Layer 2 Network Design Lab

Campus Network Design Workshop

July 10, 2011

Contents

1 Part 1

1.1 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.

There will be 5 groups of 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

1.1.1 Switch types used in the lab

Hewlett Packard Procurve Switch 2824 (J4903A) or similar

1.1.2 Remote access instructions

If you are using the remote lab, refer to the file called nsrc-lab-access-instructions.txt

1.1.3 Brief introduction to switch configuration

See Appendix A

1.2 Hierarchical network

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.

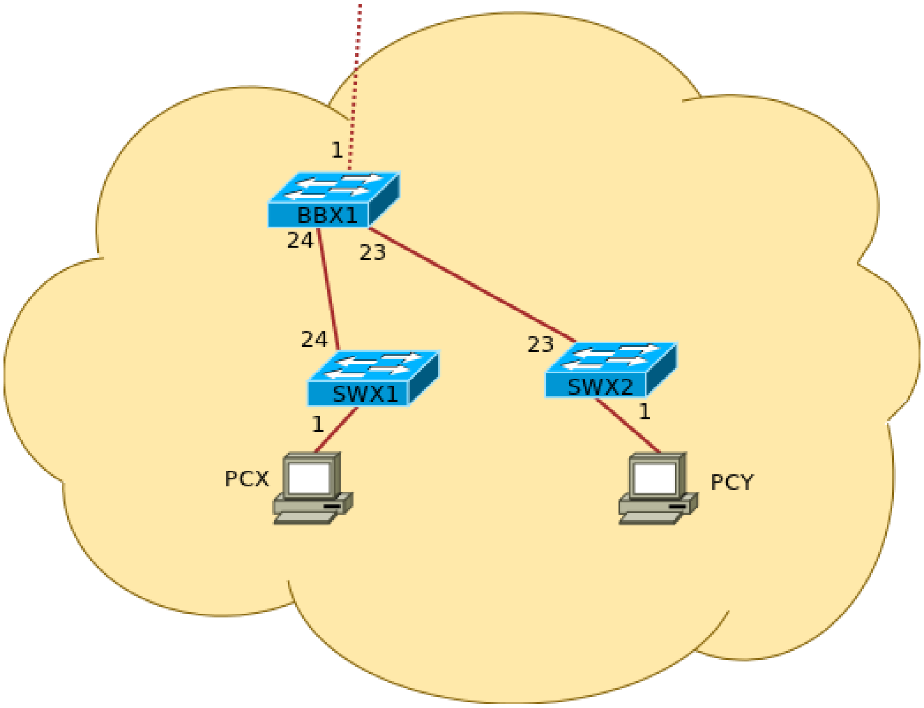

Figure 1: Initial lab topology

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:
     1. Aggregation switch: 10.X0.64.4
     2. Access switch 1: 10.X0.64.6
     3. Access switch 2: 10.X0.64.7
   - Assign each switch its host name according to the diagram

b. Connect two laptops as workstations and verify their IP addresses

   - Workstation1: 10.X0.64.20 connected to switch X1

- Workstation2: 10.X0.64.21 connected to switch X2

c. Verify connectivity by pinging each workstation and switch.

1.3 Looping

The second backbone switch is purposely not yet connected. What happens if you do?

a. Connect the second backbone switch as per the next diagram

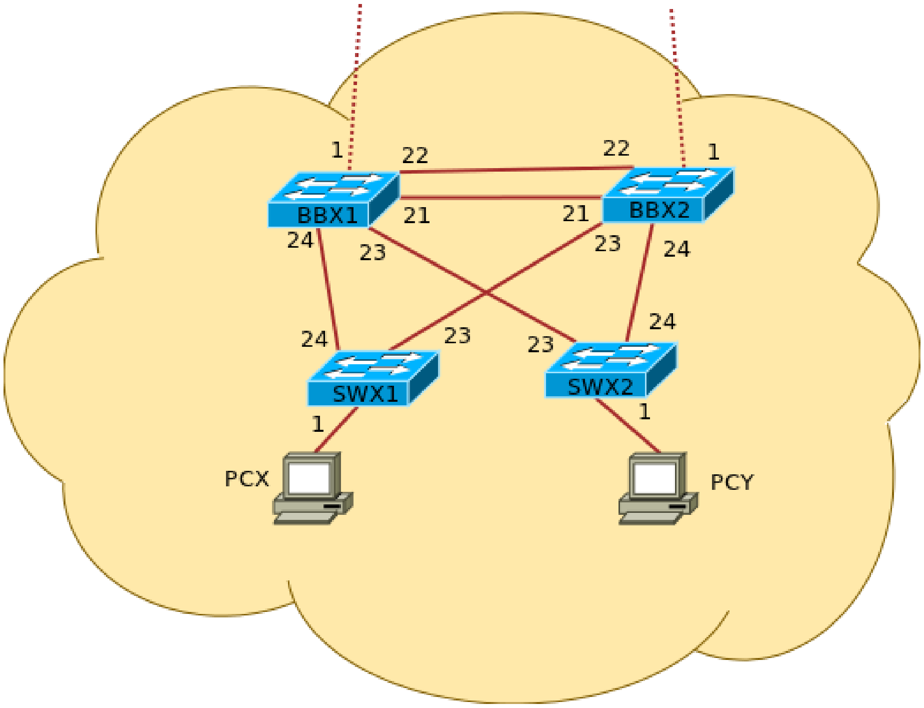

Figure 2: Redundant lab topology

b. Send a few pings. Watch the port counters on the inter-switch links. What happens with the broadcast/multicast counters?

```
# show interfaces [port]
```

c. Can the switches ping each other reliably? Why?

d. Disable the ports on the second switch

```
# switch(config)# interface 21-24 disable
```

1.4 STP

We will now configure the **Spanning Tree Protocol**.

a. Use the configuration files in Appendix C and apply it to BBX1, SWX1 and SWX2

b. What is the main difference between the configurations for the backbone switch and the edge switches?

c. Verify port roles and status on BBX1, SWX1 and SWX2:

```
# show spanning-tree config
# show spanning-tree
# show spanning-tree [port] detail
```

   - Who is the root switch?
   - Which ports are forwarding and which ones are blocking?

d. Re-enable the inter-switch links on the second backbone switch. How have things changed since the last time?

1.5 Redundancy

What happens to a network if a single aggregation switch dies? Let's now add redundancy.

a. Configure the second aggregation switch. Use the address 10.X0.64.5.

b. Configure Spanning Tree with a priority of "4" on the second aggregation switch

c. Verify which one is the root switch and explain why

d. Verify port roles and status. Which ports are blocking?

e. Reload first aggregation switch.

   1. While it is rebooting, verify spanning tree status. Who is the root now? Verify port roles and status. Verify connectivity.
   2. What happens to the spanning tree when the switch comes back online?

1.6 Testing edge ports

Unplug one of the workstations, and a few seconds later plug it back into the same switch port. How long does it take before the workstation is able to ping? Why?

If you're not running RST, then normally it takes 30 seconds for ports to enter the forwarding state when connected. Many switches have a "portfast" facility to mark edge ports, and/or to disable the port if any STP PDUs are received. Never do this on ports linking to other switches!

Decide if you need it here. A sample configuration would be:

```
# spanning-tree ethernet 1-20 bpdu-filter bpdu-protection
```

2 Part 2

2.1 VLANs

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. Verify connectivity between switches using the console connections

c. From the workstations, try pinging any of the switches using their new addresses. What happened?

2.2 Bundling

We now want more capacity and link redundancy between the aggregation switches.

a. Use Appendix E to configure **Port Bundling**.

b. Verify the status of the new trunk:

   ```
   # show lacp
   ```

c. What capacity do you have now on the new trunk?

d. Disable one of the ports in the bundle. What happens?

3 Part 3

3.1 MSTP

Suppose you wanted to load balance the traffic from/to 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.

3.2 Rogue DHCP preventation

a. If available, configure a client computer as a DHCP server. From another client computer, check if you can get an IP address assigned. What happens if your users do this without your consent?

b. Use the instructions in Appendix G to configure Rogue **DHCP prevention**. Can the client computer get an address now?

4 Reference

4.1 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]
clear statistics [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
```

4.2 Appendix B - Basic switch configuration (HP2800)

This is a minimum configuration, which just sets hostname and managament IP:

```
hostname "switch"
vlan 1
   untagged 1-24
   ip address 10.X0.64.Y 255.255.255.0
```

Here is a more complete base configuration which you might use in a production environment:

```
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
```

4.3 Appendix C - Spanning Tree Configuration

```
spanning-tree
spanning-tree protocol-version RSTP
spanning-tree priority X*
write mem
reload
```

(*) Refer to the priority table below for the appropriate priorities on each switch. Use the “multiplier” value here.

4.4 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 1,21-24
   ip igmp
exit
vlan 65
   name "VOIP"
```

Multiplier	Priority Value	Description	Notes
0	0	Core Node	The core switches/routers will not be participating in STP… reserved in case they ever are
1	4096	Redundant Core Nodes	Ditto
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-changed 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 managed network devices should have this priority.

Table 1: Priority Table

```
   tagged 1,21-24
   ip igmp
exit
vlan 255
   name "MGMT"
   tagged 1,21-24
   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
```

4.5 Appendix E - Port Bundling

On the Aggregation switches only:

```
trunk 21-22 Trk1 LACP
vlan 64 tagged Trk1
vlan 65 tagged Trk1
vlan 255 tagged Trk1
```

4.6 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 1 priority 6
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 6
```

4.7 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
```

4.8 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
```