Layer 2 Network Design Lab

Introduction

The purpose of these exercises is to build Layer 2 (switched) networks utilizing the concepts explained in today's design presentations. 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:

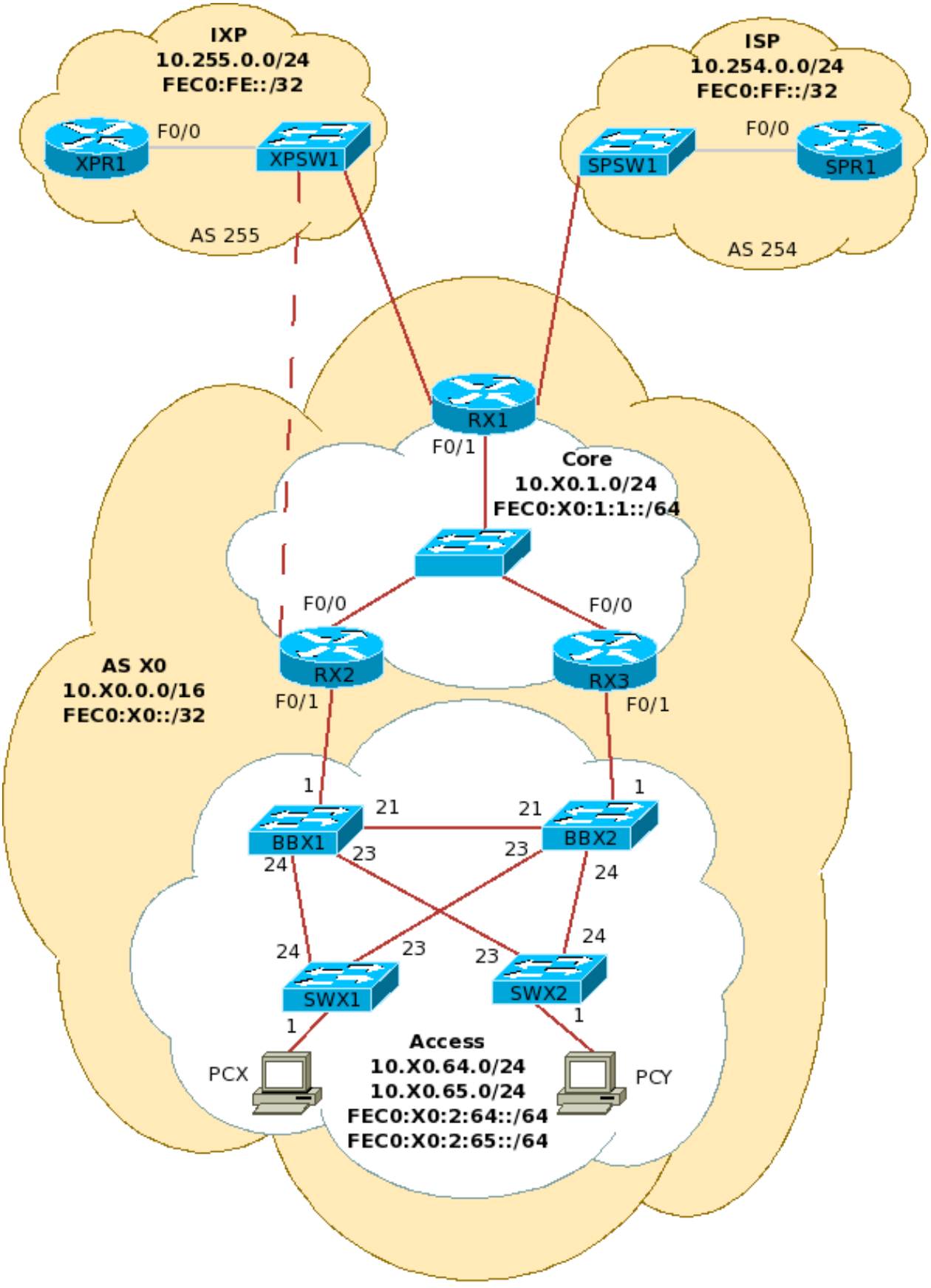
- Group 1: 10.10.64.0/24
- Group 2: 10.20.64.0/24
- Group 3: 10.30.64.0/24
- Group 4: 10.40.64.0/24
- Group 5: 10.50.64.0/24

Switch types used in the LAB

- Hewlett Packard Procurve Switch 2824 (J4903A)

Brief introduction to switch configuration

See Appendix A


IXP
10.255.0.0/24
FEC0:FE::/32
F0/0
XPR1
XPSW1
AS 255
ISP
10.254.0.0/24
FEC0:FF::/32
F0/0
SPSW1
SPR1
AS 254
RX1
F0/1
Core
10.X0.1.0/24
FEC0:X0:1:1::/64
F0/0
F0/0
RX2
RX3
AS X0
10.X0.0.0/16
FEC0:X0::/32
F0/1
F0/1
1
21
21
1
BBX1
BBX2
24
23
23
24
24
23
23
24
SWX1
SWX2
1
1
PCX
PCY
Access
10.X0.64.0/24
10.X0.65.0/24
FEC0:X0:2:64::/64
FEC0:X0:2:65::/64

Spanning Tree Design Information

Priority Table

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.

Exercises

1. 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**. 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.X0.64.4
        - Access switch 1: 10.X0.64.6
        - Access switch 2: 10.X0.64.7
    b. Connect to the workstations and verify their IP addresses
        - Workstation1: 10.X0.64.20 connected to switch11
    c. Verify connectivity by pinging each workstation and switch.

2. Take one patch cord and connect each end to two of the edge switches. What happens? **(Only when lab is local)**
    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.

3. 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 workstation to one of the access switches. How long does it take to become active?
        - Hints for remote lab: enable and disable the interface where the workstation is connected. Use ping and look at the switch logs to verify the times.
        - Change the Spanning Tree Protocol version to RSTP on all switches
        - Repeat the same test. How long does it take now?

4. 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 "4" on the second aggregation switch
    d. Verify which one is the root switch and explain why
    e. Verify port roles and status. Which ports are blocking?
    f. How can you guarantee that the first aggregation switch stays as the SPT root?
    g. Turn off the first aggregation switch (or disable its active interfaces if you are on a remote lab)
    h. Who is the root now? Verify port roles and status. Verify connectivity.

i. Bring back the first aggregation switch
j. Disable spanning tree in one of the aggregation switches. What happens?

5. We now want to segregate end-user data traffic from VOIP and network management traffic.
   a. Use the configurations in **Appendix D** to create **DATA, VOIP and MGMT VLANs**.
   b. Remove the IP addresses from VLAN 1
   c. Verify connectivity between switches using the console connections
   d. From the workstations, try pinging any of the switches. What happened?

6. We now want more capacity and link redundancy between the aggregation switches **(Only when lab is local)**
   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?

7. Suppose you wanted to load balance the traffic from the two VLANs across both aggregation switches. How can you achieve this?
   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.

8. 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 workstation 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"
time timezone -480
time daylight-time-rule Continental-US-and-Canada
lldp run
cdp run
ip icmp burst-normal 20
ip icmp reply-limit
ip ttl 6
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address 10.X0.64.Y 255.255.255.0
   ip igmp
exit
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
write mem
reload
```

* For the first aggregation switch, use priority 3

Appendix D – Data, VOIP and Management VLANs

- On the aggregation switches:

```
vlan 1
   no ip address
   no ip igmp
exit
vlan 64
   name "DATA"
   tagged 1,21,23-24
   ip igmp
exit
vlan 65
   name "VOIP"
   tagged 1,21,23-24
   ip igmp
exit
vlan 255
   name "MGMT"
   tagged 1,21,23-24
   ip address 10.X0.255.Y 255.255.255.0
exit
```

- On the access switches:

```
vlan 1
   no ip address
   no ip igmp
exit
vlan 64
   name "DATA"
```

```
   untagged 1-12
   tagged 23-24
   ip igmp
exit
vlan 65
   name "VOIP"
   untagged 13-20
   tagged 23-24
   ip igmp
exit
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
```

Appendix F - Multiple Spanning Tree (MSTP)

- 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 64 65
spanning-tree instance 1 priority 3
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 4
```

- On the second aggregation switch:

```
spanning-tree config-name "mstp1"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 64 65
```

```
spanning-tree instance 1 priority 4
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 3
```

- On the access switches:

```
spanning-tree config-name "mstp1"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 64 65
spanning-tree instance 2 vlan 255
```

Appendix F - Rapid Spanning Tree (RSTP)

- 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
```