Module 1 - Basic Device Configuration

Refer [Lab1.1.7.LooZiXuan.RSDG5] - [Appendix A] to initialize and Reload a Switch

1.1.6 Switch SVI Configuration Example

Step 1

Configure the Management Interface

From VLAN interface configuration mode, an IPv4 address and subnet mask is applied to the management SVI of the switch. Specifically, SVI VLAN 99 will be assigned the 172.17.99.11/24 IPv4 address and the 2001:db8:acad:99::1/64 IPv6 address as shown.

Note: The SVI for VLAN 99 will not appear as “up/up” until VLAN 99 is created and there is a device connected to a switch port associated with VLAN 99.

Note: The switch may need to be configured for IPv6. For example, before you can configure IPv6 addressing on a Cisco Catalyst 2960 running IOS version 15.0, you will need to enter the global configuration command **sdm prefer dual-ipv4-and-ipv6 default** and then **reload** the switch.

Task	IOS Commands
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode for the SVI.	`S1(config)# interface vlan 99`
Configure the management interface IPv4 address.	`S1(config-if)# ip address 172.17.99.11 255.255.255.0`
Configure the management interface IPv6 address	`S1(config-if)# ipv6 address 2001:db8:acad:99::11/64`
Enable the management interface.	`S1(config-if)# no shutdown`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Step 2

Configure the Default Gateway

The switch should be configured with a default gateway if it will be managed remotely from networks that are not directly connected.

Note: Because it will receive its default gateway information from a router advertisement (RA) message, the switch does not require an IPv6 default gateway.

Task	IOS Commands
Enter global configuration mode.	`S1# configure terminal`
Configure the default gateway for the switch.	`S1(config)# ip default-gateway 172.17.99.1`
Return to the privileged EXEC mode.	`S1(config)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Step 3

Verify Configuration

The show ip interface brief and show ipv6 interface brief commands are useful for determining the status of both physical and virtual interfaces. The output shown confirms that interface VLAN 99 has been configured with an IPv4 and IPv6 address.
Note: An IP address applied to the SVI is only for remote management access to the switch; this does not allow the switch to route Layer 3 packets.

```
S1# show ip interface brief
Interface      IP-Address      OK? Method   Status     Protocol
Vlan99         172.17.99.11    YES manual   down       down
(output omitted)
S1# show ipv6 interface brief
Vlan99                  [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::11
(output omitted)
```

1.2.2 Configure Switch Ports at the Physical Layer

Task	IOS Commands
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

The command to **enable auto-MDIX** is issued in interface configuration mode on the switch as shown:
S1(config-if)# **mdix auto**

1.2.4 Switch Verification Commands

Task	IOS Commands
Display interface status and configuration.	`S1# show interfaces [interface-id]`
Display current startup configuration.	`S1# show startup-config`
Display current running configuration.	`S1# show running-config`
Display information about the flash file system.	`S1# show flash`
Display system hardware and software status.	`S1# show version`
Display history of command entered.	`S1# show history`

Display IP information about an interface.	`S1# show ip interface [interface-id]`
	OR
	`S1# show ipv6 interface [interface-id]`

Display the MAC address table.	`S1# show mac-address-table`
	OR
	`S1# show mac address-table`

1.3.4 Configure SSH [can apply in Lab1.3.6.LooZiXuan.RSDG5]

Step 1

Verify SSH support.

Use the show ip ssh command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

```
S1# show ip ssh
```

Step 2

Configure the IP domain.

Configure the IP domain name of the network using the ip domain-name domain-name global configuration mode command. In the figure, the domain-name value is cisco.com.

```
S1(config)# ip domain-name cisco.com
```

Step 3

Generate RSA key pairs.

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the ip ssh version 2 global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the crypto key generate rsa global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in the figure uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes longer to generate and to use.

Note: To delete the RSA key pair, use the crypto key zeroize rsa global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

```
S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Step 4

Configure user authentication.

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the username username secret password global configuration mode command. In the example, the user admin is assigned the password ccna.

```
S1(config)# username admin secret ccna
```

Step 5

Configure the vty lines.

Enable the SSH protocol on the vty lines by using the transport input ssh line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the line vty global configuration mode command and then the login local line configuration mode command to require local authentication for SSH connections from the local username database.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

Step 6

Enable SSH version 2.

By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the show ip ssh output as supporting version 2. Enable SSH version using the ip ssh version 2 global configuration command.

```
S1(config)# ip ssh version 2
```

1.4.1 Basic Router Configuration

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#

R1(config)# banner motd #Authorized Access Only!#
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

1.5.1 Interface Verification Commands [can apply in Lab1.5.10.LooZiXuan.RSDG5]

- **show ip interface brief** and **show ipv6 interface brief** - These display a summary for all interfaces including the IPv4 or IPv6 address of the interface and current operational status.
- **show running-config interface interface-id** - This displays the commands applied to the specified interface.
- **show ip route** and **show ipv6 route** - These display the contents of the IPv4 or IPv6 routing table stored in RAM. In Cisco IOS 15, active interfaces should appear in the routing table with two related entries identified by the code 'C' (Connected) or 'L' (Local). In previous IOS versions, only a single entry with the code 'C' will appear.

1.5.6 Filter Show Command Output [can apply in Lab1.5.10.LooZiXuan.RSDG5]

section

Shows the entire section that starts with the filtering expression, as shown in the example.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 110A1016141D
 login
 transport input all
```

include

Includes all output lines that match the filtering expression, as shown in the example.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up
up
GigabitEthernet0/0/1   192.168.11.1    YES manual up
up
Serial0/1/0            209.165.200.225 YES manual up
up
Serial0/1/1            unassigned      NO  unset  down
down
R1#
```

```
R1# show ip interface brief | include up
GigabitEthernet0/0/0   192.168.10.1    YES manual up
up
GigabitEthernet0/0/1   192.168.11.1    YES manual up
up
Serial0/1/0            209.165.200.225 YES manual up
up
```

exclude

Excludes all output lines that match the filtering expression, as shown in the example.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up
up
GigabitEthernet0/0/1   192.168.11.1    YES manual up
up
Serial0/1/0            209.165.200.225 YES manual up
up
Serial0/1/1            unassigned      NO  unset  down
down
R1#
R1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up
up
GigabitEthernet0/0/1   192.168.11.1    YES manual up
up
Serial0/1/0            209.165.200.225 YES manual up
up
```

begin

Shows all the output lines from a certain point, starting with the line that matches the filtering expression, as shown in the example.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
```

```
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0
```

1.5.8 Command History Feature

```
R1# terminal history size 200
R1# show history
  show ip int brief
  show interface g0/0/0
  show ip route
  show running-config
  show history
  terminal history size 200
```

Module 3 - VLANs

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ----------------- -------  --------------------
1    default             active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, 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
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

3.3.2 VLAN Creation Commands

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Create a VLAN with a valid ID number.	`Switch(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`Switch(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`Switch(config-vlan)# end`

3.3.4 VLAN Port Assignment Commands

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Enter interface configuration mode.	`Switch(config)# interface interface-id`
Set the port to access mode.	`Switch(config-if)# switchport mode access`
Assign the port to a VLAN.	`Switch(config-if)# switchport access vlan vlan-id`

Return to the privileged EXEC mode.	`Switch(config-if)# end`

3.3.7 Voice VLAN

Use the **switchport voice vlan vlan-id** interface configuration command to assign a voice VLAN to a port.

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
S3#
```

3.3.8 Verify VLAN information

Task	Command Option
Display VLAN name, status, and its ports one VLAN per line.	**brief**
Display information about the identified VLAN ID number. For vlan-id, the range is 1 to 4094.	**id vlan-id**
Display information about the identified VLAN name. The vlan-name is an ASCII string from 1 to 32 characters.	**name vlan-name**
Display VLAN summary information.	**summary**

3.3.9 Change VLAN Port Membership

If the switch access port has been incorrectly assigned to a VLAN, then simply re-enter the **switchport access vlan vlan-id** interface configuration command with the correct VLAN ID. For instance, assume Fa0/18 was incorrectly configured to be on the default VLAN 1 instead of VLAN 20. To change the port to VLAN 20, simply enter **switchport access vlan 20**.

To change the membership of a port back to the default VLAN 1, use the **no switchport access vlan** interface configuration mode command as shown.

In the output for example, Fa0/18 is configured to be on the default VLAN 1 as confirmed by the show vlan brief command.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
VLAN Name                 Status    Ports
---- ------------------ --------- -------------------------------
1    default            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, 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   student            active
1002 fddi-default       act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default    act/unsup
1005 trnet-default      act/unsup
```

3.3.10 Delete VLANs

The **no vlan vlan-id** global configuration mode command is used to remove a VLAN from the switch vlan.dat file.

Caution: Before deleting a VLAN, reassign all member ports to a different VLAN first. Any ports that are not moved to an active VLAN are unable to communicate with other hosts after the VLAN is deleted and until they are assigned to an active VLAN.

3.4.1 Trunk Configuration Commands

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Enter interface configuration mode.	`Switch(config)# interface interface-id`

Set the port to permanent trunking mode.	`Switch(config-if)# switchport mode trunk`
Sets the native VLAN to something other than VLAN 1.	`Switch(config-if)# switchport trunk native vlan vlan-id`
Specify the list of VLANs to be allowed on the trunk link.	`Switch(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`Switch(config-if)# end`

3.4.3 Verify Trunk Configuration

The switch output displays the configuration of switch port F0/1 on switch S1. The configuration is verified with the **show interfaces interface-ID switchport** command.

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
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: 99 (VLAN0099)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30,99
Pruning VLANs Enabled: 2-1001
(output omitted)
```

3.4.4 Reset the trunk to the default state

Use the **no switchport trunk allowed vlan** and the **no switchport trunk native vlan** commands to remove the allowed VLANs and reset the native VLAN of the trunk. When it is reset to the default state, the trunk allows all VLANs and uses VLAN 1 as the native VLAN. The example shows the commands used to reset all trunking characteristics of a trunking interface to the default settings.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

The **show interfaces f0/1 switchport** command reveals that the trunk has been reconfigured to a default state.

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
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
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

This sample output shows the commands used to remove the trunk feature from the F0/1 switch port on switch S1. The **show interfaces f0/1 switchport** command reveals that the F0/1 interface is now in static access mode.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 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: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

3.5.1 Dynamic Trunking Protocol

The default DTP configuration for Cisco Catalyst 2960 and 3650 switches is dynamic auto.

To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk, but it will not generate DTP frames.

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

To re-enable dynamic trunking protocol use the switchport mode dynamic auto command.

```
S1(config-if)# switchport mode dynamic auto
```

If the ports connecting two switches are configured to ignore all DTP advertisements with the **switchport mode trunk** and the **switchport nonegotiate** commands, the ports will stay in trunk port mode. If the connecting ports are set to dynamic auto, they will not negotiate a trunk and will stay in the access mode state, creating an inactive trunk link.

When configuring a port to be in trunk mode, use the **switchport mode trunk** command. Then there is no ambiguity about which state the trunk is in; it is always on.

3.5.2 Negotiated Interface Modes

The **switchport mode** command has additional options for negotiating the interface mode. The full command syntax is the following:

```
Switch(config-if)# switchport mode { access | dynamic { auto | desirable } | trunk }
```

The options are described in the table.

Option	Description
access	• Puts the interface (access port) into permanent non trunking mode and negotiates to convert the link into a non trunk link. • The interface becomes a non-trunk interface, regardless of whether the neighboring interface is a trunk interface.
dynamic auto	• Makes the interface able to convert the link to a trunk link. • The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. • The default switchport mode for all Ethernet interfaces is dynamic auto.
dynamic desirable	• Makes the interface actively attempt to convert the link to a trunk link. • The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or dynamic auto mode.
trunk	• Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. • The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

Use the **switchport nonegotiate** interface configuration command to stop DTP negotiation. The switch does not engage in DTP negotiation on this interface. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

3.5.4 Verify DTP Mode

The default DTP mode is dependent on the Cisco IOS Software version and on the platform. To determine the current DTP mode, issue the **show dtp interface** command as shown in the output.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
```

```
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

Note: A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. On links where trunking is not intended, DTP should be turned off.

Module 4 - Inter-VLAN Routing

4.2 Router-on-a-stick Inter VLAN Routing [Lab - Configure Router-on-a-Stick Inter-VLAN Routing]

4.2.2 Switch VLAN and Trunking Configuration

1. Create and name the VLANs.
   First, the VLANs are created and named. VLANs are only created after you exit out of VLAN sub configuration mode.

```
S1(config)# vlan 10
S1(config-vlan)# name LAN10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name LAN20
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

2. Create the management interface.
   Next, the management interface is created on VLAN 99 along with the default gateway of R1.

```
S1(config)# interface vlan 99
S1(config-if)# ip add 192.168.99.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#
```

3. Configure access ports.
   Next, port Fa0/6 connecting to PC1 is configured as an access port in VLAN 10. Assume PC1 has been configured with the correct IP address and default gateway.

```
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

4. Configure trunking ports.
   Finally, ports Fa0/1 connecting to S2 and Fa05 connecting to R1 are configured as trunk ports.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# end
*Mar  1 00:23:43.093: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up
*Mar  1 00:23:44.511: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/5, changed state to up
```

4.2.4 Router Subinterface Configuration

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed.

A subinterface is created using the **interface interface_id.subinterface_id** global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

- **encapsulation dot1q vlan_id [native]** - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified vlan-id. The native keyword option is only appended to set the native VLAN to something other than VLAN 1.
- **ip address ip-address subnet-mask** - This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.
-

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur.

When all subinterfaces have been created, enable the physical interface using the no shutdown interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1,
changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1,
changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
R1#
```

4.2.6 Router-on-a-Stick Inter-VLAN Routing Verification

In addition to using ping between devices, the following show commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- show ip route
- show ip interface brief
- show interfaces
- show interfaces trunk

1. **show ip route**

Verify that the subinterfaces are appearing in the routing table of R1 by using the **show ip route** command. Notice that there are three connected routes (C) and their respective exit interfaces

for each routable VLAN. The output confirms that the correct subnets, VLANs, and subinterfaces are active.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected,
GigabitEthernet0/0/1.10
L        192.168.10.1/32 is directly connected,
GigabitEthernet0/0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected,
GigabitEthernet0/0/1.20
L        192.168.20.1/32 is directly connected,
GigabitEthernet0/0/1.20
      192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.99.0/24 is directly connected,
GigabitEthernet0/0/1.99
L        192.168.99.1/32 is directly connected,
GigabitEthernet0/0/1.99
R1#
```

2. **show ip interface brief**

Another useful router command is **show ip interface brief**, as shown in the output. The output confirms that the subinterfaces have the correct IPv4 address configured, and that they are operational.

```
R1# show ip interface brief | include up
GigabitEthernet0/0/1   unassigned      YES unset  up
up
Gi0/0/1.10             192.168.10.1    YES manual up
up
Gi0/0/1.20             192.168.20.1    YES manual up
up
Gi0/0/1.99             192.168.99.1    YES manual up
up
```

3. **show interfaces subinterface-id**

Subinterfaces can be verified using the **show interfaces subinterface-id** command, as shown.

```
R1# show interfaces g0/0/1.10
GigabitEthernet0/0/1.10 is up, line protocol is up
```

```
  Hardware is ISR4221-2x1GE, address is 10b3.d605.0301 (bia
10b3.d605.0301)
  Description: Default Gateway for VLAN 10
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive not supported
  Last clearing of "show interface" counters never
R1#
```

4. **show interfaces trunk**

The misconfiguration could also be on the trunking port of the switch. Therefore, it is also useful to verify the active trunk links on a Layer 2 switch by using the **show interfaces trunk** command, as shown in the output. The output confirms that the link to R1 is trunking for the required VLANs.

Note: Although VLAN 1 was not explicitly configured, it was automatically included because control traffic on trunk links will always be forwarded on VLAN 1.

```
S1# show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Fa0/5       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/5       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
S1#
```

Small Notes for this Router-on-a-Stick configuration

1. Router (only require 1 physical interface)
    a. Configure subinterfaces
    b. Configure the main interface
2. Switchport must be configured as trunk port

3. Configure end devices (i.e IP address and default gateway)

4.3 Inter-VLAN Routing using Layer 3 Switches [Packet Tracer - Configure Layer 3 Switching and Inter-VLAN Routing]

4.3.3 Layer 3 Switch Configuration

1. **Create the VLANs.**

First, create the two VLANs as shown in the output.

```
D1(config)# vlan 10
D1(config-vlan)# name LAN10
D1(config-vlan)# vlan 20
D1(config-vlan)# name LAN20
D1(config-vlan)# exit
D1(config)#
```

2. **Create the SVI VLAN interfaces.**

Configure the SVI for VLANs 10 and 20. The IP addresses that are configured will serve as the default gateways to the hosts in the respective VLANs. Notice the informational messages showing the line protocol on both SVIs changed to up.

```
D1(config)# interface vlan 10
D1(config-if)# description Default Gateway SVI for 192.168.10.0/24
D1(config-if)# ip add 192.168.10.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
D1(config)# int vlan 20
D1(config-if)# description Default Gateway SVI for 192.168.20.0/24
D1(config-if)# ip add 192.168.20.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
*Sep 17 13:52:16.053: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan10, changed state to up
*Sep 17 13:52:16.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan20, changed state to up
```

3. Configure access ports.

Next, configure the access ports connecting to the hosts and assign them to their respective VLANs.

```
D1(config)# interface GigabitEthernet1/0/6
D1(config-if)# description Access port to PC1
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 10
D1(config-if)# exit
D1(config)#
D1(config)# interface GigabitEthernet1/0/18
D1(config-if)# description Access port to PC2
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 20
D1(config-if)# exit
```

4. Enable IP routing.

Finally, enable IPv4 routing with the ip routing global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VLAN routing on a Layer 3 switch for IPv4.

```
D1(config)# ip routing
D1(config)#
```

4.3.7 Routing Configuration on a Layer 3 Switch

1. Configure the routed port.

Configure G1/0/1 to be a routed port, assign it an IPv4 address, and enable it.

```
D1(config)# interface GigabitEthernet1/0/1
D1(config-if)# description routed Port Link to R1
D1(config-if)# no switchport
D1(config-if)# ip address 10.10.10.2 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
```

2. Włącz routing.

Ensure IPv4 routing is enabled with the ip routing global configuration command.

```
D1(config)# ip routing
D1(config)#
```

3. Configure routing.

Configure the OSPF routing protocol to advertise the VLAN 10 and VLAN 20 networks, along with the network that is connected to R1. Notice the message informing you that an adjacency has been established with R1.

```
D1(config)# router ospf 10
D1(config-router)# network 192.168.10.0 0.0.0.255 area 0
D1(config-router)# network 192.168.20.0 0.0.0.255 area 0
D1(config-router)# network 10.10.10.0 0.0.0.3 area 0
D1(config-router)# ^Z
D1#
*Sep 17 13:52:51.163: %OSPF-5-ADJCHG: Process 10, Nbr 10.20.20.1 on
GigabitEthernet1/0/1 from LOADING to FULL, Loading Done
D1#
```

4. Verify routing.

Verify the routing table on D1. Notice that D1 now has a route to the 10.20.20.0/24 network.

```
D1# show ip route | begin Gateway
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        10.10.10.0/30 is directly connected, GigabitEthernet1/0/1
L        10.10.10.2/32 is directly connected, GigabitEthernet1/0/1
O        10.10.20.0/24 [110/2] via 10.10.10.1, 00:00:06,
GigabitEthernet1/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
D1#
```

5. Verify connectivity.

At this time, PC1 and PC2 are able to ping the server connected to R1.

```
C:\Users\PC1> ping 10.20.20.254
Pinging 10.20.20.254 with 32 bytes of data:
Request timed out.
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.20.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
!================================================
C:\Users\PC2> ping 10.20.20.254
Pinging 10.20.20.254 with 32 bytes of data:
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Ping statistics for 10.20.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC2>
```

4. 4 Troubleshoot Inter-VLAN Routing [Packet Tracer - Troubleshooting Inter-VLAN Routing]

4.4.1 Common Inter-VLAN Issues

Issue Type	How to Fix	How to Verify

Missing VLANs	• Create (or re-create) the VLAN if it does not exist.
	• Ensure the host port is assigned to the correct VLAN.
		`show vlan [brief]`
		`show interfaces switchport`
		`ping`

Switch Trunk Port Issues	• Ensure trunks are configured correctly. • Ensure the port is a trunk port and enabled.	`show interfaces trunk` `show running-config`

Switch Access Port Issues	• Assign the correct VLAN to the access port.
	• Ensure the port is an access port and enabled.
	• Host is incorrectly configured in the wrong subnet.
		`show interfaces switchport`
		`show running-config interface`
		`ipconfig`

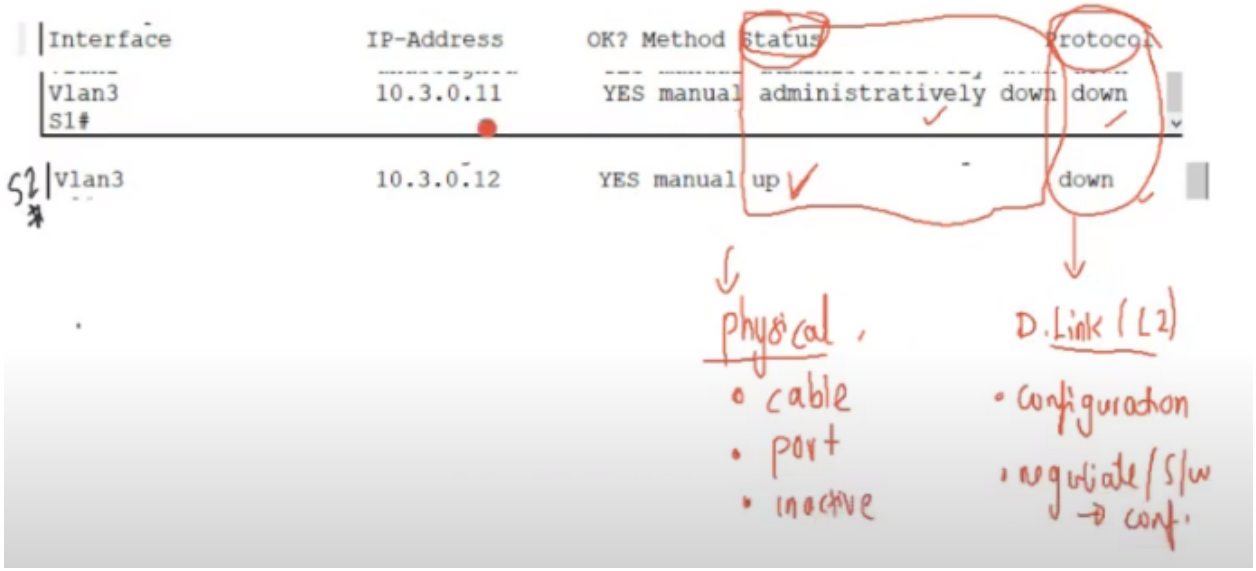
Router Configuration Issues	• Router subinterface IPv4 address is incorrectly configured. • Router subinterface is assigned to the VLAN ID.	`show ip interface brief` `show interfaces`

Packet Tracer - Troubleshooting Inter-VLAN Routing (session week 7 -- 28/2/2022)

Step 1 - Ensure L2 must work properly

- Trunk
- Same vlan must be able to ping other
    - Subnet
    - VLAN
    - Different Switches - Trunk, native vlan, allowed vlan list

Step 2 - Troubleshooting L3



Module 6 - EtherChannel

6.2.2 LACP Configuration Example [Packet Tracer - Configure EtherChannel]
Configuring EtherChannel with LACP requires the following three steps:

Step 1. Specify the interfaces that compose the EtherChannel group using the **interface range** interface global configuration mode command. The range keyword allows you to select several interfaces and configure them all together.

Step 2. Create the port channel interface with the **channel-group identifier mode active** command in interface range configuration mode. The identifier specifies a channel group number. The mode active keywords identify this as an LACP EtherChannel configuration.

Step 3. To change Layer 2 settings on the port channel interface, enter port channel interface configuration mode using the **interface port-channel** command, followed by the interface identifier. In the example, S1 is configured with an LACP EtherChannel. The port channel is configured as a trunk interface with the allowed VLANs specified.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config)# interface port-channel 1
S1(config)# switchport mode trunk
S1(config)# switchport trunk allowed vlan 1,2,20
```

6.3.1 Verify EtherChannel

As always, when you configure devices in your network, you must verify your configuration. If there are problems, you will also need to be able to troubleshoot and fix them. This topic gives you the commands to verify, as well as some common EtherChannel network problems and their solutions.

The verification command examples will use the topology shown in the figure.

1. show interfaces port-channel

The **show interfaces port-channel** command displays the general status of the port channel interface. In the figure, the Port Channel 1 interface is up.

```
S1# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
```

```
  Hardware is EtherChannel, address is c07b.bcc4.a981 (bia
c07b.bcc4.a981)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
(output omitted)
```

2. show etherchannel summary

When several port channel interfaces are configured on the same device, use the **show etherchannel summary c**ommand to display one line of information per port channel. In the output, the switch has one EtherChannel configured; group 1 uses LACP.

The interface bundle consists of the FastEthernet0/1 and FastEthernet0/2 interfaces. The group is a Layer 2 EtherChannel and it is in use, as indicated by the letters SU next to the port channel number.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not
met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
-----------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)
```

3. show etherchannel port-channel

Use the **show etherchannel port-channel** command to display information about a specific port channel interface, as shown in the output. In the example, the Port Channel 1 interface consists of two physical interfaces, FastEthernet0/1 and FastEthernet0/2. It uses LACP in active mode. It is properly connected to another switch with a compatible configuration, which is why the port channel is said to be in use.

```
S1# 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:01h:02m:10s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Load share deferral = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0
Time since last port bundled:    0d:00h:09m:30s    Fa0/2
```

4. show interfaces etherchannel

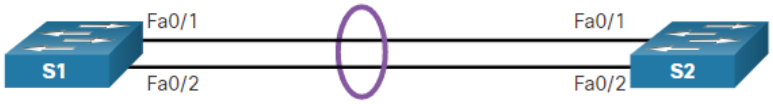
On any physical interface member of an EtherChannel bundle, the **show interfaces etherchannel** command can provide information about the role of the interface in the EtherChannel, as shown in the output. The interface FastEthernet0/1 is part of the EtherChannel bundle 1. The protocol for this EtherChannel is LACP.

```
S1# show interfaces f0/1 etherchannel
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:
                           LACP port     Admin     Oper    Port
Port      Flags   State     Priority      Key       Number  State
Fa0/1     SA      bndl      32768         0x1       0x1     0x102       0x3D
Partner's information:
                 LACP port                        Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age    key    Key    Number  State
```

```
Fa0/1      SA       32768      c025.5cd7.ef00  12s     0x0     0x1     0x102    0x3Dof
the port in the current state: 0d:00h:11m:51sllowed vlan 1,2,20
```

6.3.3 Troubleshoot EtherChannel Example [Packet Tracer - Troubleshooting EtherChannel] In the figure, interfaces F0/1 and F0/2 on switches S1 and S2 are connected with an EtherChannel. However, the EtherChannel is not operational.

two switches, S1 and S2, are connected together via two physical network connections that have formed an EtherChannel; port F0/1 on S1 is connected to port F0/1 on S2; port F0/2 on S1 is connected to port F0/2 on S2



Step 1. View the EtherChannel Summary Information | Step 2. View Port Channel Configuration | Step 3: Correct the Misconfiguration | Step 4. Verify EtherChannel is Operational

Step 1. View the EtherChannel Summary Information

The output of the **show etherchannel summary** command indicates that the EtherChannel is down.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)         -      Fa0/1(D)    Fa0/2(D)
```

Step 2. View Port Channel Configuration

In the **show run | begin interface port-channel** output, more detailed output indicates that there are incompatible PAgP modes configured on S1 and S2.

```
S1# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!====================================
S2# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
```

Step 3: Correct the Misconfiguration

To correct the issue, the PAgP mode on the EtherChannel is changed to desirable.

Note: EtherChannel and STP must interoperate. For this reason, the order in which EtherChannel-related commands are entered is important, which is why you see interface Port-Channel 1 removed and then re-added with the **channel-group** command, as opposed to directly changed. If one tries to change the configuration directly, STP errors cause the associated ports to go into blocking or errdisabled state.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```


Step 4. Verify EtherChannel is Operational

The EtherChannel is now active as verified by the output of the **show etherchannel summary** command.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/1(P)    Fa0/2(P)
```

Module 6 FHRP Concepts

Lab 9.3.3 HSRP Configuration Guide

Configure HSRP on R1.

a. Configure HSRP on the G0/1 LAN interface of R1.
   Open configuration window
   ```
   R1(config)# interface g0/1
   ```

b. Specify the HSRP protocol version number. The most recent version is version 2.
   Note: Standby version 1 only supports IPv4 addressing.
   ```
   R1(config-if)# standby version 2
   ```

c. Configure the IP address of the virtual default gateway. This address must be configured on any hosts that require the services of the default gateway. It replaces the physical interface address of the router that has been previously configured on the hosts. Multiple instances of HSRP can be configured on a router. You must specify the HSRP group number to identify the virtual interface between routers in a HSRP group. This number must be consistent between the routers in the group. The group number for this configuration is 1.
   ```
   R1(config-if)# standby 1 ip 192.168.1.254
   ```

d. Designate the active router for the HSRP group. It is the router that will be used as the gateway device unless it fails or the path to it becomes inactive or unusable. Specify the priority for the router interface. The default value is 100. A higher value will determine which router is the active router. If the priorities of the routers in the HSRP group are the same, then the router with the highest configured IP address will become the active router.
   ```
   R1(config-if)# standby 1 priority 150
   ```
   R1 will operate as the active router and traffic from the two LANs will use it as the default gateway.

e. If it is desirable that the active router resume that role when it becomes available again, configure it to preempt the service of the standby router. The active router will take over the gateway role when it becomes operable again.
   ```
   R1(config-if)# standby 1 preempt
   ```
   Question:
   What will the HSRP priority of R3 be when it is added to HSRP group 1?
   The default priority value which is 100

Configure HSRP

```
R3(config)#int g0/0
R3(config-if)#standby version 2
R3(config-if)#standby 1 ip 192.168.1.254
```

Verify HSRP Configuration

Verify HSRP by issuing the **show standby** .Verify the values for HSRP role, group, virtual IP address of the gateway, preemption, and priority. Note that HSRP also identifies the active and standby router IP addresses for the group.

Module 10 LAN Security Concepts

Authentication with a Local Password

SSH and local database methods of remote access.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Module 11 Switch Security Configuration

11.1.3 Enable Port Security

Notice in the example, the switchport port-security command was rejected. This is because port security can only be configured on manually configured access ports or manually configured trunk ports. By default, Layer 2 switch ports are set to dynamic auto (trunking on). Therefore, in the example, the port is configured with the switchport mode access interface configuration command.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Use the show port-security interface command to display the current port security settings for FastEthernet 0/1, as shown in the example. Notice how port security is enabled, port status is Secure-down which means there are no devices attached and no violation has occurred, the

violation mode is Shutdown, and how the maximum number of MAC addresses is 1. If a device is connected to the port, the switch port status would display Secure-up and the switch will automatically add the device's MAC address as a secure MAC. In this example, no device is connected to the port.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Note: If an active port is configured with the **switchport port-security** command and more than one device is connected to that port, the port will transition to the error-disabled state. This condition is discussed later in this topic.

After port security is enabled, other port security specifics can be configured, as shown in the example.

```
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
S1(config-if)# switchport port-security
```

11.1.4 Limit and Learn MAC Addresses

To set the maximum number of MAC addresses allowed on a port, use the following command:

```
Switch(config-if)# switchport port-security maximum value
```

The default port security value is 1. The maximum number of secure MAC addresses that can be configured depends on the switch and the IOS. In this example, the maximum is 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

The switch can be configured to learn about MAC addresses on a secure port in one of three ways:

1. Manually Configured
   The administrator manually configures a static MAC address(es) by using the following command for each secure MAC address on the port:
   `Switch(config-if)# switchport port-security mac-address mac-address`
2. Dynamically Learned
   When the switchport port-security command is entered, the current source MAC for the device connected to the port is automatically secured but is not added to the startup configuration. If the switch is rebooted, the port will have to re-learn the device's MAC address.

3. Dynamically Learned – Sticky
   The administrator can enable the switch to dynamically learn the MAC address and "stick" them to the running configuration by using the following command:
   `Switch(config-if)# switchport port-security mac-address sticky`
   Saving the running configuration will commit the dynamically learned MAC address to NVRAM.

The following example demonstrates a complete port security configuration for FastEthernet 0/1 with a host connected to port Fa0/1. The administrator specifies a maximum of 2 MAC addresses, manually configures one secure MAC address, and then configures the port to dynamically learn additional secure MAC addresses up to the 2 secure MAC address maximum. Use the **show port-security interface** and the **show port-security address** command to verify the configuration.

```
*Mar  1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
1    a41f.7272.676a    SecureSticky                  Fa0/1       -
1    aaaa.bbbb.1234    SecureConfigured              Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max  Addresses limit in System (excluding one mac per port) : 8192
S1#
```

11.1.5 Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port. Two types of aging are supported per port:

- **Absolute** - The secure addresses on the port are deleted after the specified aging time.
- **Inactivity** - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Aging time limits can also be increased to ensure past secure MAC addresses remain, even while new MAC addresses are added. Aging of statically configured secure addresses can be enabled or disabled on a per-port basis.

Use the **switchport port-security aging** command to enable or disable static aging for the secure port, or to set the aging time or type.

```
Switch(config-if)# switchport port-security aging { static | time
time | type {absolute | inactivity}}
```

The parameters for the command are described in the table.

Parameter	Description
static	Enable aging for statically configured secure addresses on this port.
time time	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Note: MAC addresses are shown as 24 bits for simplicity.

The example shows an administrator configuring the aging type to 10 minutes of inactivity and by using the show port-security interface command to verify the configuration.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

Port Security Violation Modes

If the MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs. By default, the port enters the error-disabled state.

To set the port security violation mode, use the following command:

```
Switch(config-if)# switchport port-security violation { protect | restrict | shutdown}
```

The following example shows an administrator changing the security violation to “restrict”. The output of the **show port-security interface** command confirms that the change has been made.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

11.1.7 Ports in error-disabled State

What happens when the port security violation is shutdown and a port violation occurs? The port is physically shutdown and placed in the error-disabled state, and no traffic is sent or received on that port.

In the figure, the port security violation is changed back to the default shutdown setting. Then the host with MAC address a41f.7272.676a is disconnected and a new host is plugged into Fa0/1.

Notice how a series of port security related messages are generated on the console.

```
S1(config)# int fa0/1
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# end
S1#
*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
S1#
*Mar  1 00:24:32.829: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in
err-disable state
*Mar  1 00:24:32.838: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address a41f.7273.018c on port FastEthernet0/1.
*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S1#
```

Note: The port protocol and link status are changed to down and the port LED is turned off.

In the example, the show interface command identifies the port status as err-disabled. The output of the show port-security interface command now shows the port status as Secure-shutdown instead of Secure-up. The Security Violation counter increments by 1.

```
S1# show interface fa0/1 | include down
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 1
S1#
```

The administrator should determine what caused the security violation If an unauthorized device is connected to a secure port, the security threat is eliminated before re-enabling the port.

In the next example, the first host is reconnected to Fa0/1. To re-enable the port, first use the **shutdown** command, then, use the **no shutdown** command to make the port operational, as shown in the example.

```
S1(config)# interface fa0/1
S1(config-if)# shutdown
S1(config-if)#
*Mar  1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
S1(config-if)# no shutdown
S1(config-if)#
*Mar  1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
S1(config-if)#
```

11.1.8

Verify Port Security

After configuring port security on a switch, check each interface to verify that the port security is set correctly, and check to ensure that the static MAC addresses have been configured correctly.

Port Security for All Interfaces

To display port security settings for the switch, use the **show port-security** command. The example indicates that only one port is configured with the switchport port-security command.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              2            2                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Port Security for a Specific Interface

Use the **show port-security interface** command to view details for a specific interface, as shown previously and in this example.

```
S1# show port-security interface fastethernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 0
S1#
```

Verify Learned MAC Addresses

To verify that MAC addresses are “sticking” to the configuration, use the **show run** command as shown in the example for FastEthernet 0/19.

```
S1# show run interface fa0/1
Building configuration...

Current configuration : 365 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a41f.7272.676a
 switchport port-security mac-address aaaa.bbbb.1234
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 switchport port-security
end

S1#
```

Verify Secure MAC Addresses

To display all secure MAC addresses that are manually configured or dynamically learned on all switch interfaces, use the **show port-security address** command as shown in the example.

```
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    a41f.7272.676a    SecureSticky                  Fa0/1       -
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

11.2.1 VLAN Attacks

Steps to Mitigate VLAN Hopping Attacks

Use the following steps to mitigate VLAN hopping attacks:

Step 1: Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.

Step 2: Disable unused ports and put them in an unused VLAN.

Step 3: Manually enable the trunk link on a trunking port by using the switchport mode trunk command.

Step 4: Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.

Step 5: Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan vlan_number command.

For example, assume the following:

- FastEthernet ports 0/1 through fa0/16 are active access ports
- FastEthernet ports 0/17 through 0/20 are not currently in use
- FastEthernet ports 0/21 through 0/24 are trunk ports.

VLAN hopping can be mitigated by implementing the following configuration.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
```

```
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
```

S1#

- FastEthernet ports 0/1 to 0/16 are access ports and therefore trunking is disabled by explicitly making them access ports.
- FastEthernet ports 0/17 to 0/20 are unused ports and are disabled and assigned to an unused VLAN.
- FastEthernet ports 0/21 to 0/24 are trunk links and are manually enabled as trunks with DTP disabled. The native VLAN is also changed from the default VLAN 1 to an unused VLAN 999.

Steps to Implement DHCP Snooping

Use the following steps to enable DHCP snooping:

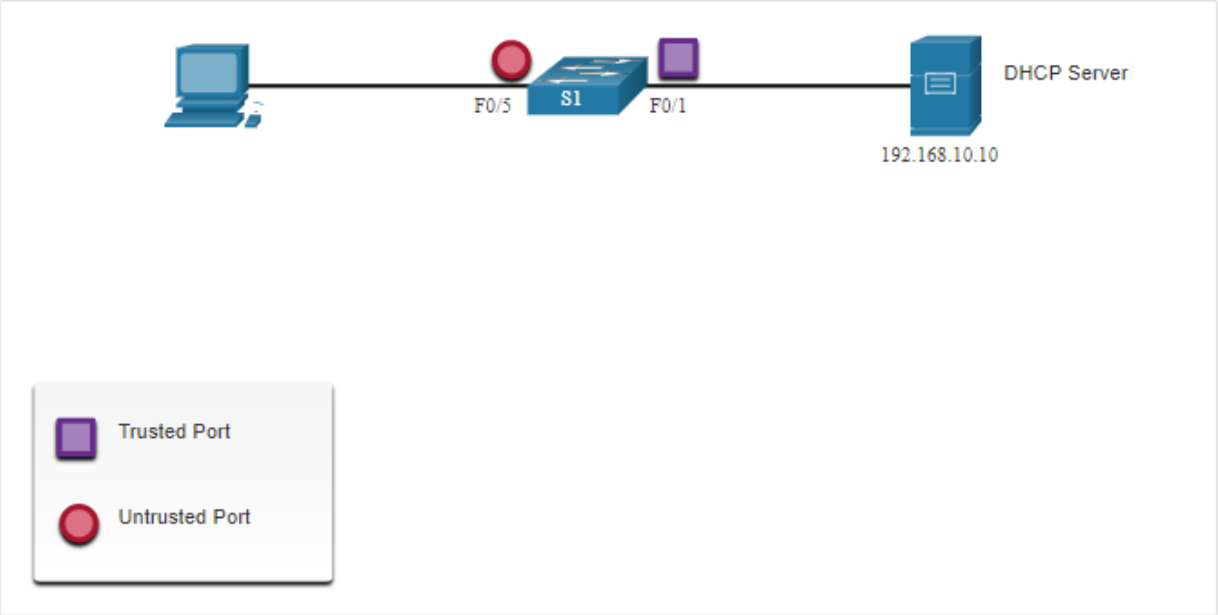
Step 1. Enable DHCP snooping by using the ip dhcp snooping global configuration command.

Step 2. On trusted ports, use the ip dhcp snooping trust interface configuration command.

Step 3. Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the ip dhcp snooping limit rate interface configuration command.

Step 4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the ip dhcp snooping vlan global configuration command.

The reference topology for this DHCP snooping example is shown in the figure. Notice that F0/5 is an untrusted port because it connects to a PC. F0/1 is a trusted port because it connects to the DHCP server.



The following is an example of how to configure DHCP snooping on S1. Notice how DHCP snooping is first enabled. Then the upstream interface to the DHCP server is explicitly trusted. Next, the range of FastEthernet ports from F0/5 to F0/24 are untrusted by default, so a rate limit is set to six packets per second. Finally, DHCP snooping is enabled on VLANS 5, 10, 50, 51, and 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Use the **show ip dhcp snooping** privileged EXEC command to verify DHCP snooping and **show ip dhcp snooping binding** to view the clients that have received DHCP information, as shown in the example.

11.4.3 DAI Configuration Example

In the previous topology, S1 is connecting two users on VLAN 10. DAI will be configured to mitigate against ARP spoofing and ARP poisoning attacks.

As shown in the example, DHCP snooping is enabled because DAI requires the DHCP snooping binding table to operate. Next, DHCP snooping and ARP inspection are enabled for the PCs on VLAN10. The uplink port to the router is trusted, and therefore, is configured as trusted for DHCP snooping and ARP inspection.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

DAI can also be configured to check for both destination or source MAC and IP addresses:

- **Destination MAC** - Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body.
- **Source MAC** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
- **IP address** - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

The **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** global configuration command is used to configure DAI to drop ARP packets when the IP addresses are invalid. It can be used when the MAC addresses in the body of the ARP packets do not match the addresses that are specified in the Ethernet header. Notice in the following example how only one command can be configured. Therefore, entering multiple **ip arp inspection validate** commands overwrites the previous command. To include more than one validation method, enter them on the same command line as shown and verified in the following output.

```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

11.5 Mitigate STP Attacks

Configure PortFast

PortFast bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge. If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.

PortFast can be enabled on an interface by using the **spanning-tree portfast** interface configuration command. Alternatively, Portfast can be configured globally on all access ports by using the **spanning-tree portfast default** global configuration command.

To verify whether PortFast is enabled globally you can use either the **show running-config | begin span** command or the **show spanning-tree summary** command. To verify if PortFast is enabled as an interface, use the **show running-config interface** *type/number* command, as shown in the following example. The **show spanning-tree interface** *type/number* **detail** command can also be used for verification.
Notice that when PortFast is enabled, warning messages are displayed.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

Configure BPDU Guard
Even though PortFast is enabled, the interface will still listen for BPDUs. Unexpected BPDUs might be accidental, or part of an unauthorized attempt to add a switch to the network.

If any BPDUs are received on a BPDU Guard enabled port, that port is put into error-disabled state. This means the port is shut down and must be manually re-enabled or automatically recovered through the **errdisable recovery cause bpduguard** global command.

BPDU Guard can be enabled on a port by using the **spanning-tree bpduguard enable** interface configuration command. Alternatively, Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on all PortFast-enabled ports.

To display information about the state of the spanning tree, use the **show spanning-tree summary** command. In the example, PortFast default and BPDU Guard are both enabled as the default state for ports configured as access mode.

Note: Always enable BPDU Guard on all PortFast-enabled ports.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
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
(output omitted)
S1#
```

Module 14 Routing Concepts

Lab 7.2.2.4 Configuring Basic EIGRP with IPv4

Enable the EIGRP routing process on each router using AS number 1

```
R1(config)# router eigrp 1
R2(config)# router eigrp 1
R3(config)# router eigrp 1
```

Use the **show ip route** command to display the directly connected networks on each router

On each router, configure EIGRP to advertise the specific directly connected subnets

```
R1#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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
L       172.16.3.1/32 is directly connected, Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/1
L       192.168.10.5/32 is directly connected, Serial0/0/1
```

```
R1(config-router)# network 172.16.1.0 0.0.0.255
R1(config-router)# network 172.16.3.0 0.0.0.3
R1(config-router)# network 192.168.10.4 0.0.0.3
```

```
R2#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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.16.2.0/24 is directly connected, GigabitEthernet0/0
L       172.16.2.1/32 is directly connected, GigabitEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
L       172.16.3.2/32 is directly connected, Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.8/30 is directly connected, Serial0/0/1
L       192.168.10.9/32 is directly connected, Serial0/0/1
```

```
R2(config-router)#network 172.16.2.0 0.0.0.255
R2(config-router)#network 172.16.3.0 0.0.0.3
R2(config-router)#
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is
up: new adjacency
R2(config-router)#network 192.168.10.8 0.0.0.3
R2(config-router)#
```

```
R3#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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/0
L       192.168.10.6/32 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
L       192.168.10.10/32 is directly connected, Serial0/0/1
```

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.10.8 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is
up: new adjacency
R3(config-router)#network 192.168.10.4 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is
up: new adjacency
R3(config-router)#network 192.168.1.0 0.0.0.255
```

Configure the LAN interfaces to not advertise EIGRP updates

```
R1(config-router)# passive-interface g0/0
R2(config-router)# passive-interface g0/0
R3(config-router)# passive-interface g0/0
```

The topology contains discontiguous networks. Therefore, disable automatic summarization on each router

```
R1(config-router)# no auto-summary
R2(config-router)# no auto-summary
R3(config-router)# no auto-summary
```

Save the configurations.

```
R1# copy run start
R2# copy run start
R3# copy run start
```