

Advanced Switch Level 2 Features

1 Introduction

This lab will explore additional Level 2 (Data Link) switch features. Lab5 introduced one such feature, namely VLANs. Additional features such as Spanning Tree Protocol (STP), VLAN Trunk Protocol (VTP), and switch monitoring are explored here.

2 Network Switch

2.1 VLAN

Extend what you learned in Lab5 by activating the Switch IP address on VLAN1, making sure it's not in a shutdown state with the show conf command. Attach the Windows host and Linux host to a VLAN1 ports. (As always, it's a good idea to "write erase", "reload" to start from a clean configuration)

Verify network connectivity

(If the Linux host cannot ping the Windows host on VLAN1, make sure the switch is setup with an IP address on VLAN1 and on subnet 10.10X.0/24. If another class has misconfigured the Linux host, you can modify it back with the instructions below:)

Log in to the Linux host using username misy, password misy and open up a terminal. Run the following command to change the Linux host's IP address to 10.10X.0.2. (sudo password is also misy)

```
misy@localhost ~ $ sudo /sbin/ifconfig eth0 10.106.0.2 netmask  
255.255.255.0
```

You should be able to ping the Switch from both the Vista host and the Linux host when configured correctly.

Run Wireshark (Lab 3) on the Vista host while you PING the switch from the Vista host. Can you see your PING (ICMP) packets in Wireshark?

PING the Vista host from the Linux host; can you see your PING packets in Wireshark?

Finally, PING from the Linux host to the Switch, can you see your PING packets in Wireshark? Explain.

2.2 SPAN Monitor

One management problem that became troublesome with switches, then compounded with VLANs, is the monitoring of packets on networks. Since switch ports and VLANs naturally separate traffic between them, using a packet sniffer (wireshark, etc.) became an impossible or manual process. The Cisco SPAN protocol answered these issues by allowing a single port to capture all traffic on any single or group of VLANs. Set up a Switch SPAN connection, on the switch port that the Vista host is attached to, monitoring all the other ports.

2.2.1 Creating a SPAN Session with the CLI and Specifying Ports to Monitor

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) and destination (monitoring) ports:

Step 1 `configure terminal` Enter global configuration mode.

Step 2 `no monitor session all` Clear any existing SPAN configuration for the session.

Step 3 `monitor session session_number source interface interface-id(s)`
Specify the SPAN session and the source port (monitored port).

For *session_number*, specify 1.

For *interface-id*, specify the source port to monitor. (ie. FastEthernet0/2)

(Optional) [, | -] Specify a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen.

Step 4 `monitor session session_number destination interface interface-id`
Specify the SPAN session and the destination port (monitoring port).

For *session_number*, specify 1.

For *interface-id*, specify the destination port.

Repeat the last experiment from section 2.1, now with the SPAN port, and report your findings and explanations.

2.3 VLAN Trunking

The VLAN Trunk Protocol can be used to propagate VLAN information throughout the network. With only one switch in the network, not much will happen, but you can configure it like below because it has ancillary effects on other operations.

2.3.1 Configuring a Trunk Port with CLI

Beginning in privileged EXEC mode, follow these steps to configure a port as 802.1Q trunk port:

Step 1 `configure terminal` Enter global configuration mode.

Step 2 `interface interface-id` Enter the interface configuration mode and the port (*interface-id*) to be configured for trunking.

Step 3 `switchport mode trunk`

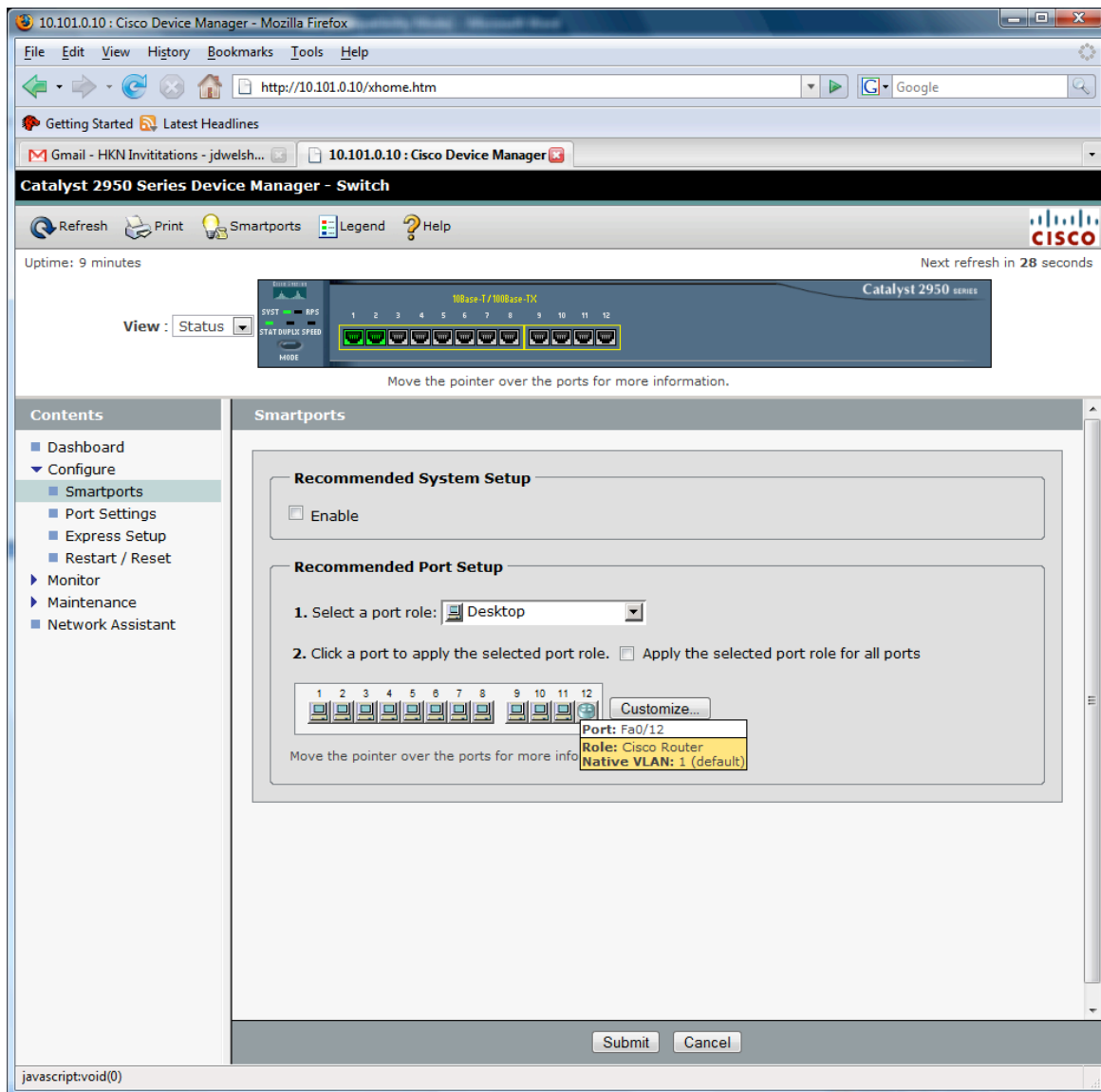
Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode).

Step 4 `switchport access vlan vlan-id` (Optional) Specify the default VLAN, which is used if the interface stops trunking.

Step 5 `switchport trunk allowed vlan {add | all | except | remove} vlan-list`
(Optional) Configure the list of VLANs allowed on the trunk.

Step 6 `switchport trunk native vlan vlan-id` Specify the native VLAN.

If using the CMS, you may create a trunk by navigating to configure->smartports and designating the desired port as a Cisco router, screenshot below.



VLAN Trunks allow many different VLANs to be transported over a single link. Since each VLAN may have to attach to a router and there may be tens or hundreds of VLANs, a trunk can substantially reduce the numbers of router ports needed in a network. Cisco developed a proprietary trunk protocol named Inter-Switch Link (ISL) and later, an IEEE standard 802.1q was released. Cisco usually supports both protocols, but both ends of the trunk must use the same one.

Configure port1 on the switch as a trunk. Use the 802.1q standard for the trunk and permit only VLAN1 and VLAN2 to transport over the trunk (you need to use the CLI to accomplish this).

Configure the server onto the 10.10X.0/24 subnet and place it into a VLAN2 port. Can the Host ping the server in VLAN2? Why/Why Not? If it can not, what additional piece of equipment might be needed?

How do Trunking and the SPAN protocol differ? How are they similar?

2.4 STP

The Spanning Tree Protocol (STP) is required on switches when there exists the possibility of multiple paths between hosts. STP monitors stations addresses as they enter, and maintains a single path to each station so possible loops cannot develop. STP should be enabled separately on each VLAN, because they each are independent logical networks and loops could still occur. STP is usually on by default.

IOS CLI spanning tree status command:

```
Switch#show spanning-tree
```

2.5 Extension – Operational STP (Optional)

Configure Router1 at your station using the same setup procedure used to configure the switch. (You should “write erase” and “reload” the router to a clean starting point, just like the Switch)

```
Router1#setup
```

```
--- System Configuration Dialog ---
```

```
Continue with configuration dialog? [yes/no]: yes
```

```
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].
```

```
Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system
```

```
Would you like to enter basic management setup? [yes/no]: yes  
Configuring global parameters:
```

```
Enter host name [Router1]: Router1
```

```
The enable secret is a password used to protect access to  
privileged EXEC and configuration modes. This password, after  
entered, becomes encrypted in the configuration.  
Enter enable secret [<Use current secret>]: 123
```

```
The enable password is used when you do not specify an  
enable secret password, with some older software versions, and  
some boot images.  
Enter enable password [123]: 123
```

```
% Please choose a password that is different from the enable secret
Enter enable password [123]: 123
```

```
The virtual terminal password is used to protect
access to the router over a network interface.
```

```
Enter virtual terminal password [123]: 123
Configure SNMP Network Management? [no]: no
```

```
Current interface summary
```

Interface Protocol	IP-Address	OK?	Method	Status
Ethernet0/0 down down	unassigned	YES	manual	administratively
FastEthernet0/0 down down	unassigned	YES	manual	administratively
FastEthernet1/1 up	unassigned	YES	unset	up
FastEthernet1/2 up	unassigned	YES	unset	up
FastEthernet1/3 down down	unassigned	YES	unset	administratively
FastEthernet1/4 down down	unassigned	YES	unset	administratively
Vlan1 up	10.102.0.1	YES	manual	up

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

```
Configuring interface Vlan1:
```

```
Configure IP on this interface? [yes]: yes
IP address for this interface [10.102.0.1]: 10.102.0.1
Subnet mask for this interface [255.0.0.0] : 255.255.255.0
Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

```
The following configuration command script was created:
```

```
hostname Router1
enable secret 5 $1$bLf.$ZX0V7dORkRw1pWRkr8TIg1
enable password 123
line vty 0 4
password 123
no snmp-server
!
no ip routing

!
interface Ethernet0/0
shutdown
no ip address
!
interface FastEthernet0/0
shutdown
no ip address
!
interface FastEthernet1/1
```

```
shutdown
no ip address
!
interface FastEthernet1/2
shutdown
no ip address
!
interface FastEthernet1/3
shutdown
no ip address
!
interface FastEthernet1/4
shutdown
no ip address
!
interface Vlan1
no shutdown
ip address 10.102.0.1 255.255.255.0
!
end
```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

```
Enter your selection [2]:2
Router1#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface FastEthernet 1/1
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet 1/2
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet 1/3
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet 1/4
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#exit
```

Connect the Linux host to one of the ports of the 4-port ethernet switch on Router 1 using a crossover cable. Try connecting a cross-over cable between VLAN1 ports of your Catalyst 2950 switch, with VLAN1 ports of the 4-port Ethernet switch on Router1, and continually PING (-t flag) between Vista host and the Linux host. Continue the PINGs and add a second cross-over cable between VLAN1 ports and see if any STP notices are posted to the switch consoles? Notice any indications on the switch port LEDs of the cross-over cables or console notices. Finally, disconnect the first cross-over cable (should have a green LED on both ends) while still PINGing and observe what happens, usually within 5min of disconnecting the cable.