LAB 12

Practice and Exercise

Virtual Local Area Network (VLAN)

BITS 2343 | Computer Network

nazrulazhar@utem.edu.my

LAB 12- Practice: Building a Scalable Network with VLAN

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Create VLANs
- Assign switch ports to a VLAN
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Configure a router to support 802.1q trunking on a Fast Ethernet interface

Scenario

A VLAN (virtual LAN) is a subnetwork that can group together collections of devices on separate physical local area networks (LANs). Any broadcast domain of VLANs will be partitioned and isolated in a computer network at the data link layer (OSI layer 2).

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Note: The switches used are Cisco Catalyst 2960s. Ensure that the switches have been erased and have no startup configurations. If you are unsure please ask your lecturer.

Topology Diagram

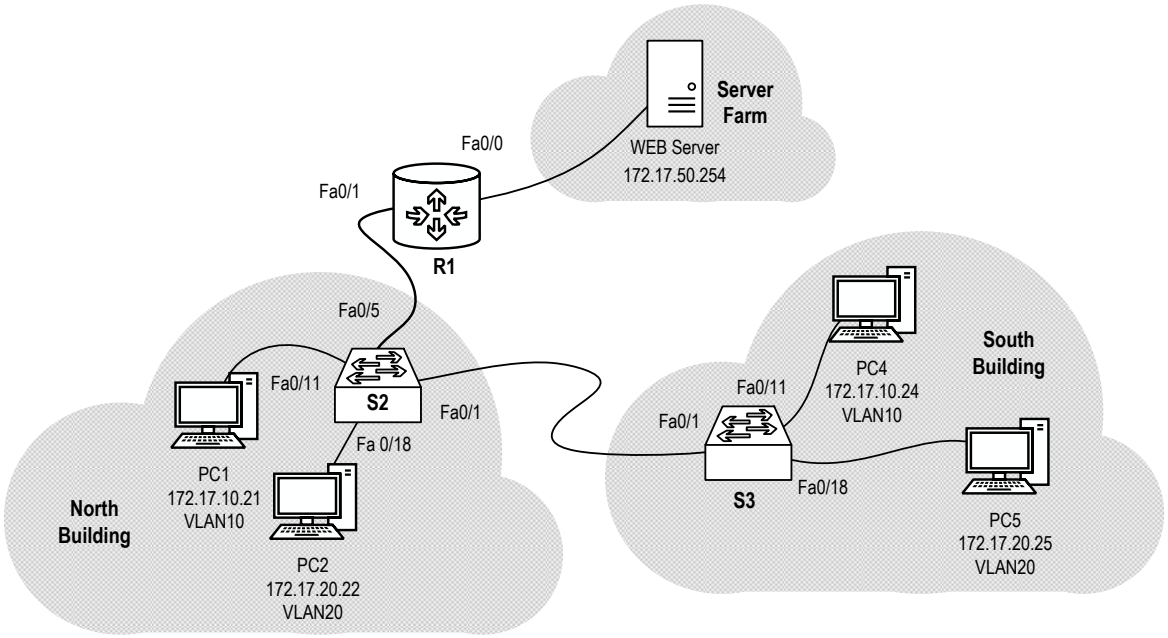

Figure 1 Topology diagram

Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/11	VLAN 10 – Sales	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Marketing	172.17.20.0 /24
Fa0/0	Port Security – Only 1 MAC Address is allowed to connect	

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.
You can use any current switch in your lab as long as it has the required interfaces shown in the topology.

Task 2: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.
Configure all four PCs with the IP addresses and default gateways.

Task 3: Configure VLANs on the Switch

Step 1: Create VLANs on switch S2.
Use the **vlan** *vlan-id* command in global configuration mode to add a VLAN to switch S2. There are three VLANS configured for this lab: VLAN 10 (Sales); VLAN 20 (Marketing); and VLAN 99 (Management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **name** *vlan name* command.

```
S2(config)#vlan 10
S2(config-vlan)#name Sales
S2(config-vlan)#vlan 20
S2(config-vlan)#name Marketing
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management
S2(config-vlan)#end
S2#
```

Step 2: Verify that the VLANs have been created on S2.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
-
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   Sales                             active
20   Marketing                         active
99   Management                        active
```

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20 and 99 on S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the three VLANs you have created?

_____

Step 4: Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. You can assign each port individually or you can use the **interface range** command to simplify this task, as shown here. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3(config-if-range)#interface fa0/11
S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end

S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Step 5: Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANS. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the interface range command in global configuration mode to simplify configuring trunking.

```
S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

```
S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Verify that the trunks have been configured with the show interface trunk command.

```
S3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Step 6: Verify that the PCs can communicate. Ping several hosts from PC2.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____

Because these hosts are on different subnets and in different VLANs, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Task 4: Configure the Router and the Remote Server LAN

Step 1: Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections—a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device is configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANS, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as dot1q trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating "virtual" interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to dot1q aware.

Using the subinterface configuration approach requires these steps:

- Enter subinterface configuration mode
- Establish trunking encapsulation
- Associate a VLAN with the subinterface
- Assign an IP address from the VLAN to the subinterface

The commands are as follows:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown

R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0

R1(config-if)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0

R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Confirm creation and status of the subinterfaces with the **show ip interface brief** command:

```
R1#show ip interface brief

Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/1.10     172.17.10.1     YES manual up                    up
FastEthernet0/1.20     172.17.20.1     YES manual up                    up
FastEthernet0/1.99     172.17.99.1     YES manual up                    up
```

Step 2: Configure the server LAN interface on R1.

```
R1(config)# interface FastEthernet0/0
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1.

```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 4 subnets
C       172.17.50.0 is directly connected, FastEthernet0/0
C       172.17.20.0 is directly connected, FastEthernet0/1.20
C       172.17.10.0 is directly connected, FastEthernet0/1.10
C       172.17.99.0 is directly connected, FastEthernet0/1.99
```

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 3: Verify Inter-VLAN routing.

From PC1, verify that you can ping the remote server (172.17.50.254) and the other two hosts (172.17.20.22 and 172.17.10.24). It may take a couple of pings before the end-to-end path is established.

Are the pings successful?

Task 5: Configure port security

Step1: configure port security on port fa0/0

Configure all switches to fulfil the condition that is only one MAC address is allowed to connect with the FastEthernet0/0 port. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3#configure terminal
S3(config)# interface fastethernet0/0
S3(config-if)# switchport mode access
S3(config-if)# switchport port-security
S3(config-if)# switchport port-security maximum 1
S3(config-if)# switchport port-security mac-address sticky
```

LAB 12 - Exercise: Building a Simple Network with VLAN and DHCP Services

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Configure all end devices.
- Configure RIPv2 on all routers.
- Create VLANs

Scenario

Please develop a simulation network as shown in Figure 1. The network has the following requirements:

- All hosts in VLAN11 and VLAN22 will automatically obtain their IP address from the DHCP server
- All end devices (hosts and server) are able to communicate with each other and also to ISP.

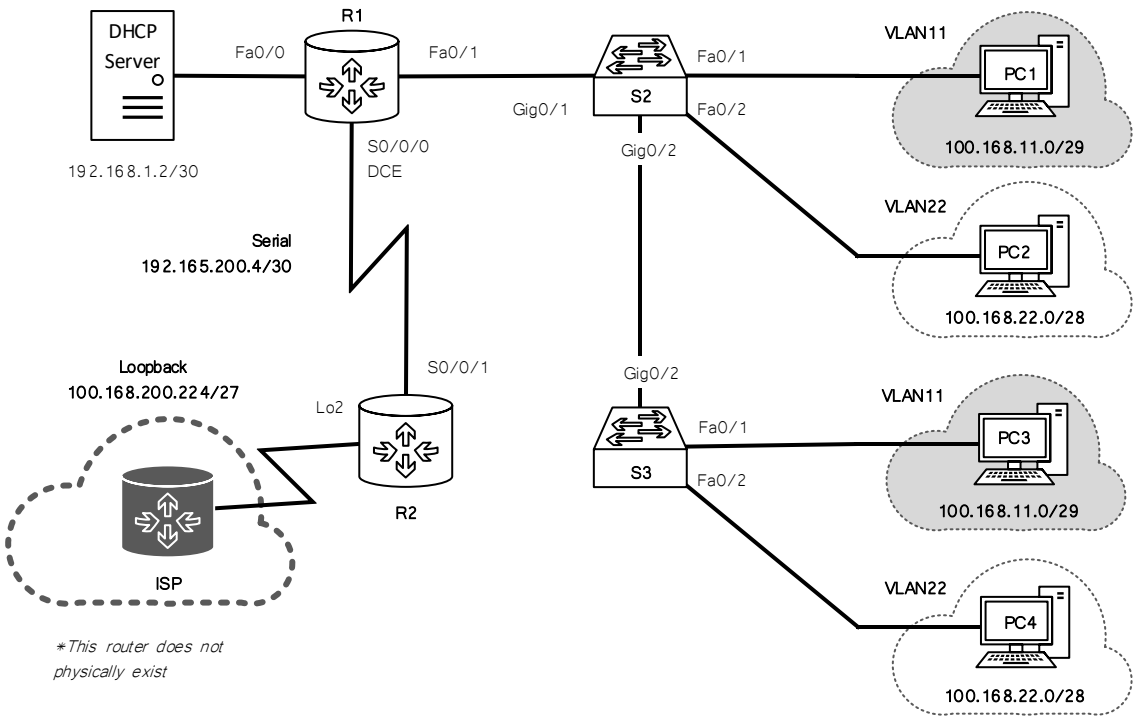

Figure 1 Topology Diagram

Test the Network Design.

Check to see that all devices on directly connected and remote networks can communicate (ping) each other. Complete all tasks in **complete network schematic diagram** and **packet tracer file**.