Layer 2 Network Design Lab

Introduction

The purpose of these exercises is to build intra-building Layer 2 networks utilizing the concepts explained in today's design presentations. The exercises are focused on the 2nd layer of the OSI model, that is, switching. Students will see how star topology, aggregation, Virtual LANs, Spanning Tree Protocol, Port bundling and some switch security features are put to work.

The lab exercises will include:

1. Basic switch configuration
2. Spanning Tree configuration
3. Redundant configuration
4. Control Plane Protection configuration
5. Port Bundling
6. MST Configuration
7. DHCP Snooping

There will be 5 groups of 4-6 students, with 4 switches per group. The distribution of IP address space for the building (Layer 2) networks will be as follows:

- Group 1: 10.10.10.0/24
- Group 2: 10.20.10.0/24
- Group 3: 10.30.10.0/24
- Group 4: 10.40.10.0/24
- Group 5: 10.50.10.0/24

Switch types used in the LAB

Modular Switches

- Hewlett Packard Procurve Switch 4000 (J4121A)
- Hewlett Packard Procurve Switch 4104gl (J4887A)

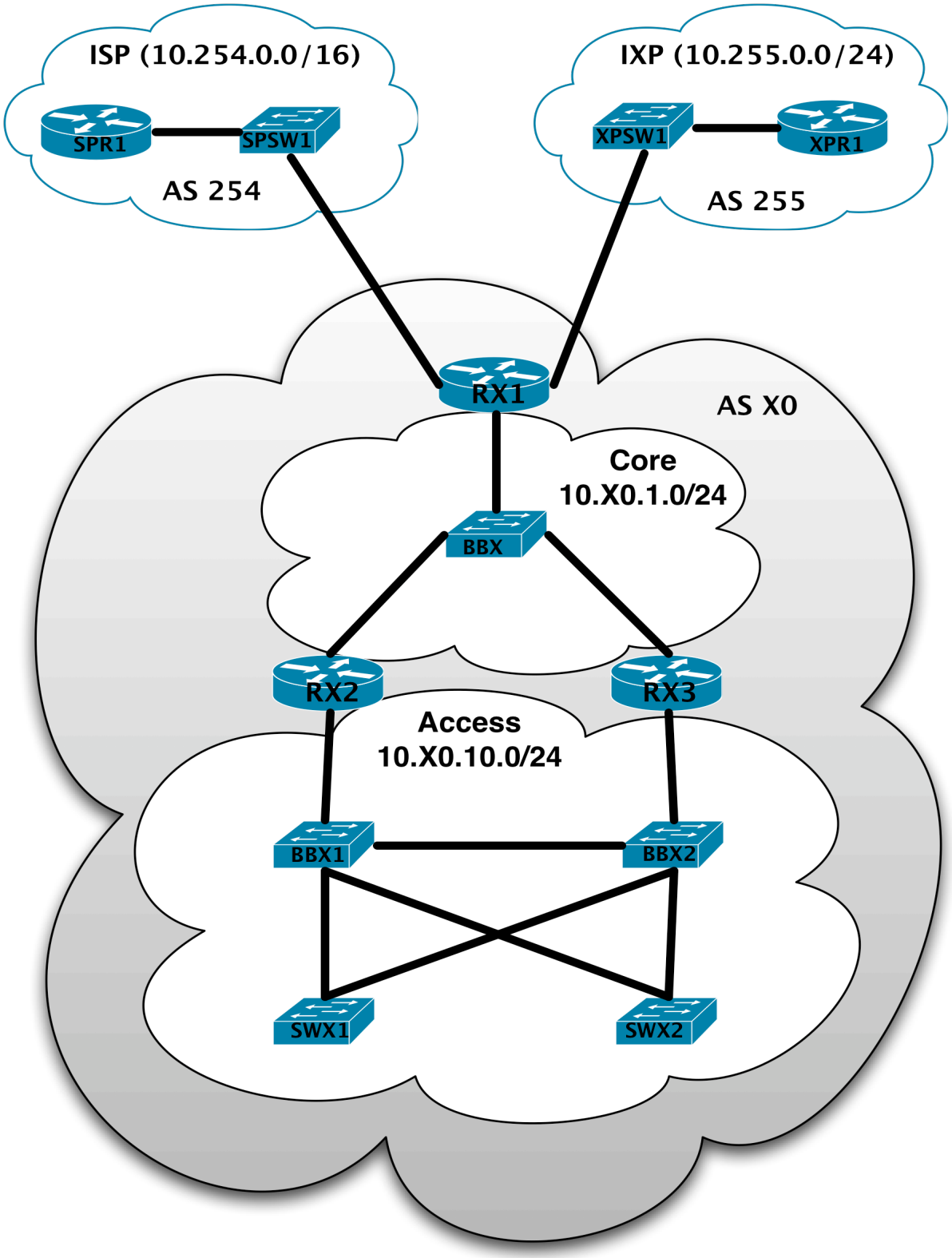
Standalone Switches

- Hewlett Packard Procurve Switch 2824 (J4903A)

Brief introduction to switch configuration

See Appendix A

Network Diagram



X = Refers to your group number (1-5)

Spanning Tree Design Information

Priority Matrix

Multiplier	Priority Value	Description	Notes
0	0	Core Node	The core switches/routers will not be participating in STP...defined in case they ever are
1	4096	Redundant Core Nodes	The core switches/routers will not be participating in STP...defined in case they ever are
2	8192		Reserved
3	12288	Building Backbone	
4	16384	Redundant Building Backbones	
5	20480	Secondary Backbone	This is for building complexes, where there are separate building (secondary) backbones that terminate at the complex backbone.
6	24576	Access Switches	This is the normal edge-device priority.
7	28672	Access Switches	Used for access switches that are daisy-chained from another access switch. We're using this terminology instead of "aggregation switch" because it's hard to define when a switch stops being an access switch and becomes an aggregation switch.
8	32768	Default	No centrally managed network devices should have this priority.

Cisco / HP STP Protocol Version Compatibility Table

Cisco 6509 Mode	Switch Type	Switch Protocol	Switch Force Protocol (HP only)	Does it work?
Mst	HP 2824	stp	stp	yes
Mst	HP 2824	rstp	stp	yes
Mst	HP 2824	rstp	rstp	yes
Mst	HP 2824	mst	mst	yes
Mst	HP 4000M	stp	N/A	yes
Mst	C 3560	any	N/A	yes
Mst	HP 4104gl	stp	stp	yes
Mst	HP 4104gl	rstp	stp	yes
Mst	HP 4104gl	rstp	rstp	yes
Mst	HP 2810	mst	stp	yes
Mst	HP 2810	mst	rstp	yes
Mst	HP 2810	mst	mst	yes
Mst	HP 2524	stp	stp	yes
Mst	HP 2524	rstp	stp	yes
Mst	HP 2524	rstp	rstp	yes
Mst	HP 2524	rstp	rstp	yes
Mst	HP 2524	rstp	rstp	yes
pvst+	Non Cisco - Non-trunking	any	any	**no**
rapid-pvst+	Non Cisco - Non-trunking	any	any	**no**

Compatibility Matrix

	c6500	c3750	c3560	c2960	hp1600m	hp224	hp2400m/2424m	hp2512/2524	hp2600-8/2626/2650	hp2810
Switch Feature										
STP	pvst+	pvst+	pvst+	pvst+	x	x	x	x	x	x
RSTP	rapid-pvst	rapid-pvst+	rapid-pvst+	Rapid-pvst+				x	x	x
MST	x	x	x	x					x	x
Root Guard	x	x	x	x					x	x
BPDU Filter	x	x	x	x					x	x
BPDU Guard	x	x	x	x					x	x
Portfast	x	x	x	x	x	x	x	x	x	x
Storm Control	x	x	x	x	bcast limit		bcast limit	bcast limit	bcast-limit (per switch)	bcast-limit
UDLD	x	x	x	x					link-keepalive	
Loopguard	x	x	x	x					x	x
Dhcp-snooping	x	x	x	x					x	
Arp-protect	x	x	x	x					x	
IPv6 support	x	x	x	x						

	hp2824/2848	Hp2900-24/48	hp3500yl	hp4000m/8000m	hp4104/4108gl	hp4208vl	hp5304xl	hp6108
Switch Feature								
STP	x	x	x	x	x	x		x
RSTP	x	x	x		x	x	x	
MST	x	x	x			x		
Root Guard	x	x	x			x	unknown	
BPDU Filter	x	x	x			x	x	
BPDU Guard	x	x	x			x	x	
Portfast	x	x	x	x	x	x	unknown	x
Storm Control	bcast-limit	Bcast-limit	bcast-limit	bcast limit	bcast limit (per switch)	bcast-limit (per switch)	unknown	bcast-limit (per switch)
UDLD	link-keepalive	Link-keepalive	link-keepalive			link-keepalive	link-keepalive	
Loopguard	x	x	x			x	x	
dhcp-snooping	x	x	x			x	x	
arp-protect	x	x	x			x	x	
IPv6 support		x	x				unknown	unknown

Note: This table assumes that all of the switches are using the most recent firmware version (as of 10/30/2007).

Note: broadcast-limiting on the HPs refers to non-unicast packets, i.e. the sum of broadcast and multicast packets on an interface. The action is to drop the packets.

Note: storm-control on the Cisco devices, depending on the ios, operates per multicast, broadcast or unicast. I.e. they can have separated thresholds. There are different actions to take when the threshold is hit. 1) send an snmp trap and block the traffic, 2) shutdown the port, 3) no alerts and drop the packets.

Exercises

1. Upgrade the system firmware to the latest version available for the switch type to be used for the lab. Your instructor will provide the IP address of the TFT server and the name of the image to be used.
    a. Connect to the console port of your assigned switch using the console cable provided
    b. Assign and IP address to the VLAN 1 interface (see "Vlan 1" section of Appendix B for your switch type)
    c. Execute the download command (see Appendix A for syntax)
        - Show menu option if available
    d. Reload the system for the firmware to be installed

2. The first goal is to build a hierarchical switched network, so you will use one switch as your aggregation (or backbone) switch, and connect two access switches to it. Follow these instructions to configure each switch:

    a. The initial configuration for the backbone and edge switches can be found in Appendix B (select the appropriate switch configuration)
    b. Notice the lines with IP addresses and replace the "X" with the corresponding octet from your group's IP prefix. Don't forget to assign each switch a different IP address:
        - Aggregation switch: 10.X0.10.4
        - Access switch 1: 10.X0.10.6
        - Access switch 2: 10.X0.10.7
    c. Connect port 24 (A24 on modular switches) of each access switch to ports 19 and 20 (A19 and A20 on modular switches) on the aggregation switch
    d. Configure IP addresses in you laptops and connect them to the access switches.
        - PC 1: 10.X0.10.50 connected to port 15 (A15 on modular switches) on access switch 1
        - PC 2: 10.X0.10.51 connected to port 15 (A15 on modular switches) on access switch 2
    e. Verify connectivity by pinging each laptop and switch. You should also be able to ssh to each switch as 'admin'.

3. Take one patch cord and connect each end to two of the edge switches. What happens?
    a. Using your connection to the switch console, monitor the logs and watch the switch LEDs.
    b. Test connectivity from two edge machines using Ping.

4. We will now configure the **Spanning Tree Protocol** across all our switches.
    a. Use the configuration files in Appendix C.
    b. What is the main difference between the configurations of the backbone switch and the edge switches?
    c. Verify port roles and status
    d. Repeat the procedures in item 3. What happens now?
    e. Remove the loop

f. Connect a computer to one of the edge ports. How long does it take to become active?
   - Change the Spanning Tree Protocol version to RSTP on all switches
   - Repeat the same test. How long does it take now?

5. What happens to the network if the aggregation switch dies? Let's now add **redundancy**.
   a. Add a second aggregation switch.
   b. Use the address 10.X0.10.5.
   c. Configure Spanning Tree with a priority of "3" on the second aggregation switch
   d. Connect port 23 (A23 on modular switches) from each edge switch to ports 19 and 20 (A19 and A20 on modular switches) on the second aggregation switch.
   e. Connect the aggregation switches to each other on port 24 (A24 on modular switches).
   f. Verify who is the root and explain why
   g. Verify port roles and status. Which ports are blocking?
   h. How can you guarantee that the first aggregation switch stays as the SPT root?
   i. Turn off the first aggregation switch.
   j. Who is the root now? Verify port roles and status. Verify connectivity.
   k. Bring back the first aggregation switch
   l. Disable spanning tree in one of the aggregation switches. What happens?

6. We now want to protect the control plane of our switched network by separating the user traffic from the management traffic.
   a. Use the configurations in Appendix D to create a **management VLAN**.
   b. Remove the IP addresses from VLAN 1
   c. Verify connectivity between switches using the console connections
   d. From the laptops, try pinging any of the switches

7. We now want more capacity and link redundancy between the aggregation switches
   a. Use Appendix E to configure **Port Bundling**.
   b. What capacity do you have now?
   c. Remove one of the links in the bundle. What happens?

8. Suppose you wanted to load balance the traffic from the two VLANs across both aggregation switches. How can you achieve this? **(Only done if MSTP is supported).**
   a. Configure MSTP using Appendix F.
   b. Verify status of each spanning tree instance. Notice the differences in port roles and status on the different instances.

9. If available, configure a computer as a DHCP server and connect it into one of the edge ports. Connect a second computer to another switch and check if you can get an IP address assigned. What happens if your users do this without your consent**? (Only done if DHCP Snooping is supported).**
   a. Use the instructions in Appendix G to configure Rogue **DHCP prevention**.
      - Can the client computer get an address now?
      - Follow the rest of the instructions to make it work with a legitimate DHCP server.

Appendix A - HP 28XX/410X CLI relevant commands

```
show config
show running-config [status]
show interfaces [brief] [config]
show system-information
show interfaces brief
show interfaces [port]
show ip
show flash
show spanning-tree [detail]
show vlan <vlan-id>
show lacp
show cdp neighbors
show lldp info remote-device
copy tftp flash <TFTP_SERVER> <IMAGE_FILE> primary
configure
password manager user-name admin
end
write mem
reload
```

Appendix B - Basic switch configuration (HP2800)

```
hostname "switch"
snmp-server contact "network services"
time timezone -480
time daylight-time-rule Continental-US-and-Canada
lldp run
cdp run
sntp server 128.223.32.35
sntp server 128.223.60.22
ip icmp burst-normal 20
ip icmp reply-limit
ip ttl 6
timesync sntp
sntp unicast
snmp-server community "public" manager restricted
snmp-server host 10.X0.10.100 "public" Not-INFO
snmp-server enable traps authentication
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address 10.X0.10.Y 255.255.255.0
```

```
   ip igmp
exit
fault-finder broadcast-storm sensitivity low
ip authorized-managers 10.X0.0.0 255.255.0.0
no dhcp-relay
crypto key generate ssh rsa
ip ssh
ip ssh key-size 1024
ip ssh port default
interface all
   no lacp
exit
no telnet-server
```

Appendix B - Basic switch configuration (HP4100)

```
hostname "switch"
snmp-server contact "network services"
time timezone -480
time daylight-time-rule Continental-US-and-Canada
lldp run
cdp run
no web-management
; web-management ssl
sntp server 128.223.60.22
sntp server 128.223.32.35
ip icmp burst-normal 20
ip icmp reply-limit
ip ttl 6
timesync sntp
sntp unicast
snmp-server community "public" manager restricted
snmp-server host 10.X0.10.100 "public" Not-INFO
snmp-server enable traps authentication
vlan 1
   name "DEFAULT_VLAN"
   ip address 10.X0.10.Y 255.255.255.0
   ip igmp
   exit
fault-finder broadcast-storm sensitivity low
ip authorized-managers 10.X0.0.0 255.255.0.0
no dhcp-relay
crypto key generate ssh rsa
ip ssh
ip ssh key-size 1024
```

```
ip ssh port default
interface all
  no lacp
exit
no telnet-server
```

Appendix C - Spanning Tree Configuration

```
spanning-tree
spanning-tree protocol-version STP
spanning-tree priority 6
```

* For the first aggregation switch, use priority 3

Appendix D - Management VLAN

- On the aggregation switches:

```
vlan 255
  name "MGMT"
  tagged 19-20
  tagged 24
  ip address 10.X0.255.Y 255.255.255.0
exit
```

- On the access switches:

```
vlan 255
  name "MGMT"
  tagged 23-24
  ip address 10.X0.255.Y 255.255.255.0
exit
```

Appendix E - Port Bundling

- On the Aggregation switches only:

```
interface 23
  lacp active
interface 24
  lacp active
```

- On all switches:
  spanning-tree protocol-version MSTP
  write mem
  reload

- On the first aggregation switch:
  spanning-tree config-name "mstp1"
  spanning-tree config-revision 1
  spanning-tree instance 1 vlan 1
  spanning-tree instance 1 priority 0
  spanning-tree instance 2 vlan 255
  spanning-tree instance 2 priority 2

- On the second aggregation switch:
  spanning-tree config-name "mstp1"
  spanning-tree config-revision 1
  spanning-tree instance 1 vlan 1
  spanning-tree instance 1 priority 2
  spanning-tree instance 2 vlan 255
  spanning-tree instance 2 priority 0

- On the access switches:
  spanning-tree config-name "mstp1"
  spanning-tree config-revision 1
  spanning-tree instance 1 vlan 1
  spanning-tree instance 2 vlan 255

- On the first aggregation switch:
  spanning-tree
  spanning-tree protocol-version rstp
  spanning-tree priority 3

- On the second aggregation switch:
  spanning-tree
  spanning-tree protocol-version rstp
  spanning-tree priority 4

- On the access switches:
  spanning-tree
  spanning-tree protocol-version rstp
  spanning-tree priority 6

Appendix G - Rogue DHCP prevention

```
dhcp-snooping
no dhcp-snooping option 82
no dhcp-snooping verify mac
dhcp-snooping option 82 untrusted-policy keep
interface <number> dhcp-snooping trust
```

Appendix H – AAA Configuration

```
no aaa authentication login privilege-mode
aaa authentication console login radius local
aaa authentication console enable local none
aaa authentication telnet login radius local
aaa authentication telnet enable local none
aaa authentication web login radius local
aaa authentication web enable local none
aaa authentication ssh login radius local
aaa authentication ssh enable local none
aaa accounting exec start-stop radius
aaa accounting commands stop-only radius
radius-server dead-time 5
radius-server timeout 3
radius-server retransmit 1
radius-server key verycomplexkey
radius-server host 128.223.60.91
radius-server host 128.223.60.92
```