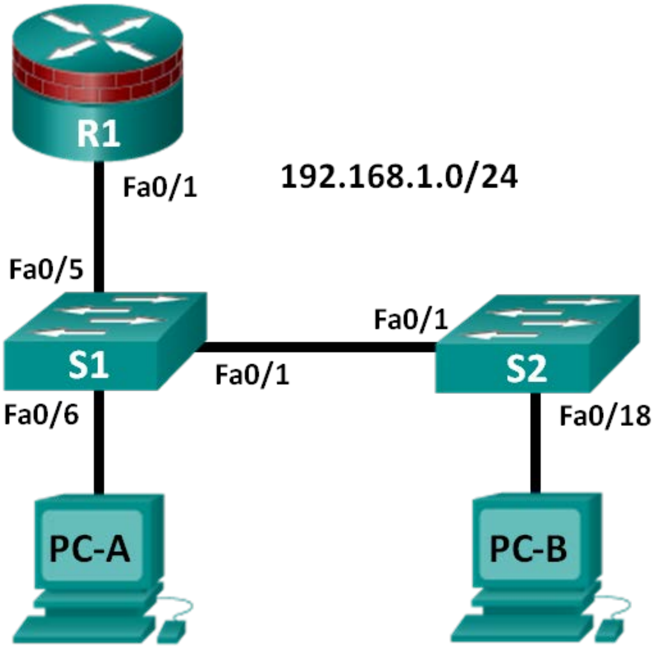
CCNA Security

Lab - Securing Layer 2 Switches

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A	N/A
S2	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 Fa0/6
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 Fa0/18

Objectives

Part 1: Configure Basic Switch Settings

- Build the topology.
- Configure the hostname, IP address, and access passwords.

Part 2: Configure SSH Access to the Switches

- Configure SSH 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.
- 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 SPAN and Monitor Traffic

- Configure the Switched Port Analyzer (SPAN).
- Monitor port activity using Wireshark.
- Analyze a sourced attack.

Background / Scenario

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 and S2. You will also configure various switch protection measures, including access port security, switch storm control, and Spanning Tree Protocol (STP) features, such as BPDU guard and root guard. Lastly, you use Cisco SPAN to monitor traffic to specific ports on the switch.

Note: The router commands and output in this lab are from a Cisco 1841 router using Cisco IOS software, release 15.1(4)M8 (Advanced IP Services image). The switch commands and output are from Cisco WS-C2960-24TT-L switches with Cisco IOS Release 15.0(2)SE4 (C2960-LANBASEK9-M image). Other routers, switches, 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, or switch model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 1 Router (Cisco 1841 with Cisco IOS Release 15.1(4)M8 Advanced IP Services image or comparable)
- 2 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE4 or comparable)

- 2 PCs (Windows Vista or Windows 7 with SSH Client, Wireshark, and Nmap/Zenmap)
- Ethernet cables as shown in the topology
- Console cables to configure Cisco networking devices

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the hostnames, IP addresses, and device access passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices, as shown in the topology diagram, and cable 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(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

c. To prevent the router or switch from attempting to translate incorrectly entered commands, disable DNS lookup. S1 is shown here as an example.

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

d. HTTP access to the switch is enabled by default. To prevent HTTP access, disable the HTTP server and HTTP secure server.

```
S1(config)# no ip http server
S1(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(config)# enable secret cisco12345
```

f. Configure console password.

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

Step 3: Configure vty lines and password on R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

Note: Do not configure the switch vty access at this time. The vty lines are configured on the switches in Part 2 for SSH access.

Step 4: 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 5: Verify basic network connectivity.

a. Ping from PC-A and PC-B to the R1 Fa0/1 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 6: 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# 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. Otherwise, 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 remote login tool of choice for network professionals. It is strongly recommended that SSH be used in place of Telnet on production networks.

Note: For a switch to support SSH, it must be configured with local authentication or AAA.

Step 1: Configure a domain name.

a. Enter global configuration mode and set the domain name.

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

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

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

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

b. Exit to the initial switch login screen, and log in with this username. What was the switch prompt after you entered the password?

____

____

Step 3: Configure the incoming vty lines.

a. Configure vty access on lines 0 to 4. Specify a privilege level of 15 so 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(config)# line vty 0 4
S1(config-line)# privilege level 15
S1(config-line)# exec-timeout 5 0
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# exit
```

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

```
S1(config)# line vty 5 15
S1(config-line)# transport input none
```

Step 4: 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** for the number of modulus bits. The default is 512, and the range is from 360 to 2,048.

```
S1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
00:15:36: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 5: Verify the SSH configuration.

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

```
S1# 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(config)# ip ssh time-out 90
S1(config)# ip ssh authentication-retries 2
```

Step 7: Save the running configuration to the startup configuration.

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

Task 2: Configure the SSH Client

PuTTy and Tera Term are two terminal emulation programs that can support SSHv2 client connections. This lab uses PuTTY.

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

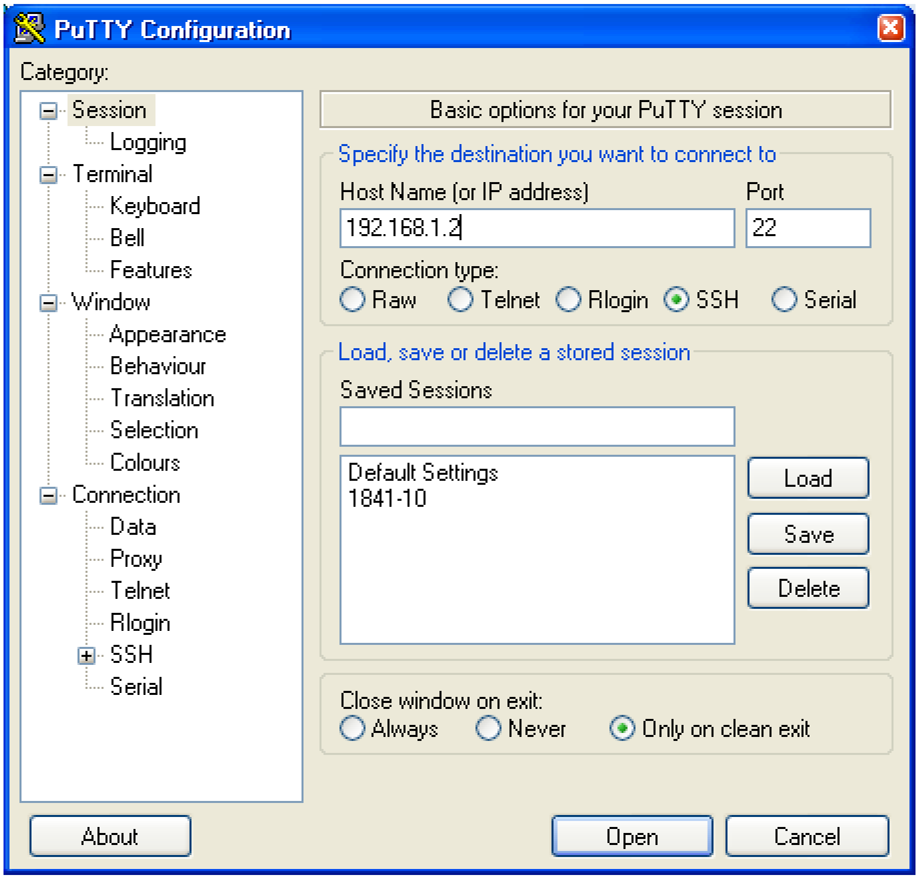
Note: The procedure described here is for PuTTY and pertains to PC-A.

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.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.2

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
1841-10

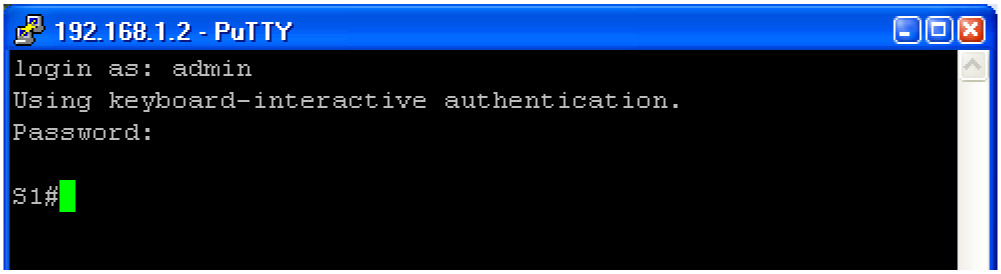
Close window on exit: ○ Always ○ Never ● Only on clean exit

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 the **admin** username and password **cisco12345**.



```
login as: admin
Using keyboard-interactive authentication.
Password:

S1#
```

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

```
S1# show users
```

What 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 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# 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, verify trunk configuration, and enable storm control for broadcasts on the trunk ports.

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 ones 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 purpose 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(config)# spanning-tree vlan 1 priority 0
S1(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 and to see the ports in use and their status.

```
S1# 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

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     001d.4635.0c80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

d. What is the S1 priority?

What ports are in use and what is their status?

Step 2: Configure trunk ports on S1 and S2.

a. Configure port Fa0/1 on S1 as a trunk port.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode trunk
```

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

b. Configure port Fa0/1 on S2 as a trunk port.

```
S2(config)# interface FastEthernet 0/1
S2(config-if)# switchport mode trunk
```

c. Verify that S1 port Fa0/1 is in trunking mode with the **show interfaces trunk** command.

```
S1# show interfaces trunk

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

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
```

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 Fa0/1 trunk interface?

   ____

b. Set the native VLAN on the S1 Fa0/1 trunk interface to an unused VLAN 99.

```
S1(config)# interface fa0/1
S1(config-if)# switchport trunk native vlan 99
S1(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 Fa0/1 trunk interface to VLAN 99.

```
S2(config)# interface fa0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

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

Setting the trunk port to not negotiate also helps to mitigate VLAN hopping by turning off the generation of DTP frames.

```
S1(config)# interface fa0/1
S1(config-if)# switchport nonegotiate

S2(config)# interface fa0/1
S2(config-if)# switchport nonegotiate
```

Step 5: Verify the trunking configuration on port Fa0/1.

```
S1# show interfaces fa0/1 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# 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: 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
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Step 6: Enable storm control for broadcasts.

Enable storm control for broadcasts on the trunk port with a **50** percent rising suppression level using the **storm-control broadcast** command.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# storm-control broadcast level 50

S2(config)# interface FastEthernet 0/1
S2(config-if)# storm-control broadcast level 50
```

Step 7: Verify your 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# show run | begin 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00

<output omitted>
```

Task 2: Secure Access Ports

By manipulating the STP root bridge parameters, network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology. 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 Fa0/5, the port to which R1 is connected, as access mode only.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# switchport mode access
```

b. On S1, configure Fa0/6, the port to which PC-A is connected, as access mode only.

```
S1(config)# interface FastEthernet 0/6
S1(config-if)# switchport mode access
```

Step 2: Disable trunking on S2 access ports.

On S2, configure Fa0/18, the port to which PC-B is connected, as access mode only.

```
S2(config)# interface FastEthernet 0/18
S2(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 enable some 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 to enable them to become active more quickly.

a. Enable PortFast on the S1 Fa0/5 access port.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree portfast
```

The following Cisco IOS warning message displays:

```
%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 FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Enable PortFast on the S1 Fa0/6 access port.

```
S1(config)# interface FastEthernet 0/6
S1(config-if)# spanning-tree portfast
```

c. Enable PortFast on the S2 Fa0/18 access ports.

```
S2(config)# interface FastEthernet 0/18
S2(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 ports previously configured as access only.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree bpduguard enable

S1(config)# interface FastEthernet 0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface FastEthernet 0/18
S2(config-if)# spanning-tree bpduguard enable
```

b. PortFast and BPDU guard can also be enabled globally with the **spanning-tree portfast default** and **spanning-tree 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 enabled with BPDU guard 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.

c. Verify that BPDU guard is configured by using the **show spanning-tree interface fa0/5 detail** command on S1.

```
S1# show spanning-tree interface fa0/5 detail

Port 5 (FastEthernet0/5) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.5.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.5, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 3349, received 0
```

Step 3: (Optional) Enable root guard.

Root guard is another option in helping to 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 Fa0/1 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 inter-switch connections.

```
S2(config)# interface gigabitEthernet 0/1
S2(config-if)# spanning-tree guard root
```

b. Issue the **show run | begin Gig** command to verify that root guard is configured.

```
S2# 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 goes into 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# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

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. If the superior BPDUs stop, the port returns to the forwarding state.

Task 4: Configure Port Security and Disable Unused Ports

Switches can be subject to CAM table, also known as 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 Fa0/0 MAC address.

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

```
R1# show interfaces fa0/1

FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256f (bia 001b.5325.256f)
  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, 100Mb/s, 100BaseTX/FX
```

What is the MAC address of the R1 Fa0/1 interface?

____

____

Step 2: Configure basic port security.

This procedure should be performed on all access ports that are in use. S1 port Fa0/5 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(config)# interface FastEthernet 0/5
```

b. Shut down the switch port.

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

c. Enable port security on the port.

```
S1(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 port-security 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(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(*xxxx.xxxx.xxxx* is the actual MAC address of the router Fast Ethernet 0/1 interface.)

Note: Optionally, you can 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(config-if)# no shutdown
```

Step 3: Verify port security on S1 Fa0/5.

a. On S1, issue the **show port-security** command to verify that port security has been configured on S1 Fa0/5.

```
S1# show port-security interface f0/5
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   : 001b.5325.256f:1
```

```
Security Violation Count   : 0
```

b. What is the status of the Fa0/5 port?

____

____

What is the Last Source Address and VLAN?

____

____

c. From the R1 CLI, ping PC-A to verify connectivity. This also ensures that the R1 Fa0/1 MAC address is learned by the switch.

```
R1# ping 192.168.1.10
```

d. You will 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(config)# interface FastEthernet 0/1
R1(config-if)# mac-address aaaa.bbbb.cccc
R1(config-if)# end
```

Note: You could also change the PC MAC address attached to S1 Fa0/6 and achieve similar results to those shown here.

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

____

____

f. On S1 console, observe the messages when port Fa0/5 detects the violating MAC address.

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5,
putting Fa0/5 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
```

g. On the switch, use the various **show port-security** command to verify that port security has been violated.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
      Fa0/5            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# show port-security interface fastethernet0/5
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# show port-security address
Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    001b.5325.256f    SecureConfigured              Fa0/5        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

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

```
R1(config)# interface FastEthernet 0/1
R1(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 Fa0/5 error disabled status.

a. From the S1 console, clear the error and re-enable the port using the following commands. This will change the port status from Secure-shutdown to Secure-up.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Note: This assumes the device/interface with the violating MAC address has been removed and replaced with the one originally configured.

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

```
R1# ping 192.168.1.10
```

Step 5: Remove basic port security on S1 Fa0/5.

From the S1 console, remove port security on Fa0/5. This procedure can also be used to re-enable the port, but **port security** commands must be reconfigured.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# no switchport port-security
S1(config-if)# no switchport port-security mac-address 001b.5325.256f
```

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

```
S1(config)# default interface fastethernet 0/5
S1(config)# interface FastEthernet 0/5
```

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

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

The following 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 the third IP address 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 Fa0/18:

```
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

Step 7: Disable unused ports on S1 and S2.

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

a. Ports Fa0/1, Fa0/5, and Fa0/6 are used on S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shut down.

```
S1(config)# interface range fa0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range Fa0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range gigabitethernet0/1 - 2
S1(config-if-range)# shutdown
```

b. Ports Fa0/1 and Fa0/18 are used on S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shut down.

```
S2(config)# interface range fa0/2 – 17 , fa0/19 – 24 , g0/1 - 2
S2(config-if-range)# shutdown
```

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

As a further security measure, you can move all active end user 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(config)# vlan 20
S1(config-vlan)# name Users

S2(config)# vlan 20
S2(config-vlan)# name Users
```

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

```
S1(config)# interface range fa0/5 - 6
S1(config-if-range)# switchport access vlan 20

S2(config)# interface fa0/18
S2(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.

To provide Telnet or 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. Enable trunking with subinterfaces on R1 to route 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 Fa0/6) and a host on another S1 port (e.g. port Fa0/7, which was previously shut down), you could use the **switchport protected** command to activate the PVLAN Edge feature on these two ports. To disable protected port, use the **no switchport protected** interface configuration command.

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

```
S1(config)# interface fastEthernet 0/6
S1(config-if)# switchport protected

S1(config-if)# interface fastEthernet 0/7
S1(config-if)# switchport protected
S1(config-if)# no shut
S1(config-if)# end
```

b. Verify that the PVLAN Edge Feature (protected port) is enabled on Fa0/6.

```
S1# show interfaces fa0/6 switchport
Name: Fa0/6
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 Fa0/6 and Fa0/7 using the following commands:

```
S1(config)# interface range fastEthernet 0/6 - 7
S1(config-if-range)# no switchport protected
```

Part 4: Configure SPAN and Monitor Traffic

Note: Cisco IOS provides a feature that can be used to monitor traffic in general and network attacks in particular, called the Switched Port Analyzer (SPAN). Cisco IOS supports local SPAN and remote SPAN (RSPAN). With local SPAN, the source VLANs, source switch ports, and the destination switch ports are on the same physical switch.

In this part of the lab, you will configure a local SPAN to copy traffic from one port where a host is connected to another port where a monitoring station is connected. The monitoring station will run the Wireshark packet sniffer application to analyze traffic.

Note: SPAN allows you to select and copy traffic from one or more source switch ports or source VLANs onto one or more destination ports.

Task 1: Option 1 - Configure a SPAN Session Using Hands-On Equipment.

Step 1: Configure a SPAN session on S1 with a source and destination.

a. Set the SPAN source interface using the **monitor session** command in global configuration mode. The following configures a SPAN source port on FastEthernet 0/5 for ingress and egress traffic. Traffic copied on the source port can be ingress only, egress only or both. S1 port Fa0/5 is connected to R1, so ingress traffic from R1 and egress to R1 on switch port Fa0/5 will be monitored.

```
S1(config)# monitor session 1 source interface fa0/5 both
```

Note: You can specify monitor tx (transmit) or rx (receive) traffic. The **both** keyword includes **tx** and **rx**. The source can be a single interface, a range of interfaces, a single VLAN, or a range of VLANs.

b. Set the SPAN destination interface.

```
S1(config)# monitor session 1 destination interface fa0/6
```

All traffic from S1 Fa0/5, where R1 is connected, will be copied to the SPAN destination port Fa0/6, where PC-A with Wireshark is connected.

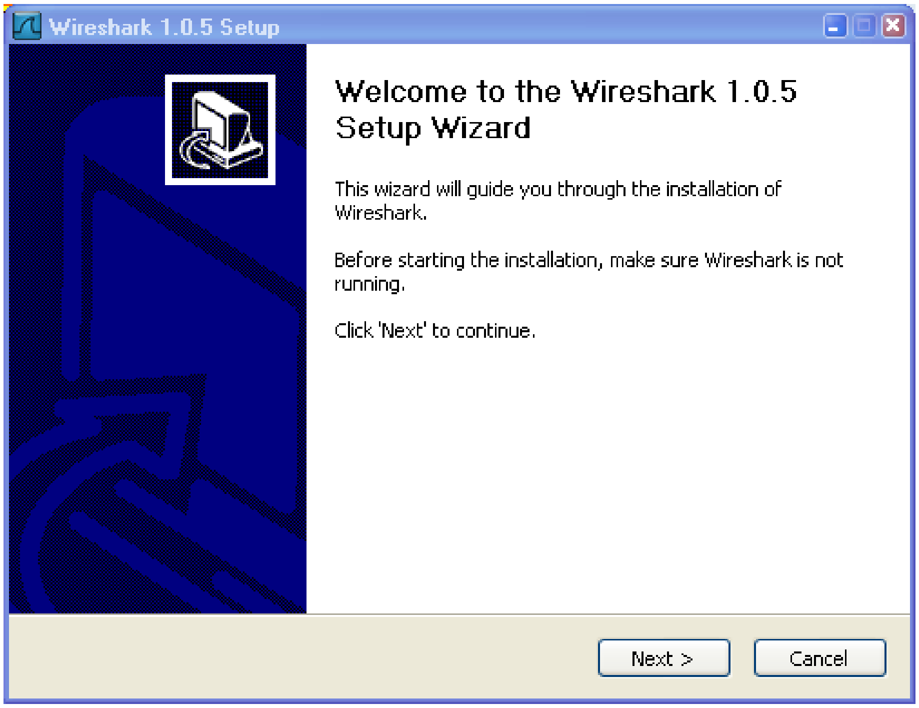
Note: The destination can be an interface or a range of interfaces.

Step 2: Verify the setup of the SPAN session on S1.

```
S1# show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/5
Destination Ports      : Fa0/6
    Encapsulation      : Native
          Ingress      : Disabled
```

Step 3: (Optional) Download and install Wireshark on PC-A.

a. Wireshark is a network protocol analyzer, also called a packet sniffer. If Wireshark is not currently available on PC-A, you can download the latest version from http://www.wireshark.org/download.html. This lab uses Wireshark version 1.0.5. The initial Wireshark installation screen is shown here.



Wireshark 1.0.5 Setup

Welcome to the Wireshark 1.0.5 Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

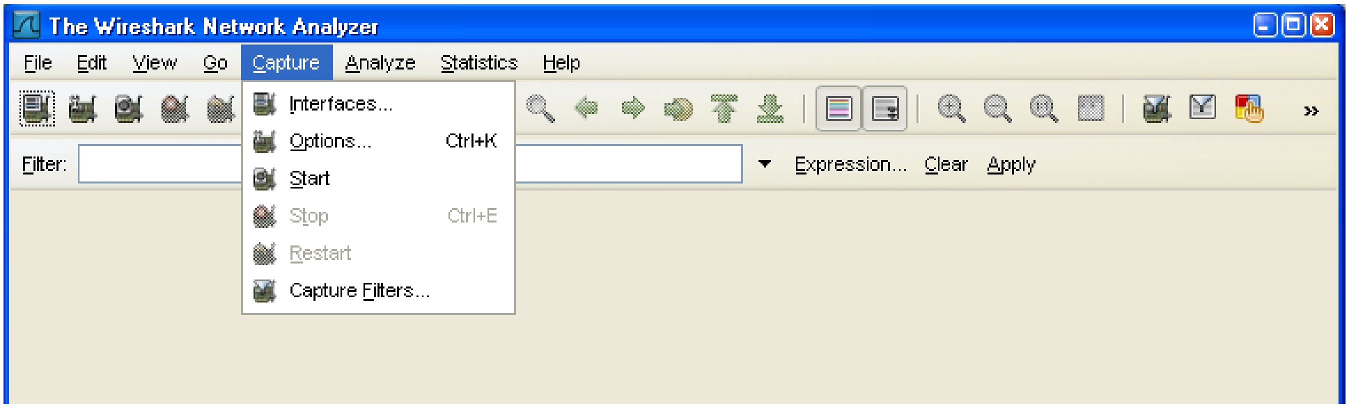
b. Click **I Agree** to the License agreement and accept the defaults by clicking **Next** when prompted.

Note: In the Install WinPcap screen, select the **install WinPcap** options, and select **Start WinPcap service** option to have other users besides those with administrative privileges run Wireshark.

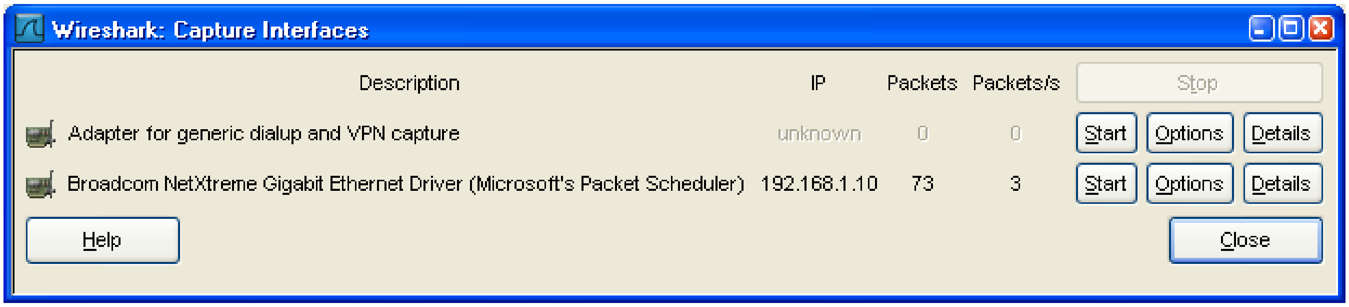
Step 4: Monitor S1 port Fa0/5 ping activity using Wireshark on PC-A.

a. If Wireshark is available, start the application.

b. On the main menu, click **Capture** > **Interfaces**.



c. Click **Start** for the LAN interface adapter with IP address 192.168.1.10.



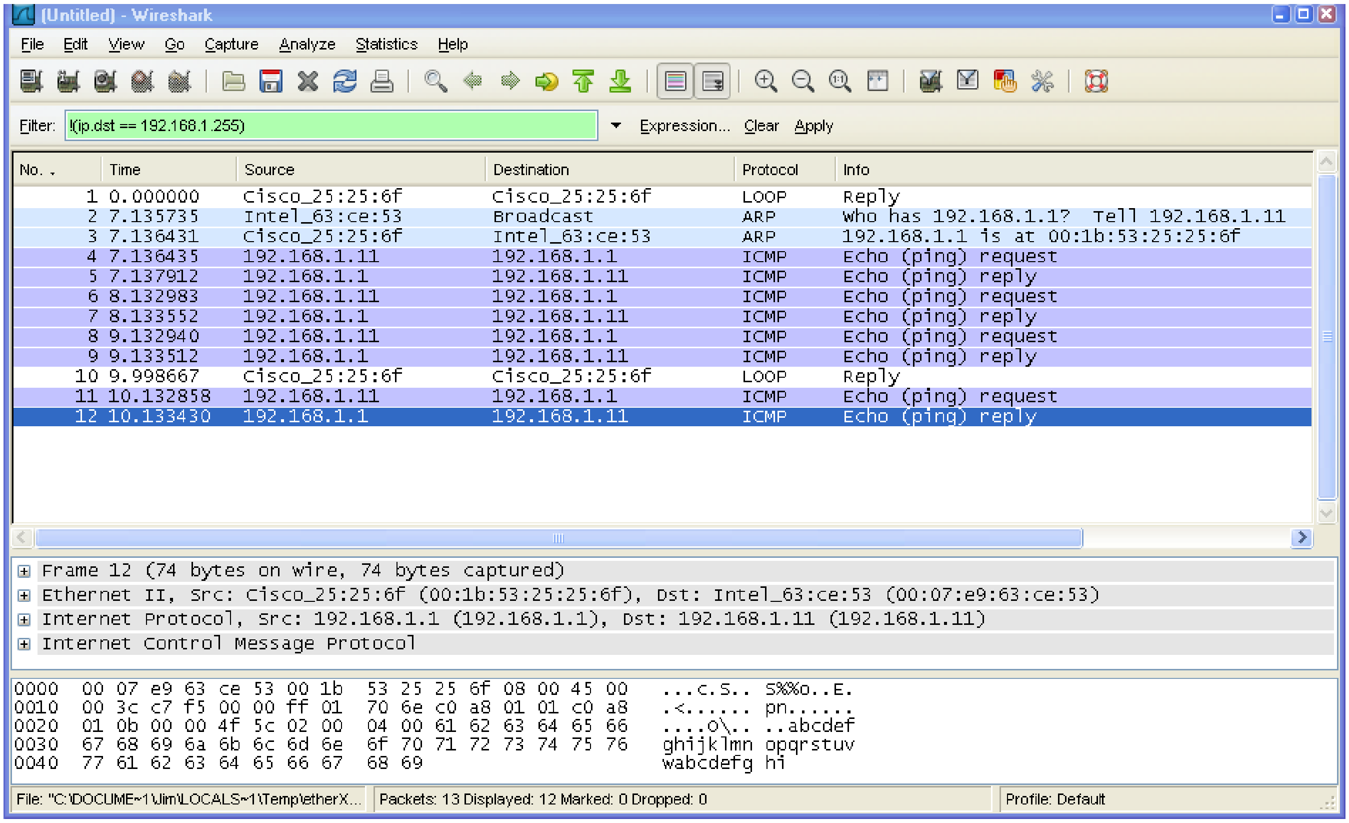
Description	IP	Packets	Packets/s
Adapter for generic dialup and VPN capture	unknown	0	0
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	192.168.1.10	73	3

d. Generate some traffic from PC-B (192.168.1.11) to R1 interface Fa0/1 (**192.168.1.1**) using **ping**. This traffic will go from S2 port Fa0/18 to S2 port Fa0/1 across the trunk link to S1 port Fa0/1, and then exit interface Fa0/5 on S1 to reach R1.

```
PC-B:\> ping 192.168.1.1
```

e. Observe the results in Wireshark on PC-A. If you have not pinged 192.168.1.1 before, you will see the initial ARP request broadcast from PC-B (Intel NIC) to determine the MAC address of the R1 Fa0/1 interface with IP address 192.168.1.1 and the ARP reply from the R1 Cisco Ethernet interface. After the ARP request, the pings (echo request and replies) can be seen going from PC-B to R1 and from R1 to PC-B through the switch. The filter **!(ip.dst == 192.168.1.255)** was applied to the Wireshark results.

Note: Your screen should look similar to the one below. Some additional packets might be captured in addition to the pings, such as the R1 Fa0/1 LOOP reply.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: !(ip.dst == 192.168.1.255)

```
No. .  Time        Source             Destination        Protocol  Info
     1 0.000000    Cisco_25:25:6f     Cisco_25:25:6f     LOOP      Reply
     2 7.135735    Intel_63:ce:53     Broadcast          ARP       Who has 192.168.1.1?  Tell 192.168.1.11
     3 7.136431    Cisco_25:25:6f     Intel_63:ce:53     ARP       192.168.1.1 is at 00:1b:53:25:25:6f
     4 7.136435    192.168.1.11       192.168.1.1        ICMP      Echo (ping) request
     5 7.137912    192.168.1.1        192.168.1.11       ICMP      Echo (ping) reply
     6 8.132983    192.168.1.11       192.168.1.1        ICMP      Echo (ping) request
     7 8.133552    192.168.1.1        192.168.1.11       ICMP      Echo (ping) reply
     8 9.132940    192.168.1.11       192.168.1.1        ICMP      Echo (ping) request
     9 9.133512    192.168.1.1        192.168.1.11       ICMP      Echo (ping) reply
    10 9.998667    Cisco_25:25:6f     Cisco_25:25:6f     LOOP      Reply
    11 10.132858   192.168.1.11       192.168.1.1        ICMP      Echo (ping) request
    12 10.133430   192.168.1.1        192.168.1.11       ICMP      Echo (ping) reply
```

```
⊞ Frame 12 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_25:25:6f (00:1b:53:25:25:6f), Dst: Intel_63:ce:53 (00:07:e9:63:ce:53)
⊞ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.11 (192.168.1.11)
⊞ Internet Control Message Protocol
```

```
0000  00 07 e9 63 ce 53 00 1b  53 25 25 6f 08 00 45 00   ...c.S.. S%%o..E.
0010  00 3c c7 f5 00 00 ff 01  70 6e c0 a8 01 01 c0 a8   .<...... pn......
0020  01 0b 00 00 4f 5c 02 00  04 00 61 62 63 64 65 66   ....O\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\DOCUME~1\Jim\LOCALS~1\Temp\etherX... | Packets: 13 Displayed: 12 Marked: 0 Dropped: 0 | Profile: Default

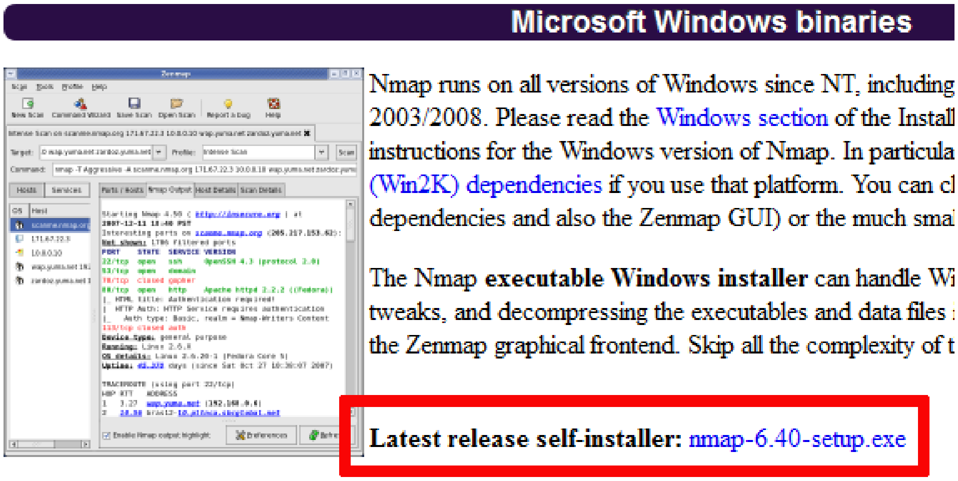
Step 5: Download and install Nmap/Zenmap.

Nmap/Zenmap is a network scanning tool which allows you to discover available hosts and resources. Zenmap is the graphical interface for Nmap. Nmap is used discovering what open ports exist on a network, including services, ports, operating systems, and other fingerprinting information. Nmap **should not** be used to scan networks without prior permission from the Network Administrator. The act of network scanning can be considered as a form of network attack.

a. If Nmap/Zenmap is not installed on PC-B, download **Nmap/Zenmap** from the following link:

http://nmap.org/download.html

b. Search for the appropriate binaries for your operating system.



Microsoft Windows binaries

Nmap runs on all versions of Windows since NT, including 2003/2008. Please read the Windows section of the Install instructions for the Windows version of Nmap. In particula (Win2K) dependencies if you use that platform. You can cl dependencies and also the Zenmap GUI) or the much smal

The Nmap **executable Windows installer** can handle Wi tweaks, and decompressing the executables and data files the Zenmap graphical frontend. Skip all the complexity of t

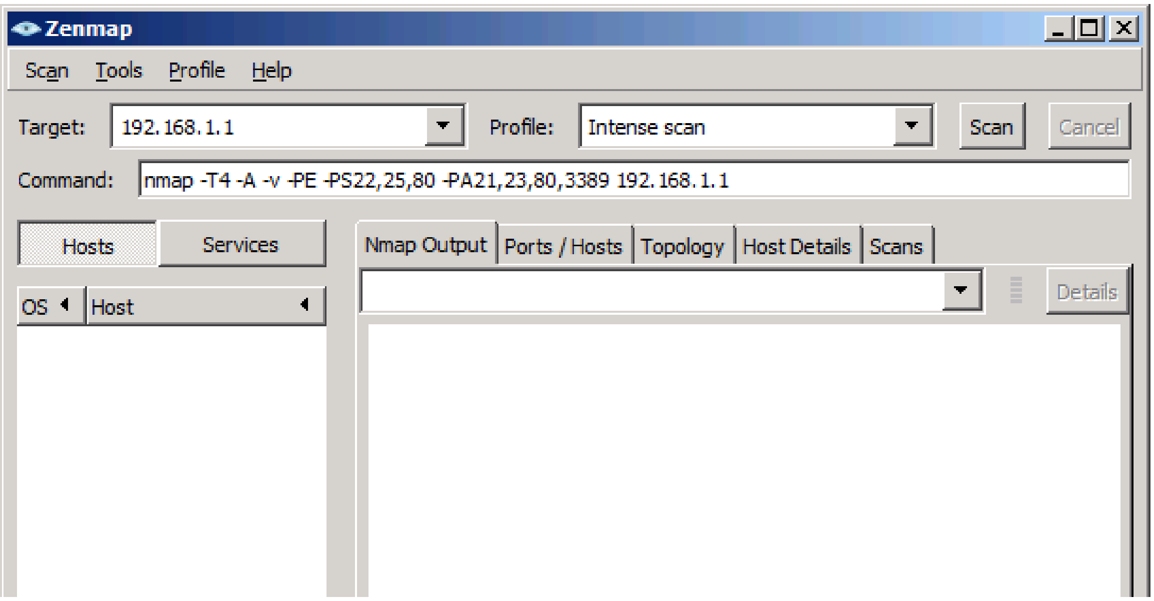
Latest release self-installer: nmap-6.40-setup.exe

c. Install **Nmap/Zenmap**.

Step 6: Monitor S1 port Fa0/5 Nmap activity using Wireshark on PC-A.

a. Start **Zenmap** on PC-B.

b. In the Target field, enter the IP address of R1 Fa0/1 (**192.168.1.1**).



Target: 192.168.1.1

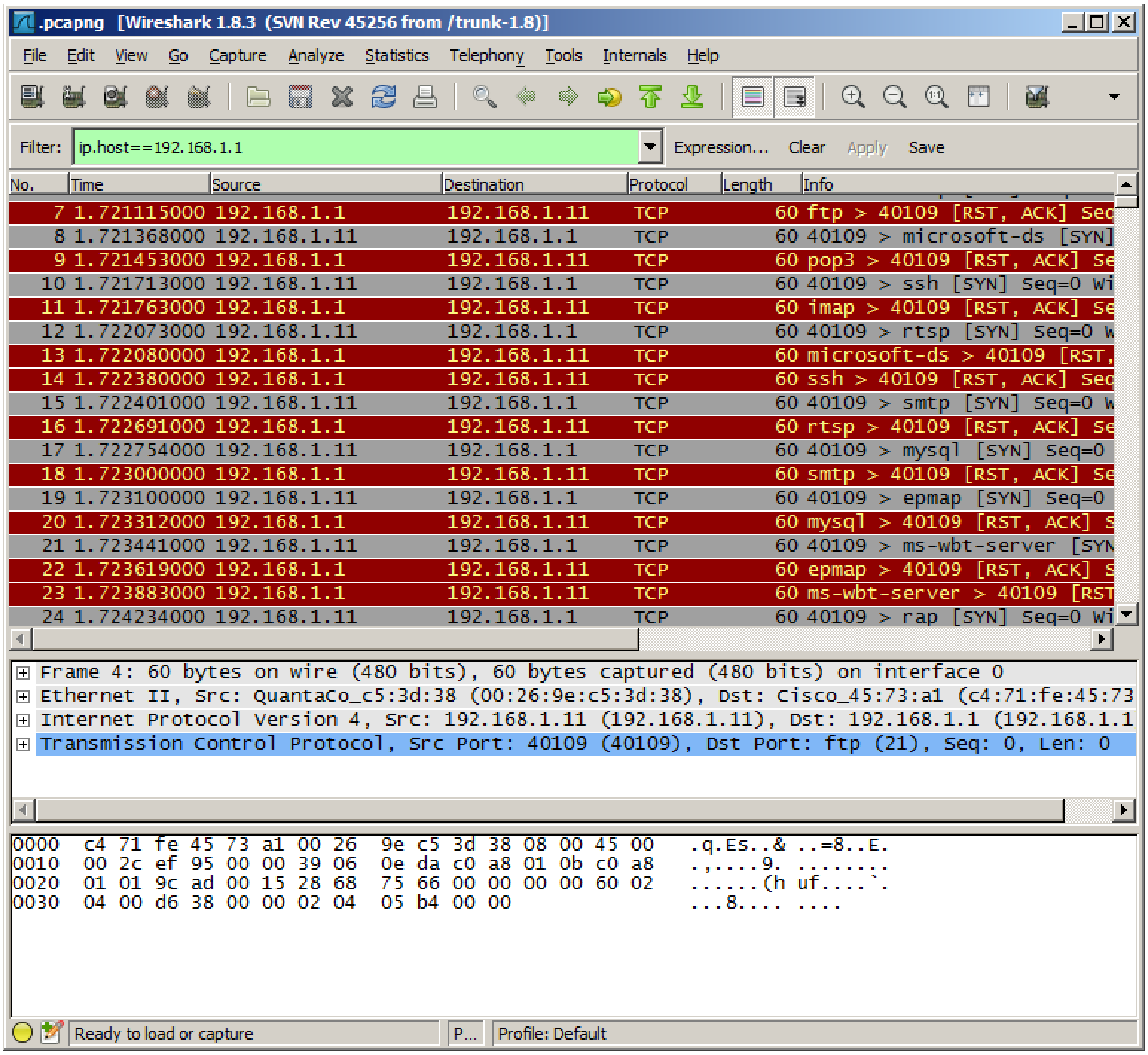
Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.1

c. Clear the previous capture in Wireshark and start a new capture by clicking **Capture** > **Start**. When prompted, click **Continue without saving**.

d. In the Zenmap program, click **Scan** to start the simulated attack.

e. Observe the results on the Wireshark window on PC-A. Notice the number and types of ports tried by the simulated Zenmap attack from PC-B (192.168.1.11) to R1 Fa0/1 (192.168.1.1). The filter, **ip.host==192.168.1.1**, was applied to the Wireshark result. Your screen looks similar to the following:


.pcapng [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Ready to load or capture
P...
Profile: Default

Filter: ip.host==192.168.1.1

```
No. Time        Source         Destination    Protocol Length Info
  7 1.721115000 192.168.1.1    192.168.1.11   TCP      60 ftp > 40109 [RST, ACK] Sec
  8 1.721368000 192.168.1.11   192.168.1.1    TCP      60 40109 > microsoft-ds [SYN]
  9 1.721453000 192.168.1.1    192.168.1.11   TCP      60 pop3 > 40109 [RST, ACK] Se
 10 1.721713000 192.168.1.11   192.168.1.1    TCP      60 40109 > ssh [SYN] Seq=0 Wi
 11 1.721763000 192.168.1.1    192.168.1.11   TCP      60 imap > 40109 [RST, ACK] Se
 12 1.722073000 192.168.1.11   192.168.1.1    TCP      60 40109 > rtsp [SYN] Seq=0 W
 13 1.722080000 192.168.1.1    192.168.1.11   TCP      60 microsoft-ds > 40109 [RST,
 14 1.722380000 192.168.1.1    192.168.1.11   TCP      60 ssh > 40109 [RST, ACK] Sec
 15 1.722401000 192.168.1.11   192.168.1.1    TCP      60 40109 > smtp [SYN] Seq=0 W
 16 1.722691000 192.168.1.1    192.168.1.11   TCP      60 rtsp > 40109 [RST, ACK] Se
 17 1.722754000 192.168.1.11   192.168.1.1    TCP      60 40109 > mysql [SYN] Seq=0
 18 1.723000000 192.168.1.1    192.168.1.11   TCP      60 smtp > 40109 [RST, ACK] Se
 19 1.723100000 192.168.1.11   192.168.1.1    TCP      60 40109 > epmap [SYN] Seq=0
 20 1.723312000 192.168.1.1    192.168.1.11   TCP      60 mysql > 40109 [RST, ACK] S
 21 1.723441000 192.168.1.11   192.168.1.1    TCP      60 40109 > ms-wbt-server [SYN
 22 1.723619000 192.168.1.1    192.168.1.11   TCP      60 epmap > 40109 [RST, ACK] S
 23 1.723883000 192.168.1.1    192.168.1.11   TCP      60 ms-wbt-server > 40109 [RST
 24 1.724234000 192.168.1.11   192.168.1.1    TCP      60 40109 > rap [SYN] Seq=0 Wi
```

```
⊞ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: QuantaCo_c5:3d:38 (00:26:9e:c5:3d:38), Dst: Cisco_45:73:a1 (c4:71:fe:45:73
⊞ Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1
⊞ Transmission Control Protocol, Src Port: 40109 (40109), Dst Port: ftp (21), Seq: 0, Len: 0
```

```
0000  c4 71 fe 45 73 a1 00 26  9e c5 3d 38 08 00 45 00   .q.Es..& ..=8..E.
0010  00 2c ef 95 00 00 39 06  0e da c0 a8 01 0b c0 a8   .,....9. ........
0020  01 01 9c ad 00 15 28 68  75 66 00 00 00 00 60 02   ......(h uf....`.
0030  04 00 d6 38 00 00 02 04  05 b4 00 00               ...8.... ....
```

Reflection

1. Why should port security be enabled on switch access ports?

____

____

2. Why should port security be enabled on switch trunk ports?

____

____

3. Why should unused ports on a switch be disabled?

____

____