
IT NE 2005

Securing the Local Area Network

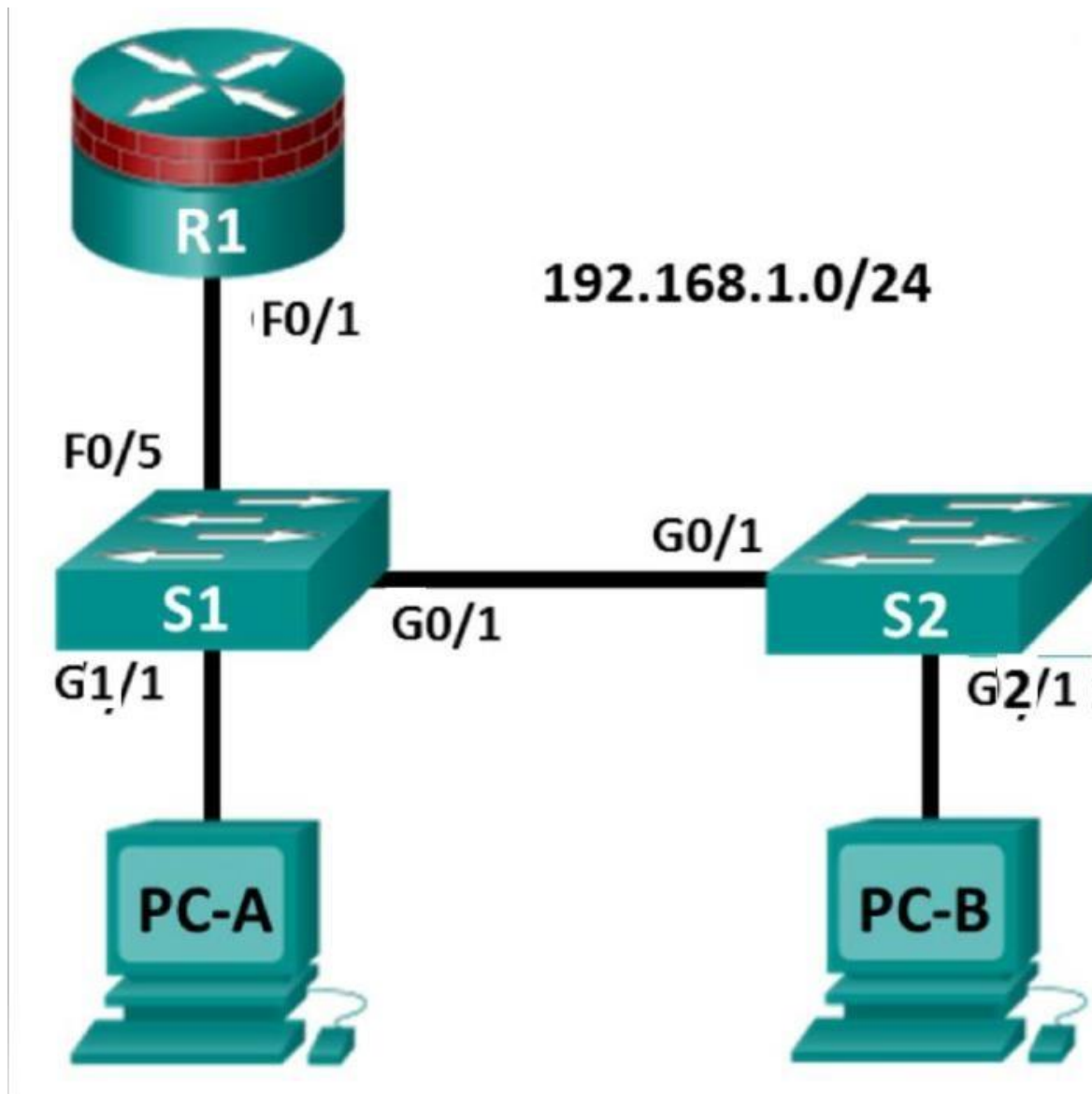
LAB 5

WEEK - 7

CONTENTS

Week 7 Implementing Securing the Local Area Network

Objective: Configure Securing the Local Area Network **TOPOLOGY:**



Note: ISR G1 devices have Fast Ethernet interfaces instead of Gigabit Ethernet Interfaces.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1-S0000	F0/1	192.168.1.1	255.255.255.0	N/A	S1 G0/0
S1-S0000	VLAN 1	192.168.1.2	255.255.255.0	N/A	N/A

S2-S0000	VLAN 1	192.168.1.3	255.255.255.0	N/A	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	S1 G1/1
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 G2/1

In this lab, you will perform the following tasks:

Part 1: Configure Basic Device Settings

- Build the topology
- Configure basic settings such as host name, interface IP addresses, and access passwords.

Part 2: Configure SSH Access to the Switches

- Configure SSH version 2 access on the switch.
- Configure an SSH client to access the switch.
- Verify the configuration.

Part 3: Configure Secure Trunks and Access Ports

- Configure trunk port mode.
- Change the native VLAN for trunk ports.
- Verify trunk configuration.
- Enable storm control for broadcasts.
- Configure access ports.
- Enable PortFast and BPDU guard.
- Verify BPDU guard.
- Enable root guard.
- Enable loop guard.
- Configure and verify port security.
- Disable unused ports.
- Move ports from default VLAN 1 to alternate VLAN.
- Configure the PVLAN Edge feature on a port.

Part 4: Configure IP DHCP Snooping

- Configure DHCP on R1.
- Configure Inter-VLAN communication on R1.
- Configure S1 interface G0/0 as a trunk.
- Verify DHCP operation on PC- A and B.
- Enable DHCP Snooping.
- Verify DHCP Snooping.

BACKGROUND

The Layer 2 infrastructure consists mainly of interconnected Ethernet switches. Most end-user devices, such as computers, printers, IP phones, and other hosts, connect to the network via Layer 2 access switches. As a result, switches can present a network security risk. Similar to routers, switches are subject to attack from malicious internal users. The switch Cisco IOS software provides many security features that are specific to switch functions and protocols.

In this lab, you will configure SSH access and Layer 2 security for S1-StudentID and S2-StudentID. You will also configure various switch protection measures, including access port security and Spanning Tree Protocol (STP) features, such as BPDU guard and root guard.

Note: The router commands and output in this lab are from a Cisco 1941 with Cisco IOS Release 15.4(3)M2 (Universalk9-M). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Before beginning, ensure that the switches have been erased and have no startup configurations.

Task 1: Configure Basic Device Settings

The desktop system assigned to you serves as an end-user terminal. You access and manage the lab environment from the student desktop system using GNS3 Software.

Students should perform the steps in this task individually.

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1-S0000.

The procedure for R1 is shown here as an example.

Step 1: Configure and Deploy switch in GNS3 network.

If you have not already configured, Configure Switch appliance **cisco-iosvl2.gns3a** from \\10.1.2.78\student\$GNS3 and use Switch image **IOS-S465-CLI.pkg**. Attach the devices, as shown in the topology diagram, and connection as necessary.

Step 2: Configure basic settings for the router and each switch.

Perform all tasks on R1, S1, and S2. The procedure for S1 is shown here as an example.

a. Configure hostnames, as shown in the topology.

b. Configure interface IP addresses, as shown in the IP Addressing Table. The following configuration displays the VLAN 1 management interface on S1:

```
S1-S0000(config)# interface vlan 1
S1-S0000(config-if)# ip address 192.168.1.2 255.255.255.0
S1-S0000(config-if)# no shutdown
```

c. Prevent the router or switch from attempting to translate incorrectly entered commands by disabling DNS lookup. S1 is shown here as an example.

```
S1-S0000(config)# no ip domain-lookup
```

d. HTTP access to the switch is enabled by default. Prevent HTTP access by disabling the HTTP server and HTTP secure server.

```
S1-S0000(config)# no ip http server
S1-S0000(config)# no ip http secure-server
```

Note: The switch must have a cryptography IOS image to support the ip http secure-server command. HTTP access to the router is disabled by default.

e. Configure the enable secret password.

```
S1-S0000(config)# enable secret cisco12345
```

f. Configure console password.

```
S1-S0000(config)# line console 0
S1-S0000(config-line)# password ciscoconpass
S1-S0000(config-line)# exec-timeout 5 0
S1-S0000(config-line)# login
S1-S0000(config-line)# logging synchronous
```

Step 3: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-B, as shown in the IP Addressing Table.

Step 4: Verify basic network connectivity.

a. Ping from PC-A and PC-B to the R1 F0/1 interface at IP address 192.168.1.1.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing. b.

Ping from PC-A to PC-B.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 5: Save the basic configurations for the router and both switches.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

```
S1-S0000# copy running-config startup-config
```

Part 2: Configure SSH Access to the Switches

In Part 2, you will configure S1 and S2 to support SSH connections and install SSH client software on the PCs.

Note: A switch IOS image that supports encryption is required to configure SSH. If this version of image is not used you cannot specify SSH as an input protocol for the vty lines and the crypto commands are unavailable.

Task 1: Configure the SSH Server on S1 and S2 Using the CLI.

In this task, use the CLI to configure the switch to be managed securely using SSH instead of Telnet. SSH is a network protocol that establishes a secure terminal emulation connection to a switch or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the preferred remote login tool for network professionals. It is strongly recommended that SSH be used in place of Telnet on production networks.

Note: A switch must be configured with local authentication or AAA in order to support SSH.

Step 1: Configure a domain name and hostname.

Enter global configuration mode and set the domain name.

```
S1-S0000# conf t
```

```
S1-S0000# hostname S-S0000
```

```
S1-S0000(config)# ip domain-name ccnasecurity.com
```

Step 2: Configure a privileged user for login from the SSH client.

Use the username command to create the user ID with the highest possible privilege level and a secret password.

```
S1-S0000(config)# username admin privilege 15 secret cisco12345
```

Step 3: Generate the RSA encryption key pair for the router.

The switch uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with 1024 modulus bits. The default number of modulus bits is 512, and the range is from 360 to 2,048. S1-S0000(config)# crypto key generate rsa general-keys modulus 1024

Step 4: Configure SSH version 2

```
S1-S0000(config)# ip ssh version 2
```

Step 5: Verify the SSH configuration.

- a. Use the show ip ssh command to see the current settings.

```
S1-S0000# show ip ssh
```

- b. Fill in the following information based on the output of the show ip ssh command: SSH version

enabled: _____

Authentication timeout: _____

Authentication retries: _____

Step 6: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
S1-S0000(config)# ip ssh time-out 90
```

```
S1-S0000(config)# ip ssh authentication-retries 2
```

Step 7: Configure the incoming vty lines.

- a. Configure vty access on lines 0 to 4. Specify a privilege level of 15. This will ensure that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Specify the use of local user accounts for mandatory login and validation and accept only SSH connections.

```
S1-S0000(config)# line vty 0 4
```

```
S1-S0000(config-line)# privilege level 15
```

```
S1-S0000(config-line)# exec-timeout 5 0
```

```
S1-S0000(config-line)# login local
```

```
S1-S0000(config-line)# transport input ssh
```

```
S1-S0000(config-line)# exit
```

- b. Disable login for switch vty lines 5 to 15 by allowing no transport input.

```
S1-S0000(config)# line vty 5 15
```

```
S1-S0000(config-line)# transport input none
```

Step 8: Save the running configuration to the startup configuration.

```
S1-S0000# copy running-config startup-config
```

Task 2: Configure the SSH Client

SSH from R1 to S1 and S2 **OR** use PuTTY and Tera Term are two terminal emulation programs that can support SSHv2 client connections.

Step: Verify SSH connectivity to R1 from R2.

a. From Router2-STUDENTID, telnet to R1-STUDENTID again.

S2-S0000# ssh -l admin 192.168.1.2 (l=small L)

Use cisco12345 as password

OR

Step 1: (Optional) Download and install an SSH client on PC-A and PC-B.

If the SSH client is not already installed, download PuTTY from the following link:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> Note:

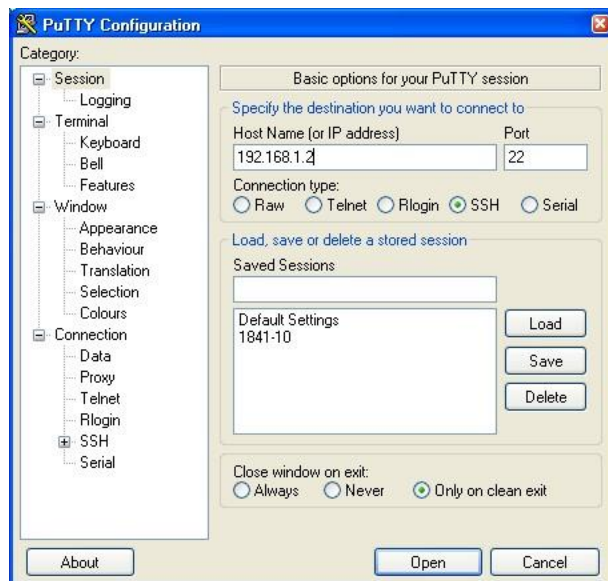
The procedure described here is for PuTTY and pertains to PC-A.

Step 2: Verify SSH connectivity to S1 from PC-A.

a. Launch PuTTY by double-clicking the putty.exe icon (and clicking Run if prompted).

b. Input the S1 IP address 192.168.1.2 in the Host Name (or IP address) field.

c. Verify that the SSH radio button is selected. PuTTY defaults to SSH version 2.



d. Click Open.

Note: Upon first connection, the user is prompted with a PuTTY Security Alert stating that the server's host key is not cached in the registry.

e. In the PuTTY Security Alert window, click Yes to cache the server's host key.

f. In the PuTTY window, enter admin as the username and cisco12345 as the password.



g. At the S1 privileged EXEC mode prompt, enter the show users command.

```
S1-S0000# show users
```

Which users are connected to S1 at this time?

h. Close the PuTTY SSH session window with the exit or quit command.

Try to open a Telnet session to S1 from S2 or PC-A. Were you able to open the Telnet session? Explain.

Step 3: Save the configuration.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

```
S1-S0000# copy running-config startup-config
```

Part 3: Configure Secure Trunks and Access Ports

In Part 3, you will configure trunk ports, change the native VLAN for trunk ports, and verify trunk configuration.

Securing trunk ports can help stop VLAN hopping attacks. The best way to prevent a basic VLAN hopping attack is to explicitly disable trunking on all ports except the ports that specifically require trunking. On the required trunking ports, disable DTP (auto trunking) negotiations and manually enable trunking. If no trunking is required on an interface, configure the port as an access port. This disables trunking on the interface.

Note: Tasks should be performed on S1 or S2, as indicated.

Task 1: Secure Trunk Ports

Step 1: Configure S1 as the root switch.

For the purposes of this lab, S2 is currently the root bridge. You will configure S1 as the root bridge by changing the bridge ID priority level.

a. From the console on S1, enter global configuration mode.

b. The default priority for S1 and S2 is 32769 (32768 + 1 with System ID Extension). Set S1 priority to 0 so that it becomes the root switch.

```
S1-S0000(config)# spanning-tree vlan 1 priority 0
```

```
S1-S0000(config)# exit
```

Note: You can also use the spanning-tree vlan 1 root primary command to make S1 the root switch for VLAN 1.

- c. Issue the show spanning-tree command to verify that S1 is the root bridge, to see the ports in use, and to see their status.

```
S1-S0000# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority      1
```

```
Address      001d.4635.0c80
```

```
This bridge is the root
```

```
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

- d. What is the S1 priority?

Which ports are in use and what is their status?

Step 2: Configure trunk ports on S1 and S2.

- a. Configure port G0/1 on S1 as a trunk port.

```
S1-S0000(config)# interface g0/1
```

```
S1-S0000(config-if)# switchport mode trunk OR switchport trunk encapsulation dot1q
```

Note: If performing this lab with a 3560 switch, the user must first enter the switchport trunk encapsulation dot1q command.

- b. Configure port G0/1 on S2 as a trunk port.

```
S2-S0000(config)# interface g0/1
```

```
S2-S0000(config-if)# switchport mode trunk OR switchport trunk encapsulation dot1q
```

- c. Verify that S1 port G0/1 is in trunking mode with the show interfaces trunk command.

```
S1-S0000# show interfaces trunk
```

Step 3: Change the native VLAN for the trunk ports on S1 and S2.

- a. Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

From the output of the show interfaces trunk command in the previous step, what is the current native VLAN for the S1 G0/1 trunk interface?

b. Set the native VLAN on the S1 G0/1 trunk interface to an unused VLAN 99.

```
S1-S0000(config)# interface G0/1
```

```
S1-S0000(config-if)# switchport trunk native vlan 99
```

```
S1-S0000(config-if)# end
```

c. The following message should display after a brief period of time:

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with S2
FastEthernet0/1 (1).
```

What does the message mean?

d. Set the native VLAN on the S2 G0/1 trunk interface to VLAN 99.

```
S2-S0000(config)# interface G0/1
```

```
S2-S0000(config-if)# switchport trunk native vlan 99
```

```
S2-S0000(config-if)# end
```

Step 4: Prevent the use of DTP on S1 and S2.

Setting the trunk port to nonegotiate also helps to mitigate VLAN hopping by turning off the generation of DTP frames.

```
S1-S0000(config)# interface g0/1
```

```
S1-S0000(config-if)# switchport nonegotiate
```

```
S2-S0000(config)# interface g0/1
```

```
S2-S0000(config-if)# switchport nonegotiate
```

Step 5: Verify the trunking configuration on port F0/1.

```
S1-S0000# show interfaces g0/1 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1

S1-S0000# show interfaces G0/1 switchport

```

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: 99 (Inactive)
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 private VLANs: none
Operational private-vlan: none

```

Step 6: Verify the configuration with the show run command.

Use the show run command to display the running configuration, beginning with the first line that has the text string "0/1" in it.

S1-S0000# show run | begin 0/1

```
interface GigabitEthernet0/1
```

```
switchport trunk native vlan 99

switchport mode trunk switchport

nonegotiate
```

Task 2: Secure Access Ports

Network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology by manipulating the STP root bridge parameters. If a port that is configured with PortFast receives a BPDU, STP can put the port into the blocking state by using a feature called BPDU guard.

Step 1: Disable trunking on S1 access ports.

- a. On S1, configure Ga0/5, the port to which R1 is connected, as access mode only.

```
S1-S0000(config)# interface g0/0

S1-S0000(config-if)# switchport mode access
```

- b. On S1, configure Ga0/6, the port to which PC-A is connected, as access mode only.

```
S1-S0000(config)# interface g1/1

S1-S0000(config-if)# switchport mode access
```

Step 2: Disable trunking on S2 access ports.

- On S2, configure Ga0/18, the port to which PC-B is connected, as access mode only.

```
S2-S0000(config)# interface g2/1

S2-S0000(config-if)# switchport mode access
```

Task 3: Protect Against STP Attacks

The topology has only two switches and no redundant paths, but STP is still active. In this step, you will enable switch security features that can help reduce the possibility of an attacker manipulating switches via STP-related methods.

Step 1: Enable PortFast on S1 and S2 access ports.

PortFast is configured on access ports that connect to a single workstation or server, which enables them to become active more quickly.

- a. Enable PortFast on the S1 Ga0/0 access port.

```
S1-S0000(config)# interface g0/0

S1-S0000(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 gigabitEthernet0/x but will only have effect when the interface is in a non-trunking mode.

- b. Enable PortFast on the S1 G1/1 access port.

```
S1-S0000(config)# interface g1/1
S1-S0000(config-if)# spanning-tree portfast
```

- c. Enable PortFast on the S2 G2/1 access ports.

```
S2-S0000(config)# interface g2/1
S2-S0000(config-if)# spanning-tree portfast
```

Step 2: Enable BPDU guard on the S1 and S2 access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports.

- a. Enable BPDU guard on the switch port G1/1.

```
S1-S0000(config)# interface g1/1
S1-S0000(config-if)# spanning-tree bpduguard enable
S2-S0000(config)# interface g2/1
S2-S0000(config-if)# spanning-tree bpduguard enable
```

Note: PortFast and BPDU guard can also be enabled globally with the spanning-tree portfast default and spanningtree portfast bpduguard commands in global configuration mode.

Note: BPDU guard can be enabled on all access ports that have PortFast enabled. These ports should never receive a BPDU. BPDU guard is best deployed on user-facing ports to prevent rogue switch network extensions by an attacker. If a port is enabled with BPDU guard and receives a BPDU, it is disabled and must be manually re-enabled. An err-disable timeout can be configured on the port so that it can recover automatically after a specified time period.

- b. Verify that BPDU guard is configured by using the show spanning-tree interface g1/1 detail command on S1.

```
S1-S0000# show spanning-tree interface g1/1 detail

Port 6 (FastEthernet0/6) of VLAN0001 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.6.

Designated root has priority 1, address 001d.4635.0c80

Designated bridge has priority 1, address 001d.4635.0c80

Designated port id is 128.6, designated path cost 0

Timers: message age 0, forward delay 0, hold 0
```

Step 3: Enable root guard.

Root guard is another option to help prevent rogue switches and spoofing. Root guard can be enabled on all ports on a switch that are not root ports. It is normally enabled only on ports connecting to edge switches where a

superior BPDU should never be received. Each switch should have only one root port, which is the best path to the root switch.

- a. The following command configures root guard on S2 interface Gi0/1. Normally, this is done if another switch is attached to this port. Root guard is best deployed on ports that connect to switches that should not be the root bridge. In the lab topology, S1 G0/1 would be the most logical candidate for root guard.

However, S2 Gi0/1 is shown here as an example, as Gigabit ports are more commonly used for interswitch connections.

```
S2-S0000(config)# interface g0/1
```

```
S2-S0000(config-if)# spanning-tree guard root
```

- b. Issue the show run | begin Gig command to verify that root guard is configured. S2-S0000# show run | begin Gig
interface GigabitEthernet0/1 spanning-tree guard root

Note: The S2 Gi0/1 port is not currently up, so it is not participating in STP. Otherwise, you could use the show spanning-tree interface Gi0/1 detail command.

Note: The expression in the command show run | begin is case-sensitive.

- c. If a port that is enabled with BPDU guard receives a superior BPDU, it enters a root-inconsistent state.

Use the show spanning-tree inconsistentports command to determine if there are any ports currently receiving superior BPDUs that should not be.

```
S2-S0000# show spanning-tree inconsistentports
```

Name Interface Inconsistency

Note: Root guard allows a connected switch to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. The port returns to the forwarding state if the superior BPDUs stop.

Step 4: Enable Loop Guard

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops).

An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. Having all ports in forwarding state will result in forwarding loops. If a port enabled with loopguard stops hearing BPDUs from the designated port on the segment, it goes into the loop inconsistent state instead of transitioning into forwarding state.

Loop inconsistent is basically blocking, and no traffic is forwarded. When the port detects BPDUs again it automatically recovers by moving back into blocking state.

- a. Loop guard should be applied to non-designated ports. Therefore, the global command can be configured on non-root switches.

```
S2-S0000(config)# spanning-tree loopguard default
```

b. Verify Loopguard configuration

```
S2-S0000# show spanning-tree summary
```

Switch is in pvst mode

```
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is enabled
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

Task 4: Configure Port Security and Disable Unused Ports

Switches can be subject to a CAM table, also known as a MAC address table, overflow, MAC spoofing attacks, and unauthorized connections to switch ports. In this task, you will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Record the R1 G0/0 MAC address.

From the R1 CLI, use the show interface command and record the MAC address of the interface.

```
R1-S0000# show interfaces g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
```

```
Internet address is 192.168.1.1/24
```

```
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 Omitted>
```

What is the MAC address of the R1 G0/1 interface?

Step 2:

Configure basic port security.

This procedure should be performed on all access ports that are in use. S1 port G0/5 is shown here as an example.

- a. From the S1 CLI, enter interface configuration mode for the port that connects to the router (Fast Ethernet 0/5).

```
S1-S0000(config)# interface G0/0
```

- b. Shut down the switch port.

```
S1-S0000(config-if)# shutdown
```

- c. Enable port security on the port.

```
S1-S0000(config-if)# switchport port-security
```

Note: A switch port must be configured as an access port to enable port security.

Note: Entering just the switchport port-security command sets the maximum MAC addresses to 1 and the violation action to shutdown. The switchport port-security maximum and switchport portsecurity violation commands can be used to change the default behavior.

- d. Configure a static entry for the MAC address of R1 Fa0/1/ interface recorded in Step 1.

```
S1-S0000(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx c201.c188.0001
```

Note: xxxx.xxxx.xxxx is the actual MAC address of the router F0/1 interface.

Note: You can also use the switchport port-security mac-address sticky command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

- e. Enable the switch port.

```
S1-S0000(config-if)# no shutdown
```

Step 3: Verify port security on S1 G0/0.

- a. On S1, issue the show port-security command to verify that port security has been configured on S1 G0/0. S1-

```
S0000# show port-security interface G0/0
```

```
Port Security : Enabled
```

```
Port Status : Secure-up
```

```
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 : 0000.0000.0000:0

Security Violation Count : 0

What is the Security Violation Count? _____

What is the status of the G0/0 port?

What is the Last Source Address and VLAN?

b. From the R1 CLI, ping PC-A to verify connectivity. This also ensures that the R1 G0/1 MAC address is learned by the switch.

```
R1-S0000# ping 192.168.1.10
```

c. Now, violate security by changing the MAC address on the router interface. Enter interface configuration mode for the Fast Ethernet 0/1. Configure a MAC address for the interface on the interface, using aaaa.bbbb.cccc as the address.

```
R1-S0000(config)# interface f0/1
```

```
R1-S0000(config-if)# mac-address aaaa.bbbb.cccc
```

```
R1-S0000(config-if)# end
```

Note: You can also change the PC MAC address attached to S1 G1/1 and achieve similar results to those shown here.

d. From the R1 CLI, ping PC-A. Was the ping successful? Explain.

e. On S1 console, observe the messages when port G0/0 detects the violating MAC address.

*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on Ga0/5, putting Ga0/5 in err-disable state

*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address aaaa.bbbb.cccc on port FastEthernet0/5.

*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

*Jan 14 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down

f. On the switch, use the show port-security commands to verify that port security has been violated.

S1-S0000# show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action (Count) (Count) (Count)

Ga0/5 1 1 1 Shutdown

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

S1-S0000# show port-security interface g0/0

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 : aaaa.bbbb.cccc:1

Security Violation Count : 1

S1-S0000# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining	Age (mins)
------	-------------	------	-------	-----------	------------

1	fc99.4775.c3e1	SecureConfigured	Ga0/1	-	
---	----------------	------------------	-------	---	--

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

g. Remove the hard-coded MAC address from the router and re-enable the Fast Ethernet 0/1 interface.

```
R1-S0000(config)# interface g0/1
```

```
R1-S0000(config-if)# no mac-address aaaa.bbbb.cccc
```

Note: This will restore the original FastEthernet interface MAC address.

From R1, try to ping the PC-A again at 192.168.1.10. Was the ping successful? Why or why not?

Step 4: Clear the S1 Ga0/0 error disabled status.

a. From the S1 console, clear the error and re-enable the port using the commands shown in the example.

This will change the port status from Secure-shutdown to Secure-up.

```
S1-S0000(config)# interface g0/0
```

```
S1-S0000(config-if)# shutdown
```

```
S1-S0000(config-if)# no shutdown
```

Note: This assumes the device/interface with the violating MAC address has been removed and replaced with the original device/interface configuration.

b. From R1, ping PC-A again. You should be successful this time.

```
R1-S0000# ping 192.168.1.10
```

Step 5: Remove basic port security on S1 G0/0.

From the S1 console, remove port security on Ga0/5. This procedure can also be used to re-enable the port, but port security commands must be reconfigured.

```
S1-S0000(config)# interface G0/0
```

```
S1-S0000(config-if)# no switchport port-security
```

```
S1-S0000(config-if)# no switchport port-security mac-address fc99.4775.c3e1
```

You can also use the following commands to reset the interface to its default settings:

```
S1-S0000(config)# default interface G0/0
```

```
S1-S0000(config)# interface G0/0
```

Note: This default interface command also requires that you reconfigure the port as an access port to re-enable the security commands.

Step 6: (Optional) Configure port security for VoIP.

This example shows a typical port security configuration for a voice port. Three MAC addresses are allowed and should be learned dynamically. One MAC address is for the IP phone, one is for the switch, and one is for the PC connected to the IP phone. Violations of this policy result in the port being shut down. The aging timeout for the learned MAC addresses is set to two hours.

The following example displays S2 port G2/1:

```
S2-S0000(config)# interface g2/1
```

```
S2-S0000(config-if)# switchport mode access
```

```
S2-S0000(config-if)# switchport port-security
```

```
S2-S0000(config-if)# switchport port-security maximum 3
```

```
S2-S0000(config-if)# switchport port-security violation shutdown
```

```
S2-S0000(config-if)# switchport port-security aging time 120
```

Step 7: Disable unused ports on S1 and S2.

As a further security measure, disable ports that are not being used on the switch.

- a. Ports G0/0, and G1/2 are used on S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shut down.

```
S1-S0000(config)# interface range G3/0 - 3
```

```
S1-S0000(config-if-range)# shutdown
```

- b. Ports Ga0/1 and Ga2/1 are used on S2. The remaining Gigabit Ethernet ports will be shut down.

```
S2-S0000(config)# interface range g3/0 - 3
```

```
S2-S0000(config-if-range)# shutdown
```

Step 8: Move active ports to a VLAN other than the default VLAN 1.

As a further security measure, you can move all active end-user ports and router ports to a VLAN other than the default VLAN 1 on both switches.

a. Configure a new VLAN for users on each switch using the following commands:

```
S1-S0000(config)# vlan 20
```

```
S1-S0000(config-vlan)# name Users
```

```
S2-S0000(config)# vlan 20
```

```
S2-S0000(config-vlan)# name Users
```

b. Add the current active access (non-trunk) ports to the new VLAN.

```
S1-S0000(config)# interface g0/1
```

```
S1-S0000(config-if-range)# switchport access vlan 20
```

```
S2-S0000(config)# interface g2/1
```

```
S2-S0000(config-if)# switchport access vlan 20
```

Note: This will prevent communication between end-user hosts and the management VLAN IP address of the switch, which is currently VLAN 1. The switch can still be accessed and configured using the console connection.

Note: To provide SSH access to the switch, a specific port can be designated as the management port and added to VLAN 1 with a specific management workstation attached. A more elaborate solution is to create a new VLAN for switch management (or use the existing native trunk VLAN 99), and configure a separate subnet for the management and user VLANs. In Part 4 you will enable trunking with subinterfaces on R1 to provide communication between the management and user VLAN subnets.

Step 9: Configure a port with the PVLAN Edge feature.

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of the Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch. The PVLAN Edge feature can only be implemented for ports on the same switch and is locally significant.

For example, to prevent traffic between host PC-A on S1 (port Ga1/1) and a host on another S1 port (e.g. port Ga3/1, which was previously shut down), you could use the switchport protected command to activate the PVLAN Edge feature on these two ports. Use the no switchport protected interface configuration command to disable protected port.

a. Configure the PVLAN Edge feature in interface configuration mode using the following commands:

```
S1-S0000(config)# interface g1/1
```

```
S1-S0000(config-if)# switchport protected
```

```
S1-S0000(config-if)# interface g1/2
```

```
S1-S0000(config-if)# switchport protected
```

```
S1-S0000(config-if)# no shut
```

S1-S0000(config-if)# end

b. Verify that the PVLAN Edge Feature (protected port) is enabled on Ga1/1.

S1-S0000# show interfaces ga1/1 switchport

Name: Ga1/1

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 20 (Users)

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 private VLANs: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Capture Mode Disabled

Capture VLANs Allowed: ALL

Protected: true

Unknown unicast blocked: disabled

Unknown multicast blocked: disabled

Appliance trust: none

c. Deactivate protected port on interfaces Ga1/1 and Ga3/1 using the following commands:

```
S1-S0000(config)# interface range g1/1,g3/1
```

```
S1-S0000(config-if-range)# no switchport protected
```

Part 4: Configure DHCP Snooping

DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. It enables only authorized DHCP servers to respond to DHCP requests and distribute network information to clients.

Task 1: Set Up DHCP

Step 1: Set up DHCP on R1 for VLAN 1.

```
R1-S0000(config)# ip dhcp pool CCNAS
```

```
R1-S0000(dhcp-config)# network 192.168.1.0 255.255.255.0
```

```
R1-S0000(dhcp-config)# default-router 192.168.1.1
```

```
R1-S0000(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.4
```

Step 2: Set up DHCP on R1 for VLAN 20.

```
R1-S0000(config)# ip dhcp pool 20Users
```

```
R1-S0000(dhcp-config)# network 192.168.20.0 255.255.255.0 R1-S0000(dhcp-config)#
```

```
default-router 192.168.20.1
```

```
R1-S0000(config)# ip dhcp excluded-address 192.168.20.1 Task
```

2: Configure Inter-VLAN Communication

Step 1: Configure subinterfaces on R1.

```
R1-S0000(config)# interface f0/1
```

```
R1-S0000(config-if)# shutdown
```

```
R1-S0000(config-if)# no ip address 192.168.1.1 255.255.255.0
```

```
R1-S0000(config-if)# no shutdown
```

```
R1-S0000(config-if)# int f0/1.1
```

```
R1-S0000(config-if)# encapsulation dot1q 1
```

```
R1-S0000(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1-S0000(config-if)# int f0/1.20
```

```
R1-S0000(config-if)# encapsulation dot1q 20
```



```
R1-S0000(config-if)# ip address 192.168.20.1 255.255.255.0
```

```
R1-S0000(config-if)# int f0/1.99
```

```
R1-S0000(config-if)# encapsulation dot1q 99
```

```
R1-S0000(config-if)# ip address 192.168.99.1 255.255.255.0
```

Step 2: Configure S1 interface g0/0 as a trunk port.

```
S1-S0000(config)# int g0/0
```

```
S1-S0000(config-if)# switchport trunk encapsulation dot1q
```

```
S1-S0000(config-if)# switchport mode trunk
```

```
S1-S0000(config-if)# switchport trunk native vlan 99
```

Step 3: Configure PC-A and PC-B to obtain an IP Address using DHCP.

Change network settings on PC-A and PC-B to obtain an IP Address automatically.

Step 4: Verify DHCP operation.

Use ipconfig at the command prompt of PC-A and PC-B.

Task 3: Configure DHCP Snooping

Step 1: Enable DHCP snooping globally.

```
S1-S0000(config)# ip dhcp snooping
```

```
S1-S0000(config)# ip dhcp snooping information option
```

Step 2: Enable DHCP snooping for VLAN 1 and 20.

```
S1-S0000(config)# ip dhcp snooping vlan 1,20
```

Step 3: Limit the number of DHCP requests on an interface.

```
S1-S0000(config)# interface g0/1
```

```
S1-S0000(config-if)# ip dhcp snooping limit rate 10
```

```
S1-S0000(config-if)# exit
```

Step 4: Identify the trusted interface(s). DHCP responses are only permitted through trusted ports.

```
S1-S0000(config)# interface g0/0
```

```
S1-S0000(config-if)# description connects to DHCP server
```

```
S1-S0000(config-if)# ip dhcp snooping trust
```

Step 5: Verify DHCP snooping configuration.

S1-S0000# show ip dhcp snooping

Save running configuration on all routers