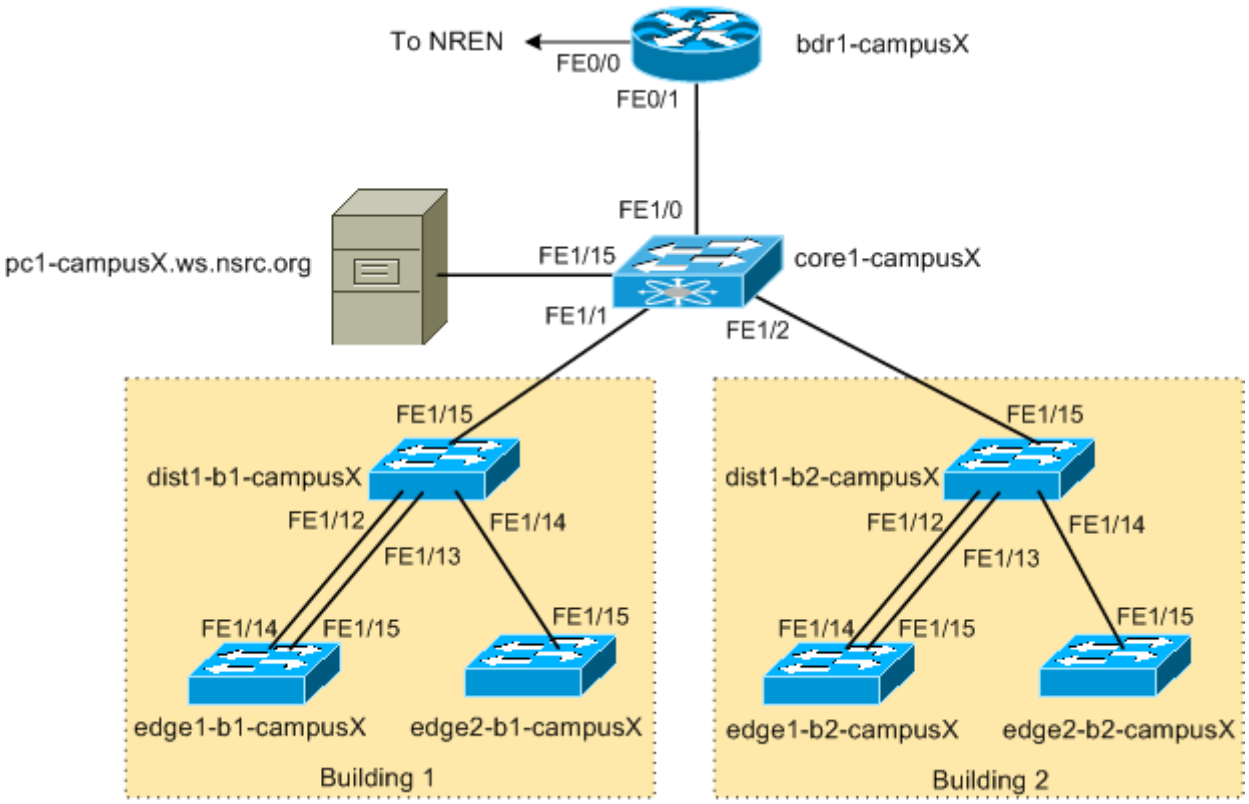
Layer 2 Network Design Lab - VLANs

Introduction

The purpose of this exercise is to create separate VLANs for different groups of users in each building. In a later exercise we will configure the core router so that each VLAN is using a different IP subnet.

This lab is a continuation from the Spanning Tree exercise and the lab setup is identical:



Accessing the Lab & Current IP Addressing

Here is a reminder of how to access the lab. Refer to the **correct** document below for information about logging into the devices that have been assigned to you:

VIRTUAL ENVIRONMENT: Lab Access Instructions - Virtualised Platform

PHYSICAL HARDWARE: Lab Access Instructions - Physical Hardware

And here is a reminder of the management IP addresses currently configured on each switch. Replace the “X” with your campus number.

Name	IPv4	IPv6
core1-campusX	172.2X.0.1/16	2001:db8:X:0::0:1/64
dist1-b1-campusX	172.2X.1.2/16	2001:db8:X:0::1:2/64
edge1-b1-campusX	172.2X.1.3/16	2001:db8:X:0::1:3/64

edge2-b1-campusX	172.2X.1.4/16	2001:db8:X:0::1:4/64
dist1-b2-campusX	172.2X.2.2/16	2001:db8:X:0::2:2/64
edge1-b2-campusX	172.2X.2.3/16	2001:db8:X:0::2:3/64
edge2-b2-campusX	172.2X.2.4/16	2001:db8:X:0::2:4/64

VLANs

We now want to segment the network to separate network management traffic from end-user traffic (staff and students). Running one large flat network across the entire campus simply does not scale as was covered during the presentation. Each of these segments will be a separate subnet.

We need to take a structured approach with this migration. While we have the luxury of working in a lab for this workshop, on a campus network migration from a flat to a routed backbone needs care and planning.

The process will be this:

- Create a VLAN for the Staff (called STAFF)
- Create a VLAN for the Students (called STUDENT)
- Create a VLAN for device management (called MGMT)
- Shutting down VLAN1 - VLAN1 is the Cisco default, has many well documentedsecurity risks for campus networks, and should never be used.

VLANs and Address Plan

We will now create the VLANs described in the previous steps. As each VLAN is a different network, they need their own address subnet (IPv4 and IPv6). The Campus Core switch will route between each VLAN (so called L3-switch: an ethernet switch which has some L3 routing capability).

Name	VLAN	IPv4	IPv6
Building 1 Management	10	172.2X.10.0/24	2001:db8:X:10::/64
Building 1 Staff	11	172.2X.11.0/24	2001:db8:X:11::/64
Building 1 Student	12	172.2X.12.0/24	2001:db8:X:12::/64
Building 2 Management	20	172.2X.20.0/24	2001:db8:X:20::/64
Building 2 Staff	21	172.2X.21.0/24	2001:db8:X:21::/64
Building 2 Student	22	172.2X.22.0/24	2001:db8:X:22::/64

These IP addresses are also documented in the master IP Address Plan.

Disabling VTP

VTP (VLAN Trunking Protocol) is a proprietary Cisco technology that allows for dynamic VLAN provisioning. We will not use it here.

Disable VTP by setting it to “transparent mode”:

```
vtp mode transparent
```

Configure trunk ports

The Core switch connects to the Distribution switches in each building, which in turn connect to two Edge switches in each building. So that we can pass VLAN tags from switch to switch, we need to convert the interfaces which connect between the switches two trunk ports. (The Cisco default is for the interfaces to pass ethernet frames untagged.)

Referring to the network diagram above, configure the following for each port that needs to tag VLAN frames. For example, on Distribution switch in Building1 in Campus1:

```
interface FastEthernet 1/13
 description Trunk Link to edge1-campus1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Note: The Cisco default is to use dot1q encapsulation (rather than the Cisco proprietary ISL). But we include the dot1q command in the configuration in any case.

Reminder: Check the diagram to see which ports you need to modify - don’t just guess!

And don’t forget to put the descriptions on the interfaces!

Configure the switches with MGMT, STAFF and STUDENT VLANs.

Add the VLANs to the VLAN database on each switch and give them names to better identify them. If you don’t do this, the switches won’t know which VLANs are present in the network.

On the Core Switch:

```
vlan 10
 name MGMT1
vlan 11
 name STAFF1
vlan 12
 name STUDENT1
vlan 20
 name MGMT2
vlan 21
 name STAFF2
vlan 22
```

```
 name STUDENT2
```

On Building 1 switches:

```
vlan 10
 name MGMT1
vlan 11
 name STAFF1
vlan 12
 name STUDENT1
```

On Building 2 switches:

```
vlan 20
 name MGMT
vlan 21
 name STAFF2
vlan 22
 name STUDENT2
```

Configuring STP for each VLAN

Verify the Spanning Tree status:

```
show spanning-tree brief
```

Notice the root and bridge priorities on each VLAN (1,10,11,12) and (1,20,21,22). Are they the same?

Copy the bridge priority which you previously set on VLAN 1 to the new VLANs you have created. (This was from the table in **Appendix A** in the Spanning Tree exercise)

Note: This is called “Per-VLAN spanning tree”, or PVST. This means that the switches are creating 4 separate trees, each with its own parameters, status, calculations, etc. Imagine if you had several hundred VLANs! This is certainly not ideal. There are better standards, like “Multiple Spanning Tree” (MST), that allow the administrator to create only the desired number of trees, and map groups of VLANs to each tree. Unfortunately, this Cisco device does not support MST.

For example, for the distribution switch in Building 1:

```
spanning-tree vlan 10 priority 12288
spanning-tree vlan 11 priority 12288
spanning-tree vlan 12 priority 12288
```

Once the priorities have been set, check the output of the spanning tree status command. Which is the root bridge for each VLAN?

IP Addressing for the MGMT VLAN

We originally configured the switches so that we were using VLAN 1 to manage them (and provide end user access for the whole campus!). And the IPv4 address block we have used up to now was the entire 172.2X.0.0/16 (for IPv6 we only used 2001:DB8:X:0::/64) as we had one large broadcast domain for the whole campus.

We need to move away from this now.

We cannot simply address the VLANs we created using a subnet of 172.2X.0.0/16 while that entire address block is being used for VLAN 1 - Cisco IOS does not allow overlapping subnets to be configured on routing devices (the core1-campusX switch will be routing traffic between the VLANs).

For this exercise we will simply remove the management IP addresses from VLAN 1 and set up new subnets on VLAN10 (MGMT for Building 1) and VLAN 20 (MGMT for Building 2).

(**Note:** If doing this on a live network, removing the IP addressing and shutting down VLAN 1 will remove all Internet connectivity for all users connected to the switches - so this activity is best done when the network is unused, usually early in the mornings or at weekend, depending on when the campus is quietest.)

Remember that while we can delete an IPv4 address simply by doing “no ip address”, we have to type in the entire IPv6 address to delete it (because IPv6 allows multiple addresses per interfaces, unlike IPv4).

On the Core Switch:

```
interface vlan 1
 no ip address
 no ipv6 address 2001:db8:X:0::1:1/64
 shutdown
!
interface vlan 10
 description Management VLAN Building 1
 ip address 172.2X.10.1 255.255.255.0
 ipv6 address 2001:db8:X:10::1/64
 no shutdown
!
interface vlan 20
 description Management VLAN Building 2
 ip address 172.2X.20.1 255.255.255.0
 ipv6 address 2001:db8:X:20::1/64
 no shutdown
!
```

In Building 1:

```
interface vlan 1
 no ip address
 no ipv6 address 2001:db8:X:0::1:Y/64
 shutdown
```

```
!
interface vlan 10
 description Management VLAN Building 1
 ip address 172.2X.10.Y 255.255.255.0
 ipv6 address 2001:db8:X:10::Y/64
 no shutdown
!
```

In Building 2:

```
interface vlan 1
 no ip address
 no ipv6 address 2001:db8:X:0::2:Y/64
 shutdown
!
interface vlan 20
 description Management VLAN Building 2
 ip address 172.2X.20.Y 255.255.255.0
 ipv6 address 2001:db8:X:20::Y/64
 no shutdown
!
```

Notice the sequence. It is very important to remove all IP addresses (both IPv4 and IPv6) from VLAN 1 and shut VLAN 1 down before anything is configured on VLAN 10 and VLAN 20.

This table shows the IP addresses which are assigned to the management interfaces of the core, distribution and edge switches. Replace the **X** and **Y** in the examples above with the appropriate numbers from this table:

Building 1 Management	**VLAN**	**IPv4**	**IPv6**
core1-campusX	10	172.2X.10.1/24	2001:db8:X:10::1/64
dist1-b1-campusX	10	172.2X.10.2/24	2001:db8:X:10::2/64
edge1-b1-campusX	10	172.2X.10.3/24	2001:db8:X:10::3/64
edge2-b1-campusX	10	172.2X.10.4/24	2001:db8:X:10::4/64
Building 2 Management	**VLAN**	**IPv4**	**IPv6**
core1-campusX	20	172.2X.20.1/24	2001:db8:X:20::1/64
dist1-b2-campusX	20	172.2X.20.2/24	2001:db8:X:20::2/64
edge1-b2-campusX	20	172.2X.20.3/24	2001:db8:X:20::3/64
edge2-b2-campusX	20	172.2X.20.4/24	2001:db8:X:20::4/64

Verify connectivity between switches. Can you ping?

Note: changing Management VLANs is quite tricky to achieve by remotely accessing the switch - it is normally done by accessing the switch's console port (like we are doing here in the lab). Cisco IOS requires VLAN 1 to be shutdown before any packets are moved on VLAN 10 or VLAN 20, so we can't even use the trick of accessing the switch over IPv6 while the IPv4 address is being moved.

Configure IP addresses for the STAFF and STUDENT VLANs.

We now configure the IP addresses of the STAFF and STUDENT VLANs on the Core Switch. Here is an example for VLAN 11, the STAFF VLAN in Building 1:

```
interface vlan 11
 description STAFF VLAN of Building 1
 ip address 172.2X.11.1 255.255.255.0
 ipv6 address 2001:db8:X:11::1/64
 no shutdown
```

Replace **X** with your campus number. Do the same for all the other VLANs as well.

Once completed, your Core switch should have VLANs 11, 12, 21 and 22 configured with both IPv4 and IPv6 addresses.

Question: What is significant about the IP address configured on each VLAN?

Answer: This IP address now serves as the default gateway for every device connecting to this VLAN. So a user on VLAN 11 will have default gateway 172.2X.11.1, etc.

Designating Edge Switch Ports

Now that the STAFF and STUDENT VLANs have been created, and an IPv4 and IPv6 address has been assigned to each one, we can now move the end users to these VLANs.

Now designate 7 edge ports each for STAFF and STUDENT VLAN access on the **edge** switches only (example is for Building 1):

```
interface range Fast1/0 - 6
 description Access Port VLAN 11 STAFF
 switchport mode access
 switchport access vlan 11
!
interface range Fast1/7 - 13
 description Access Port VLAN 12 STUDENT
 switchport mode access
 switchport access vlan 12
```

Verify which ports are members or trunks of each vlan:

```
show vlan-switch id `<VLAN ID>`
```

Imagine that there are computers connected to the STAFF vlan. Would they be able to ping the switch? Explain your response.

Now run the command:

```
show interface description
```

What do you see?

This is why it is important to make sure all interfaces have a description line configured - the above diagnostic command lets any operator see at one easy glance which switch interfaces are used for which function.

Set up the default gateway on the switches

The switches need a default route added to them so that their MGMT VLAN can forward traffic to elsewhere in the network - without it, management traffic will only ever be able to reach other devices on their own VLAN.

On each switch we add this route to forward traffic to the Core router.

For Building 1 try:

```
ip route 0.0.0.0 0.0.0.0 172.2X.10.1
ipv6 route ::/0 2001:db8:X:10::1
```

For Building 2 try:

```
ip route 0.0.0.0 0.0.0.0 172.2X.20.1
ipv6 route ::/0 2001:db8:X:20::1
```

Verifying Connectivity

Trying pinging from switch to switch within your campus. Ping the management interface addresses - and also trying pinging the STAFF and STUDENT subnet addresses configured on the Core Switch too. What do you see?