Layer 2 Network Design Lab

Campus Network Design & Operations Workshop

Introduction

The purpose of this exercise is to build Layer 2 (switched) networks utilizing the concepts explained in today's design presentation. Students will see how star topology, aggregation, Spanning Tree Protocol and VLANs are put to work.

The classroom is divided into 6 groups, with 7 switches per group. We will start off by building a flat campus network to demonstrate some of the key design concepts mentioned in the presentation. The flat network will be numbered out of a single IPv4 /16 address block and a single IPv6 /64 address block.

Lab Layout

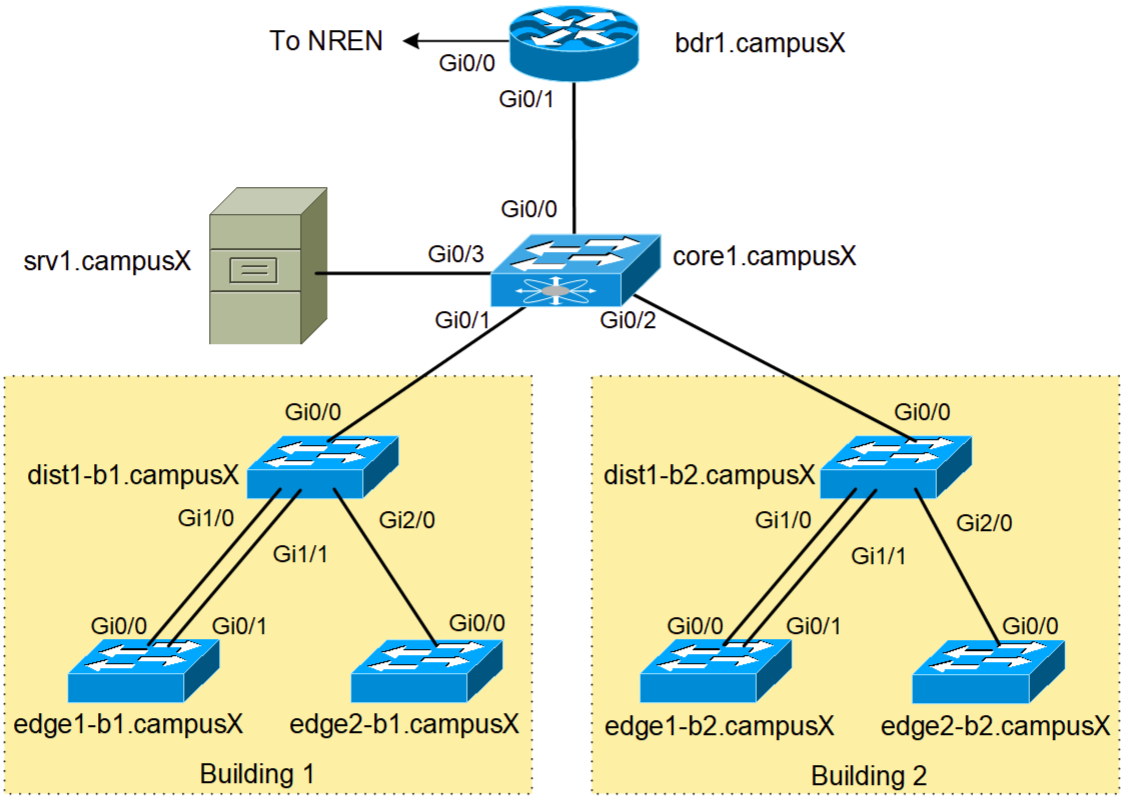
The IP addresses for the building (Layer 2) devices will be as follows:

Device	IPv4	IPv6
core1.campusX	172.2X.0.2/16	2001:DB8:X:1::2/64
dist1-b1.campusX	172.2X.0.3/16	2001:DB8:X:1::3/64
edge1-b1.campusX	172.2X.0.4/16	2001:DB8:X:1::4/64
edge2-b1.campusX	172.2X.0.5/16	2001:DB8:X:1::5/64
dist1-b2.campusX	172.2X.0.6/16	2001:DB8:X:1::6/64
edge1-b2.campusX	172.2X.0.7/16	2001:DB8:X:1::7/64
edge2-b2.campusX	172.2X.0.8/16	2001:DB8:X:1::8/64

You will need to replace **X** with the number of your campus group!

Note: The overall architecture can be found in the IP Address Plan.

The following diagram shows the layout of the devices and all the links for each campus:



The following table shows the connections between each device in the campus:

Device	Interface	Remote Device	Remote Interface
dist1-bY.campusX	GigabitEthernet1/0	edge1-bY.campusX	GigabitEthernet0/0
	GigabitEthernet1/1	edge1-bY.campusX	GigabitEthernet0/1
	GigabitEthernet2/0	edge2-bY.campusX	GigabitEthernet0/0
core1.campusX	GigabitEthernet0/0	bdr1.campusX	GigabitEthernet0/1
	GigabitEthernet0/1	dist1-b1.campusX	GigabitEthernet0/0
	GigabitEthernet0/2	dist1-b2.campusX	GigabitEthernet0/0
	GigabitEthernet0/3	srv1.campusX	ens3
bdr1.campusX	GigabitEthernet0/0	transit1-nren	GigabitEthernet0/X
	GigabitEthernet0/2	transit2-nren	GigabitEthernet0/X

Replace **Y** with your building number and **X** with your campus number.

Accessing the Lab

The Workshop Instructors will let you know what the lab environment is. It will either be run on a Virtual Platform, or on real physical switches provided in the Training Room.

Refer to the **correct** document below for information about logging into the devices that have been assigned to you:

VIRTUAL ENVIRONMENT: Virtual Environment Lab Access Instructions

PHYSICAL HARDWARE: Physical Hardware Lab Access Instructions

Basic Switch Configuration

Our building network consists of a distribution (aggregation) switch and two edge switches. Each building distribution switch connects to the core switch of our campus network and serve as aggregation points for all the edge switches. Edge switches serve the end users.

Each switch will be named according to the table above: `core1.campus1` , `dist1-b1.campus1` , `edge2-b1.campus5` , etc

Your group should share out the seven switches amongst the team members and configure each one using the example shown below.

Hostname

Your switches should be given a basic configuration as follows:

```
Switch> enable
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname dist1-b1.campusX
dist1-b1.campusX(config)#
```

Turn Off Domain Name Lookups

Cisco devices will always try to look up the DNS for any name or address specified in the command line. You can see this when doing a trace on a router with no DNS server or a DNS server with no in-addr.arpa entries for the IP addresses. We will turn this lookup off for the labs for the time being to speed up traceroutes.

```
dist1-b1.campusX(config)# no ip domain lookup
```

Set the Domain Name

We will now set the domain name of our campus devices, for future use in this workshop.

```
dist1-b1.campusX(config)# ip domain name ws.nsrc.org
```

Turn Off the builtin Webserver

More modern Cisco devices have a builtin Webserver which tends to be turned on by default. Given this is a potential security risk, we will turn it off:

```
dist1-b1.campusX(config)# no ip http server
```

Configure console and other ports

By default, Cisco devices will try all transports available if they don’t recognise what is typed into the command line. This behaviour is annoying especially if making a typo during configuration work, so we will disable the behaviour completely. We will also set the idle-timeout on the console and other ports to 30 minutes - after 30 minutes of no activity on the port, the device will disconnect the connection.

```
dist1-b1.campusX(config)# line con 0
dist1-b1.campusX(config-line)# transport preferred none
dist1-b1.campusX(config-line)# exec-timeout 30 0
dist1-b1.campusX(config-line)# line aux 0
dist1-b1.campusX(config-line)# transport preferred none
dist1-b1.campusX(config-line)# exec-timeout 30 0
dist1-b1.campusX(config-line)# line vty 0 4
dist1-b1.campusX(config-line)# transport preferred none
dist1-b1.campusX(config-line)# exec-timeout 30 0
```

Usernames and Passwords

All router usernames should be **cndlab** with password being **lab-PW**. The enable password (which takes the operator into configuration mode) needs to be **lab-EN**[1].

Please do not change the username or password to anything else, or leave the password unconfigured (access to vty ports is not possible if no password is set). It is essential for a smooth operating lab that all participants have access to all routers.

```
dist1-b1.campusX(config)# username cndlab secret lab-PW
dist1-b1.campusX(config)# enable secret lab-EN
dist1-b1.campusX(config)# service password-encryption
```

The service password-encryption directive tells the router to encrypt all passwords stored in the router’s configuration (apart from enable secret[2] which is already encrypted).

Enabling login access for other devices

In order to let you telnet into your device in future modules of this workshop, you need to configure a password for all virtual terminal lines.

```
dist1-b1.campusX(config)# aaa new-model
dist1-b1.campusX(config)# aaa authentication login default local
dist1-b1.campusX(config)# aaa authentication enable default enable
```

This series of commands tells the router to look locally for standard user login (the username password pair set earlier), and to the locally configured enable secret for the enable login. By default, login will be enabled on all vtys for other teams to gain access.

Configure system logging

A vital part of any Internet operational system is to record logs. The router by default will display system logs on the router console. However, this is undesirable for Internet operational routers, as the console is a 9600 baud connection, and can place a high processor interrupt load at the time of busy traffic on the network. However, the router logs can also be recorded into a buffer on the router – this takes no interrupt load and it also enables to operator to check the history of what events happened on the router.

```
dist1-b1.campusX(config)# no logging console
dist1-b1.campusX(config)# logging buffer 8192 debug
```

which disables console logs and instead records all logs in a 8192 byte buffer set aside on the router. To see the contents of this internal logging buffer at any time, the command `show log` should be used at the command prompt.

And we also want to set up improved time-stamping for the log messages as well:

```
dist1-b1.campusX(config)# service timestamps debug datetime msec localtime show-timezone
year
dist1-b1.campusX(config)# service timestamps log datetime msec localtime show-timezone year
```

which will give resolution down to milliseconds, and include the year as well.

Setting a login banner

Depending on which environment is used, you will find that your switch might have a default login banner already set. We will modify this so that it is a bit more informative:

```
dist1-b1.campusX(config)# banner login ^
Campus Network Design and Operations Workshop Lab
         Network Startup Resource Center
^
```

Note the `^` symbol - this is used as the marker for the start and end of the banner text.

This banner will notify administrators every time they connect to the device. In real life, we'd also include wording about authorised access, authorised use, and that the device is being monitored.

We will also remove the `exec` banner (if there is one):

```
dist1-b1.campusX(config)# no banner exec
```

as that is only used as a reminder to administrators of, for example, special configurations once they have logged into the switch.

Save the Configuration.

With the basic configuration in place, save the configuration. To do this, exit from enable mode by typing `end` or `<ctrl>Z` , and at the command prompt enter `write memory` . If you are prompted `[confirm]` hit enter again.

```
dist1-b1.campusX(config)# end
dist1-b1.campusX# write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 3788 bytes to 1832 bytes[OK]
[OK]
dist1-b1.campusX#
```

It is highly recommended that the configuration is saved quite frequently to NVRAM. If the configuration is not saved to NVRAM, any changes made to the running configuration will be lost after a power cycle or virtual machine failure

Log off the switch:

```
dist1-b1.campusX# exit
```

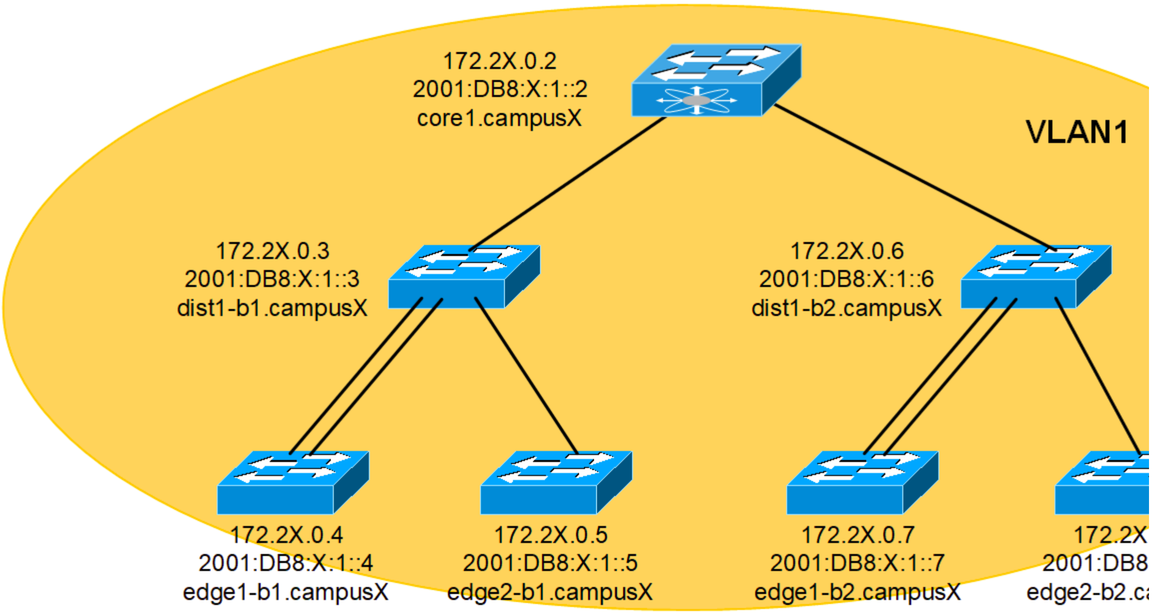
and then log back in again. Notice how the login sequence has changed, prompting for a `username` and `password` from the user, like this:

```
dist1-b1.campusX con0 is now available

Press RETURN to get started.

User Access Verification

Username:
```

Note that at each checkpoint in the workshop, you should save the configuration to memory – remember that powering the device off will result in it reverting to the last saved configuration in NVRAM.

IP Address Configuration

Now that we have done the initial configuration of all the switches in our campus, we can now configure the Management IP addresses (in IPv4 and IPv6). The following diagram shows the flat network we have just built.



Assign each switch a different IPv4 address and IPv6 address as follows:

```
interface vlan 1
 ip address 172.2X.0.N 255.255.0.0
 ipv6 address 2001:DB8:X:1::N/64
 load-interval 30
 no shutdown
end
```

Replace the **X** with your group number, and **N** with the address according to the address plan earlier in the notes. Note the `load-interval` command which will calculate the average traffic load on the interface over a 30 second period (rather than over the default 5 minutes).

Verify connectivity by pinging each switch within the building. Do not continue until you can ping each switch from every other switch in the campus.

HINT: If ping fails, but the configuration seems OK, try doing the following:

```
interface vlan 1
 shutdown
 no shutdown
end
```

(this is not normal, but most likely a bug in the IOS code somewhere)

If this still doesn't work, check your switch configuration to see if you have anything looking like this:

```
mac-address-table static c40d.5eca.0000 interface GigabitEthernet0/0 vlan 1
```

For some unknown reason, the switch on rare occasions will add static MAC entries. These often point to the wrong interface. If you have entries like these in your configuration, trying shutting down the VLAN 1 interface mentioned, deleting the line by putting a `no` in front of the offending configuration, and then bringing the VLAN 1 interface back up again. If that doesn't work (the `mac-address-table` line is still there), ask your lab instructor.

(this is also not normal, and most likely a bug in the IOS code somewhere)

Question: Are you able to ping all the switches in the network?

If not, check the configuration of your switch and of the other switches as well. All seven switches in the campus should be able to ping each other now.

NOTES

1. There is the temptation to simply have a username of `cisco` and password of `cisco` as a lazy solution to the username/password problem. Under no circumstances must any service provider operator ever use easily guessable passwords as these on their live operational network. This sentence cannot be emphasized enough. It is quite common for attackers to gain access to networks simply because operators have used familiar or easily guessed passwords.

2. For IOS releases prior to 12.3, the username/secret pair was not available, and operators would have had to configure username/password instead. Do **NOT** use the username/password combination, nor the `enable password` directive - these use type-7 encryption which is not secure at all, whereas the `secret` uses the more secure md5 based encryption.