Layer 2 Network Design Lab

Campus Network Design Workshop

August 21, 2012

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.

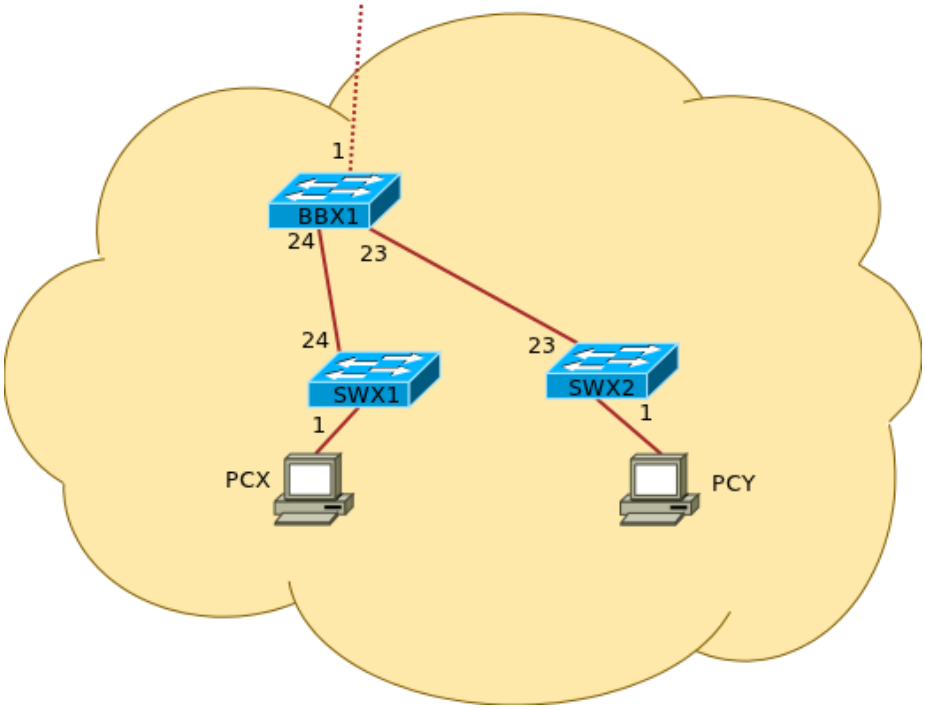

Figure 1: Initial lab topology

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 as follows:
  1. BBX1: 10.X0.64.4
  2. SWX1: 10.X0.64.6
  3. SWX2: 10.X0.64.7
- Assign each switch its host name according to the diagram

b. Connect two PCs and verify their IP addresses

- PCX: 10.X0.64.20 connected to SWX1

- PCY: 10.X0.64.21 connected to SWX2

c. Verify connectivity by pinging each PC and switch.

1.3 Redundancy

What happens to the network if BBX1 fails?

a. Configure BBX2. Use the address 10.X0.64.5.

b. Connect BBX2 as per the next diagram

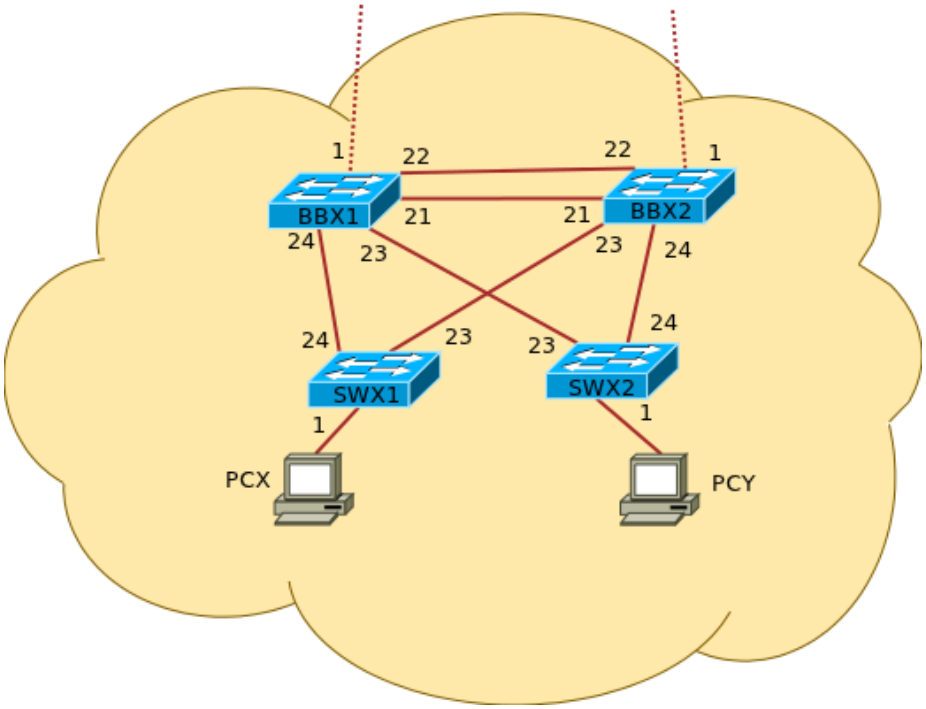

Figure 2: Redundant lab topology

If you are using the remote lab: login to BBX2 and enable ports 21–24 as follows:

```
# switch# conf t
# switch(config)# interface 21-24 enable
# switch(config)# end
```

c. Can the switches ping each other reliably? Why? Watch the port counters on the inter-switch links. What happens with the broadcast/multicast counters?

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

1.4 STP

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

a. Use the configuration files in Appendix C and apply it to all four switches.

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
```

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

How have things changed since the last time? Can you ping all switches?

d. Reboot BBX1.

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?

1.5 Testing edge ports

If you are working with real switches (not remote lab), unplug one of the PCs, and a few seconds later plug it back into the same switch port. How long does it take before the PC is able to ping? Why?

Normally it takes 30 seconds for ports to enter the forwarding state when connected. When running RSTP or MST, you can nominate certain ports as "edge ports", and this is worthwhile.

Some HP switches have a feature called "auto-edge-port" (enabled by default), which looks for BPDUs for three seconds; if none are seen, the port is switched to edge port automatically. Otherwise, you can force this manually by enabling `admin-edge-port` on the relevant ports.

There may also be facilities to ignore STP BPDUs on those ports, or to disable the port if any BPDUs are received. Never configure these features on ports linking to other switches!

A sample configuration combining these features would be:

```
# spanning-tree ethernet 1-20 admin-edge-port bpdu-filter bpdu-protection
```

2 Part 2

2.1 VLANs

We now want to segment the network to separate end-user traffic from VOIP and network management traffic. Each of these segments will use its own separate IP subnet.

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 PCs, 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. Is the trunk still up?

3 Part 3

3.1 MSTP

Your two aggregation switches are each connected to a core router (not shown in the pictures).

Suppose you wanted to load-balance the traffic from your various VLANs as they leave your aggregation switches towards your routers? 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 prevention

a. If possible, configure a PC as a DHCP server. From another PC, 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.

Mult	Priority	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 Node	Ditto
2	8192	Reserved	
3	12288	**Building Backbone**	
4	16384	**Redundant 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 manag	ed network devices should have this priority.

Table 1: Priority Table

4.4 Appendix D - Data, VOIP and Management VLANs

On the aggregation switches (BBX1 and BBX2):

```
vlan 1
   no ip address
   no ip igmp
exit
vlan 64
   name "DATA"
   tagged 1,21-24
   ip igmp
exit
vlan 65
   name "VOIP"
   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 (SWX1 and SWX2):

```
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:

```
interface 21-22 disable
trunk 21-22 trk1 LACP
interface 21-22 enable
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 1.2.3.4
radius-server host 5.6.7.8
```