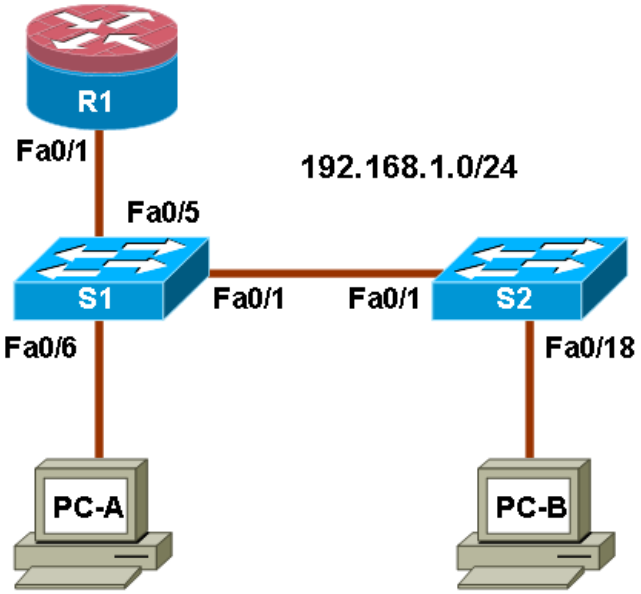
Network Forensics Lab 2- Secure Trunks and Access Ports



IP Address 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

In this lab, you 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 turn off 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 switches S1 or S2 as indicated.

Task 1: Secure Trunk Ports

Step 1: Configure switch S1 as the root switch.

For the purposes of this lab, assume that switch S2 is currently the root bridge and that switch S1 is preferred as the root switch. To force S1 to become the new root bridge, you configure a new priority for it.

a. From the console on S1, enter privileged EXEC mode and then global configuration mode.

b. The default priority for switches 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
```

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?

e. 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
```

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.

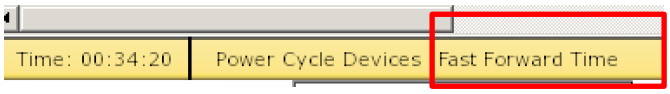
Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

a. From the output of the **show interfaces trunk** 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. On the main packet tracer interface click to FAST FORWARD TIME



d. The following message should be displayed 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?

e. 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 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 interface 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
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
```

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
```

c. 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 is displayed:

```
%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.

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.

```
S2(config)#interface Fastethernet 0/24
S2(config-if)#spanning-tree guard root
```

b. Issue the **show run** command and navigate to the Gigabit Interfaces section to verify that root guard is configured.

```
S2#sh run
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 fa0/24 detail** command.

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 also be subject to CAM table overflow, MAC spoofing attacks, and unauthorized connections to switch ports. In this task, you 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.

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

```
R1#show interface 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
```

b. 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. Switch S1 port Fa0/5 is shown here as an example.

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

a. From the switch 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: 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. Bring up 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 router 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 interface and shut it down.

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#shutdown
```

e. Configure a MAC address for the interface on the interface, using aaaa.bbbb.cccc as the address.

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

f. Enable the Fast Ethernet 0/1 interface.

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

g. From the router R1 CLI, ping PC-A. Was the ping successful? Why or why not?.

h. On switch 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
*Mar  1 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5,
changed state to down
```

i. On the switch, use the various **show port-security** commands 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
-------------------------------------------------------------------
-----

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        -
-------------------------------------------------------------------
------
```

j. On the router, shut down the Fast Ethernet 0/1 interface, 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)#shutdown
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown
```

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

k. 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.

a. 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 will need to be reconfigured.

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

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

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

Note: This **default interface** command also requires you to reconfigure the port as an access port in order 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. Two MAC addresses are allowed, and they are to be learned dynamically. One MAC address is for the IP phone, and the other 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.

This example is shown for switch 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 2
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address sticky
```

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 switch S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shutdown.

```
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 Fa0/18 and Gi0/1 are used on switch S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shutdown.

```
S2(config)#interface range Fa0/2 - 17
S2(config-if-range)#shutdown
S2(config-if-range)#interface range Fa0/19 - 24
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#interface gigabitethernet0/2
S2(config-if)#shutdown
```

Step 8: Move unused ports to an "Invalid" VLAN on S1 and S2.

As a further security measure, move any ports not being used on the switch into an invalid VLAN.

c. Ports Fa0/1, Fa0/5, and Fa0/6 are used on switch S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shutdown.

```
S1(config)# vlan 100
S1(config-vlan)# name unused
S1(config-vlan)# exit
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)#switchport access vlan 100
S1(config-if-range)#interface range gigabitethernet0/1 - 2
S1(config-if-range)#switchport access vlan 100
```

d. Ports Fa0/18 and Gi0/1 are used on switch S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shutdown.

```
S2(config)# vlan 100
S2(config-vlan)# name unused
S2(config-vlan)# exit
S2(config)#interface range Fa0/2 - 17
S2(config-if-range)#shutdown
S2(config-if-range)#interface range Fa0/19 - 24
S2(config-if-range)#switchport access vlan 100
S2(config-if-range)#interface gigabitethernet 0/2
S2(config-if-range)#switchport access vlan 100
```

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)#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.

If you need 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. You would also need to enable trunking with subinterfaces on R1 to route between the management and user VLAN subnets.