6 address 2001:db8:0a01:1400::1/64
```

**Task 2: Enable IPv6 EIGRP**

**Step 1**

Enter these commands on the Branch router:

```
Branch(config)#ipv6 router eigrp 1
Branch(config-rtr)#no shutdown
```

EIGRP for IPv6 has a shutdown feature. The routing process should be in **no shutdown** mode in order to start running.

**Step 2**

Enter these commands on the Branch router:

```
Branch(config)#interface Serial0/0/0
Branch(config-if)#ipv6 eigrp 1
Branch(config-if)#exit
Branch(config)#interface GigabitEthernet0/0.1
Branch(config-subif)#ipv6 eigrp 1
Branch(config-subif)#exit
Branch(config)#interface GigabitEthernet0/0.10
Branch(config-subif)#ipv6 eigrp 1
Branch(config-subif)#exit
Branch(config)#interface GigabitEthernet0/0.20
Branch(config-subif)#ipv6 eigrp 1
```
Lab 4-1: Configuring Multiarea OSPF

Task 1: Configure Multiarea OSPF

Step 2
Enter the following commands on the Branch router:

```
Branch# configure terminal
Branch(config)# no router eigrp 1
```

Step 3
Enter the following commands on the Branch router:

```
Branch(config)# interface Loopback10
Branch(config-if)# ip address 10.100.100.100 255.255.255.255
```

Step 4
Enter the following command on the Branch router:

```
Branch(config)# router ospf 1
```

Step 5
Enter the following command on the Branch router:

```
Branch(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Step 6
Enter the following commands on the Branch router:

```
Branch(config-router)# network 10.1.1.0 0.0.0.255 area 1
Branch(config-router)# network 10.1.10.0 0.0.0.255 area 1
Branch(config-router)# network 10.1.20.0 0.0.0.255 area 1
Branch(config-router)# network 10.100.100.100 0.0.0.0 area 1
```

Task 2: Verify Multiarea OSPF
**Step 3**
The network is seen as an intra-area route. The Branch router is an ABR, which means that routes from Area 0 and Area 1 are all seen as intra-area routes.

**Step 5**
The LAN networks are seen as interarea routes. The Headquarters router is the backbone router in Area 0, while the LAN networks came from Area 1.

**Step 8**
Enter this command on the Branch router:

```
Branch# copy run start
```

**Lab 4-2: Troubleshooting Multiarea OSPF**

**Task 1: Troubleshoot OSPF Neighbor Issues**

**Step 5**
The Serial0/0/0 interface is enabled on the router.

**Step 6**
OSPF is enabled for Area 0 on the Serial0/0/0 interface.

**Step 7**
The Serial0/0/0 interface is configured as a passive interface. Adjacencies are not established over passive interfaces because hello packets are not sent over passive interfaces.

**Step 8**
Enter these commands on the Branch router:

```
Branch# configure terminal
Branch(config)# router ospf 1
Branch(config-router)# no passive-interface Serial0/0/0
```


**Step 13**

Enter these commands on the Headquarters router:

```
Branch# telnet 192.168.1.2
Trying 192.168.1.2 ... Open
HQ# configure terminal
HQ(config)# router ospf 1
HQ(config-router)# no network 192.168.1.0 0.0.0.255 area 1
HQ(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

**Task 2: Troubleshoot OSPF Routing Table Issues**

**Step 2**

The Headquarters router incorrectly advertises the 172.16.1.0/24 network. The router is configured to advertise the 172.16.2.0/24 network, which is not connected to the Headquarters router.

**Step 3**

Enter these commands on the Headquarters router:

```
HQ# configure terminal
HQ(config)# router ospf 1
HQ(config-router)# no network 172.16.2.0 0.0.0.255 area 0
HQ(config-router)# network 172.16.1.0 0.0.0.255 area 0
```

**Step 4**

Enter this sequence of commands:

```
HQ# copy running-config startup-config
HQ# exit
[Connection to 192.168.1.2 closed by foreign host]
Branch# copy running-config startup-config
```

**Lab 4-3: Configuring OSPF for IPv6**

**Task 1: Enable OSPFv3**

**Step 1**

Enter these commands on the Branch router:
Step 2

Enter these commands on the Branch router:

```
Branch(config)# ipv6 router ospf 1
Branch(config-rtr)# router-id 2.2.2.2.
```

Step 4

Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# ipv6 ospf 1 area 0
Branch(config-if)# exit
Branch(config)# interface GigabitEthernet0/0.1
Branch(config-subif)# ipv6 ospf 1 area 1
Branch(config-subif)# exit
Branch(config)# interface GigabitEthernet0/0.10
Branch(config-subif)# ipv6 ospf 1 area 1
Branch(config-subif)# exit
Branch(config)# interface GigabitEthernet0/0.20
Branch(config-subif)# ipv6 ospf 1 area 1
Branch(config-subif)# exit
```

Step 5

Enter this command on the Branch router:

```
Branch# copy run start
```

Lab 5-1: Configuring and Troubleshooting a Serial Connection

Task 1: Troubleshoot PPP

Step 5

Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# ppp authentication chap
```
Step 6
Enter this command on the Branch router:

```
Branch# debug ppp authentication
```

Step 9
On the Branch router, configure this command:

```
Branch(config)# username HQ password cisco
```

Task 2: Enable HDLC Encapsulation

Step 2
Enter these commands on the Headquarters router:

```
HQ# configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
   HQ(config)# interface Serial 0/0/0
   HQ(config-if)# encapsulation hdlc
```

Step 4
Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
   Branch(config-if)# encapsulation hdlc
```

Step 5
Enter this sequence of commands:

```
Branch# copy running-config startup-config
   Destination filename [startup-config]? 
   Building configuration...
   [OK]
   Branch# telnet 192.168.1.2
   Trying 192.168.1.2 ... Open
   HQ# copy running-config startup-config
   Destination filename [startup-config]? 
   Building configuration...
   [OK]
```
Lab 5-2: Establishing a Frame Relay WAN

Task 1: Configure and Verify Basic Frame Relay

Step 2
Enter these commands on the Branch router:

```
Branch# configure terminal
Branch(config)# interface GigabitEthernet 0/1
Branch(config-if)# no shutdown
```

Step 6
Enter the following commands on the Branch router:

```
Branch# configure terminal
Branch(config)# interface Serial0/0/0
Branch(config-if)# encapsulation frame-relay
```

Step 3
The local DLCI number is 120.

Step 4
DLCI: 120, IP address: 192.168.1.2

Task 2: Configure and Verify Frame Relay Subinterfaces

Step 2
Enter the following commands on the Branch router:

```
Branch# configure terminal
Branch(config)# interface Serial0/0/0
Branch(config-if)# no ip address
```

Step 3
Enter the following commands on the Branch router:

```
Branch(config)# interface Serial0/0/0.120 point-to-point
Branch(config-subif)# ip address 192.168.1.1 255.255.255.0
```
**Step 4**

On point-to-point subinterfaces, it is always assumed that the end point of the point-to-point connection automatically resides on the same subnet as the start point.

**Step 5**

Enter the following commands on the Branch router:

```
Branch(config)# interface Serial0/0/0.120 point-to-point
Branch(config-subif)# frame-relay interface-dlci 120
```

**Task 3: Remove Frame Relay Configuration**

**Step 2**

Enter the following commands on the Branch router:

```
Branch# configure terminal
Branch(config)# no interface Serial0/0/0.120
```

**Step 3**

Enter the following commands on the Branch router:

```
Branch(config)# interface Serial0/0/0
Branch(config-if)# encapsulation hdlc
```

**Step 4**

Enter the following command on the Branch router:

```
Branch(config-if)# ip address 192.168.1.1 255.255.255.0
```

**Step 6**

Enter the following commands on the Headquarters router:

```
HQ(config)# interface Serial0/0/0
HQ(config-if)# encapsulation hdlc
```
Step 7

Enter these commands:

```
HQ# copy running-config startup-config
HQ# exit
[Connection to 209.165.201.2 closed by foreign host]
Branch# copy running-config startup-config
```

Lab 5-3: Establishing a GRE Tunnel

Task 1: Configure and Verify a GRE Tunnel

Step 1

Enter these commands on the Branch router:

```
Branch(config)# interface Tunnel0
Branch(config-if)# tunnel source 209.165.201.1
Branch(config-if)# tunnel destination 209.165.201.2
Branch(config-if)# ip address 192.168.2.1 255.255.255.0
```

Step 2

Enter these commands:

```
Branch# telnet 172.16.1.100
Trying 172.16.1.100 ... Open
HQ# configure terminal
HQ(config)# interface Tunnel0
HQ(config-if)# no shutdown
```

Task 2: Configure and Verify OSPF over a GRE Tunnel

Step 1

Enter these commands on the Branch router:

```
Branch(config)# router ospf 1
Branch(config-router)# network 192.168.2.0 0.0.0.255 area 0
Branch(config-router)# no passive-interface Tunnel 0
```

Step 4

Enter these commands on the Branch router:
**Step 8**

Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# shutdown
```
Task 2: Configure Router for Syslog

Step 1
Enter this command on the Branch router:

```
Branch(config)# logging 10.1.10.100
```

Step 2
Enter this command on the Branch router:

```
Branch(config)# logging trap debugging
```

Step 4
Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# shutdown
```

Step 5
Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# no shutdown
```

Lab 6-2: Analyzing NetFlow Data

Task 1: Analyze NetFlow Data

Step 1
HTTP is responsible for generating the most traffic in your network.

Step 2
The most bandwidth-consuming conversation is the one between user "hmorisondev" and "rapidshare.com."

Step 3
User "hmorisondev" is the receiver that consumes the most bandwidth.
**Step 4**

Web site "rapidshare.com" is the transmitter that consumes the most bandwidth.

**Step 5**

IP group "External" is responsible for the most traffic on your network.

**Lab 6-3: Managing Cisco Devices and Licensing**

**Task 2: Router Password Recovery**

**Step 2**

Power-cycle the Branch router.

When the router starts booting, send a break sequence to the console to interrupt the boot procedure.

```
Branch>
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC enabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Change the configuration register to the value 0x2142 and reset the router.

```
rommon 1 > confreg 0x2142
You must reset or power cycle for new config to take effect
rommon 2 > reset
```

Observe the Branch router console output. The router will start booting. Cancel the initial configuration dialog.
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC enabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x5d433c0
Self decompressing the image : #################################################
########################################################################
########################################################################
########################################################################
########################################################################
########################################################################
########################################################################
########################################################################
########################################################################
[OK]

Smart Init is enabled
smart init is sizing iomem

<table>
<thead>
<tr>
<th>TYPE</th>
<th>MEMORY_REQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>HWIC Slot 0</td>
<td>0x00200000</td>
</tr>
<tr>
<td>Onboard devices &amp; buffer pools</td>
<td>0x0228F000</td>
</tr>
</tbody>
</table>

---

TOTAL: 0x0248F000
Rounded IOMEM up to: 40Mb.
Using 7 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco CISCO2901/K9 (revision 1.0) with 483328K/40960K bytes of memory.
Processor board ID FCZ1642C5XG
2 Gigabit Ethernet interfaces
1 Serial(sync/async) interface
Enter privileged mode and copy the startup configuration into the running configuration.

Router> enable
Router# copy startup-config running-config
Destination filename [running-config]? <Enter>
1174 bytes copied in 0.116 secs (10121 bytes/sec)
Branch#

On the Branch router, set the enable secret password to "cisco" and save the running configuration into the startup configuration.

Branch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)# enable secret cisco
Branch(config)# end
Branch#

On the Branch router, change the configuration register back to the value 0x2102.

Branch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)# config-register 0x2102
Branch(config)#

Step 3

Enter these commands on the Branch router:

Branch(config)# interface Serial0/0/0
Branch(config-if)# no shutdown
Branch(config-if)# exit
Branch(config)# interface GigabitEthernet0/0.1
Branch(config-subif)# no shutdown
Branch(config-subif)# exit
Branch(config-subif)# interface GigabitEthernet0/0.10
Branch(config-subif)# no shutdown
Branch(config-subif)# exit
Branch(config-subif)# interface GigabitEthernet0/0.20
Branch(config-subif)# no shutdown
Task 3: Backing up an IOS Image

Step 1

Enter these commands on the Branch router:

```
Branch# show flash0:
-#- --length-- -----date/time------ path
1     97794040 Nov 16 2012 19:14:08 +00:00 c2900-universalk9-mz.SPA.152-4.M1.bin
2      2814 Nov 16 2012 19:14:20 +00:00 cpconfig-29xx.cfg
3    1551184 Nov 16 2012 19:14:28 +00:00 securedesktop-ios-3.1.1.45-k9.pkg
4    122880 Nov 16 2012 19:14:34 +00:00 home.tar
5    415956 Nov 16 2012 19:14:40 +00:00 sslclient-win-1.1.4.176.pkg
6    300320 Nov 16 2012 19:14:48 +00:00 cpexpress.tar
7    1038 Nov 16 2012 19:14:56 +00:00 home.shtml
8     290 Nov 23 2012 10:24:04 +00:00 TSHOOT_Troubleshoot_ACLs_Branch.cfg
153583616 bytes available (102903808 bytes used)
```

Step 4

Enter these commands on the Branch router:

```
Branch# copy flash0: tftp:
Source filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
Address or name of remote host []? 10.1.10.100
Destination filename [c2900-universalk9-mz.SPA.152-4.M1.bin]?<Enter>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
97794040 bytes copied in 374.688 secs (261001 bytes/sec)
```

Task 4: Manage a Configuration File

Step 1

Enter these commands on the Branch router:

```
Branch# copy running-config tftp:
Address or name of remote host []? 10.1.10.100
Destination filename [branch-config]?<Enter>
!!
2049 bytes copied in 0.384 secs (5336 bytes/sec)
```

Step 3

Enter these commands on the Branch router:
Branch# copy tftp: running-config
Address or name of remote host []? 10.1.10.100
Source filename []? branch-config
Destination filename [running-config]?><Enter>
Accessing tftp://10.1.10.100/branch-config...
Loading branch-config from 10.1.10.100 (via GigabitEthernet0/0.10): !
[OK - 2216 bytes]
2216 bytes copied in 0.268 secs (8269 bytes/sec)

Configuration that is being copied from the TFTP server will not overwrite the running configuration. A merge of the two configuration files will occur.

**Step 5**

Enter these commands on the Branch router:

```
Branch-changedconfiguration# configure terminal
Branch-changedconfig(config)# hostname Branch
Branch(config)#
```

**Step 6**

Enter this command on the Branch router:

```
Branch# copy running-config startup-config
```

**Task 5: Verify Licensing**

**Step 1**

Enter these commands on the Branch router:
Branch#  show license
Index 1 Feature: ipbasek9
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 2 Feature: securityk9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 3 Feature: uck9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 4 Feature: datak9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 5 Feature: gatekeeper
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
<output omitted>

Only the IP Base technology package is activated, which is by default. This is a permanent license.

**Lab S-2: ICND2 Superlab**

**Task 1: Secure Router and Configure Inter-VLAN Routing**

**Step 1**

Enter this command on the Branch router:

```
Branch(config)# enable secret cisco
```

**Step 2**

Enter the following commands on the Branch router:
Step 3

Enter the following commands on the Branch router:

Branch(config)# line con 0
Branch(config-line)# password cisco
Branch(config-line)# login
Branch(config-line)# logging synchronous

Step 4

Enter the following commands on the Branch router:

Branch(config)# line vty 0 ?
<1-1114> Last Line number
<cr>
Branch(config)# line vty 0 1114
Branch(config-line)# password cisco
Branch(config-line)# login

Step 5

Enter the following commands on the Branch router:

Branch(config)# interface GigabitEthernet0/0
Branch(config-if)# no shutdown
Branch(config)#
Branch(config-if)# interface GigabitEthernet0/0.1
Branch(config-subif)# encapsulation dot1Q 1 native
Branch(config-subif)# ip address 10.1.1.1 255.255.255.0
Branch(config-subif)#
Branch(config)#
Branch(config-subif)# interface GigabitEthernet0/0.10
Branch(config-subif)# encapsulation dot1Q 10
Branch(config-subif)# ip address 10.1.10.1 255.255.255.0
Branch(config-subif)#
Branch(config)#
Branch(config-subif)# interface GigabitEthernet0/0.20
Branch(config-subif)# encapsulation dot1Q 20
Branch(config-subif)# ip address 10.1.20.1 255.255.255.0

Task 2: Configure Basic Settings, VLANs, and Trunks on Switch
**Step 1**

Enter the following commands on the SW1 switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
```

**Step 2**

Enter the following commands on the SW1 switch:

```
SW1(config)# interface vlan 1
SW1(config-if)# ip address 10.1.1.11 255.255.255.0
SW1(config-if)# no shutdown
```

**Step 3**

Enter the following command on the SW1 switch:

```
SW1(config)# enable secret cisco
```

**Step 4**

Enter the following commands on the SW1 switch:

```
SW1(config)# line con 0
SW1(config-line)# password cisco
SW1(config-line)# login
```

**Step 5**

Enter the following commands on the SW1 switch:

```
SW1(config)# vlan 10
SW1(config-vlan)# vlan 20
SW1(config-vlan)# exit
```

**Step 6**

Enter the following commands on the SW1 switch:

```
SW1(config)# interface range FastEthernet 0/3 - 4
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# switchport trunk allowed vlan 1,10,20
```
**Step 7**

Enter the following commands on the SW1 switch:

```plaintext
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
```

**Step 9**

Enter the following commands on the SW1 switch:

```plaintext
SW1# configure terminal
SW1(config)# interface FastEthernet0/13
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 1,10,20
```

**Task 3: Troubleshoot EtherChannel**

**Step 4**

Enter the following commands on the SW1 switch:

```plaintext
SW1(config)# interface range FastEthernet0/3 - 4
SW1(config-if-range)# no channel-group 1 mode auto
SW1(config-if-range)# channel-group 1 mode active
```

**Task 4: Port Security (Trouble Ticket)**

**Step 4**

Enter the following commands on the SW2 switch:

```plaintext
SW2# configure terminal
SW2(config)# interface FastEthernet0/1
SW2(config-if)# no switchport port-security
SW2(config-if)# no switchport port-security mac-address 000c.abcd.abcd
SW2(config-if)# switchport port-security violation protect
SW2(config-if)# switchport port-security mac-address <PC2-MAC>
SW2(config-if)# switchport port-security
SW2(config-if)# shutdown
SW2(config-if)# no shutdown
```

By default, the maximum number of MAC addresses that are allowed on a port is set to 1, so there is no need to use the `switchport port-security maximum 1` command.
Task 5: Enable SSH Access on the Branch Router

Step 1

Enter the following commands on the Branch router:

```bash
Branch(config)# ip domain-name cisco.com
Branch(config)# crypto key generate rsa modulus 1024
The name for the keys will be: Branch.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Branch(config)# ip ssh version 2
Branch(config)# line vty 0 1114
Branch(config-line)# transport input ssh
```

Step 2

Enter the following commands on the Branch router:

```bash
Branch(config)# username ccna password cisco
Branch(config)# line vty 0 ?
  <1-1114>  Last Line number
  <cr>
Branch(config)# line vty 0 1114
Branch(config-line)# login local
```

Task 6: Configure DHCP Server

Step 1

Enter the following commands on the Branch router:

```bash
Branch(config)# ip dhcp excluded-address 10.1.10.1 10.1.10.199
Branch(config)# ip dhcp excluded-address 10.1.10.201 10.1.10.254
Branch(config)# ip dhcp pool VLAN10
Branch(dhcp-config)# network 10.1.10.0 255.255.255.0
Branch(dhcp-config)# default-router 10.1.10.1
Branch(dhcp-config)# lease 0 0 3
```

Step 2

On PC1, open the lab Ethernet adapter properties, find the TCP/IPv4 item, and click the Properties button:
Change the IPv4 setting on the lab Ethernet adapter to acquire the IP setting dynamically.
Task 7: Stateless Autoconfiguration on the PC

**Step 1**

Enter this command on the Branch router:

```
Branch(config)# ipv6 unicast-routing
```

**Step 2**

Enter these commands on the Branch router:

```
Branch(config)# interface GigabitEthernet 0/0.1
Branch(config-subif)# ipv6 address 2001:DB8:0A01:100::1/64
Branch(config-subif)# interface GigabitEthernet 0/0.10
Branch(config-subif)# ipv6 address 2001:DB8:0A01:A00::1/64
Branch(config-subif)# interface GigabitEthernet 0/0.20
Branch(config-subif)# ipv6 address 2001:DB8:0A01:1400::1/64
Branch(config-subif)# interface GigabitEthernet 0/1
Branch(config-subif)# ipv6 address 2001:DB8:D1A5:C900::1/64
Branch(config-if)# interface Serial0/0/0
Branch(config-if)# ipv6 address 2001:DB8:C0A8:100::1/64
```
Task 8: Configure PPP Encapsulation

Step 1
Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# no shutdown
```

Step 4
Enter these commands on the Branch router:

```
Branch(config)# interface Serial 0/0/0
Branch(config-if)# encapsulation ppp
Branch(config-if)# ip address 192.168.1.1 255.255.255.0
```

Task 9: Configure Dynamic Routing Protocol

Step 1
Enter the following commands on the Branch router:

```
Branch(config)# router ospf 1
Branch(config-router)# network 192.168.1.0 0.0.0.255 area 0
Branch(config-router)# network 10.1.1.0 0.0.0.255 area 0
Branch(config-router)# network 10.1.10.0 0.0.0.255 area 0
Branch(config-router)# network 10.1.20.0 0.0.0.255 area 0
```

Task 10: Configure the OSPFv3 Routing Protocol

Step 1
Enter this sequence of commands on the Branch router:

```
Branch(config)# interface Serial0/0/0
Branch(config-if)# ipv6 ospf 1 area 0
Branch(config-if)#
Branch(config)# interface GigabitEthernet0/0.1
Branch(config-subif)# ipv6 ospf 1 area 0
Branch(config-subif)#
Branch(config)# interface GigabitEthernet0/0.10
Branch(config-subif)# ipv6 ospf 1 area 0
Branch(config-subif)#
Branch(config)# interface GigabitEthernet0/0.20
Branch(config-subif)# ipv6 ospf 1 area 0
Branch(config-subif)#
```

Task 11: Troubleshoot the IP Access Control List (Trouble Ticket)
**Step 1**

From PC2, trace to IP address 172.16.1.100:

```
C:\Windows\system32> tracert -d 172.16.1.100
Tracing route to 172.16.1.100 over a maximum of 30 hops
1    1 ms  <1 ms  <1 ms  10.1.20.1
2  192.168.1.2 reports: Destination net unreachable.
Trace complete.
```

There is a "Destination Net Unreachable" report that is received from IP address 192.168.1.2 (Headquarters router). From PC2, use PuTTY to use Telnet to connect to IP address 192.168.1.2.

On the Headquarters router, verify which interface has IP address 192.168.1.2.

```
HQ# show ip interface brief | include 192.168.1.2
Serial0/0/0                192.168.1.2     YES manual up                    up
```

IP address 192.168.1.2 belongs to the Serial 0/0/0 interface. On the Headquarters router, investigate if Serial 0/0/0 has an access list that is applied to the interface.

```
HQ# show ip int Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  Peer address is 192.168.1.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10 224.0.0.5
  Outgoing access list is not set
  Inbound access list is denyPING
  Proxy ARP is enabled
  <output omitted>
```

From the output, you can see that there is an inbound ACL that is set to the Serial 0/0/0 interface. On the Headquarters router, verify the ACL configuration.

```
HQ# show ip access-lists denyPING
Extended IP access list denyPING
    10 deny icmp host 10.1.20.100 host 172.16.1.100 (9 matches)
    20 permit ip any any (373 matches)
```

There is line 10 in the ACL denyPING that prohibits pings from PC2 (10.1.20.100) to the IP address of the server (172.16.1.100). Enter the following commands on the Headquarters router:

```
HQ# configure terminal
HQ(config)# ip access-list extended denyPING
HQ(config-ext-nacl)# 5 permit icmp host 10.1.20.100 host 172.16.1.100 echo
```