University of Rwanda (UR) /College of Science and Technology (CST)

School of Engineering/Department: Electrical and Electronic Engineering

Module: ETE 4163, Computer Networks

Laboratory Experiments

Description

Networking is one of the fastest-growing and important fields in the computer industry today. The Internet, interconnecting millions of computers, provides a global communication and resource-sharing infrastructure which elicits many changes in the workplace and in working style. These changes create a growing need for small business and home networks. No computerized office today is able to be productive without some sort of networking technology. Working from home over a network during both business and non-business hours is now currently standard. Realizing these various types of networks requires professionals who are familiar with a variety of networking technologies. Students cannot be expected to compete in the current job market unless they can demonstrate to prospective employers that they have data communication and networking experience that goes beyond the purely theoretical.

The objective of the laboratory experiments is to fully prepare students to be able to set up or maintain networks using current and emerging networking technologies. This document contains two main parts: Lab assignments (1&2) and reports. **Lab assignments will be done into two different ways: using packet tracer and in labs for hands-on practice**.

Reporting

You will prepare a report which summarizes the main tasks and output results of the labs. Your report will include codes and answers to questions given in the lab protocols. **Submission deadline is on 09 January 2025.**

Note: You will need install the ***Cisco Packet Tracer*** software for configuration. The lecturer will guide you about the basics configuration where necessary. In addition to the configuration in Cisco Packet Tracer, students will perform themselves the same configuration in the lab for hands-on practices. Assistance will be provided if needed.

LAB 1: SMALL HOME NETWORK CONFIGURATION USING PACKET TRACER

This Lab1 recapitulates the presentation you learned in class. We will walk through the essentials of setting up a basic home network that consists of a router and a few computers. Setting up an actual network takes time, so we're going to use Cisco Packet Tracer. Packet Tracer is a powerful tool that allows you to virtually simulate network setup just by interacting on your computer.

Step 1. Open **Packet Tracer**> for example, Go to Start. Type "Cisco Packet Tracer" and click the application to open it.

Step 2. Physical Setup. To make a network, we first need a source such as a network hub. For this example, we will use a router>

a) Go ahead and click the **Router** section and choose the **1841 Router** (as example, it may be another router from your choice).
b) Move your mouse to the white space, and click to place the router on the workspace.
c) Click End Devices and click **Generic P**C.
d) Move your mouse to the white space, and click once to place the PC on the workspace.
e) Repeat, and add a second **Generic PC**.
f) Now we are going to connect them together. **Click Connections**.
g) Choose the **Copper Cross-Over** cable.
h) Click on **PC-0** and select **FastEthernet.**
i) Click on the other side to **Router** and select the **FastEthernet0/0**. (or GigabitEthernet0/0)
j) Repeat and connect **PC-1** to the **FastEthernet** interface.
k) Connect **PC-1** to the Router and select **FastEthernet0/1** (or GigabitEthernet0/1)

Step 3. **Router configuration**

1) Click Router0. A window will come up. Go to the **CLI** tab.
2) Type **no** when asked to continue with configuration dialog.
3) Type **enable** to go to "**privileged execution mode**".
4) Type **config t**, to enter "**global configuration mode**".
5) Type **hostname Router0**, to name the router.
6) Type **enable secret class**, to password protect the "privileged execution mode".
7) Configure the password for the console line. Type **line con 0**. Then type **password cisco**, to set the password as cisco.
8) Type **login** to enable password prompting.
9) Type **exit** to return to "global configuration mode".
10) To configure the password for the "virtual terminal lines". Type in **line vty 0 4**. Type in **password cisco**.
11) To enable the password requirement. Type in **login**.

12) Type exit to return to "global configuration mode".

13) We connected the computers (PCs) to the router using the FastEthernet interface. We are going to set up the router to work with those interfaces. Type in **interface (int) GigabitEthernet0/0 (gig 0/0)**

14) Type in **ip address 192.168.1.1 255.255.255.0** (This will set the IP address and Subnet mask of the first FastEthernet Interface)

15) To set a description on the router for later reference. To do this, we will type in **description Router0 FastEthernet0/0** (or GigabitEthernet0/0)

16) To start the interface, we are going to type **no shutdown**.

17) Type **exit** to return to "global configuration mode".

18) Repeat this process with FastEthernet0/1 (GigabitEthernet0/1). Type in interface **FastEthernet0/1** (or **GigabitEthernet0/1)**.

19) This time, type ip address 192.168.2.1 255.255.255.0

20) Type in description **Router0 FastEthernet0/1** (or **GigabitEthernet0/1)**.

21) To start the interface, type **no shutdown**.

22) Type **exit** to exit from "interface configuration mode".

23) Type **exit** to return to "global configuration mode".

24) Hit the Enter key, and we will be back at the "privileged execution mode" when we first started the command line.

25) To check the information that we entered into the system. To do this, type **show running-config**. Continuously hit Enter to scroll down the list. You will see all the configurations you just set. 27. We want the router to run these configurations when it starts up. To do this, we need to copy the configuration files into the Router's NV RAM. To do this, we type **in copy running-config startup-config**. Hit Enter to confirm.
The router configuration is now complete.

Step 4. **PC configuration**

We are now going to configure the computers to connect to the network

1) First, click on **PC-0**. A configuration window will come up.

2) Go to the **Desktop tab** and click **IP Configuration**.

3) We will set a Static IP.

4) Set the IP Address to 192.168.1.2

5) Set the Subnet Mask to 255.255.255.0

6) Set the Default Gateway to 192.168.1.1

7) Close the PC-0 configuration window.

8) Repeat with PC-1, except use 192.168.2.2 for the IP Address.

9) Set the Subnet Mask to 255.255.255.0

10) Set the Default Gateway to 192.168.2.1

11) Close the PC-1 configuration window.

By now, you should see green dots on the cables connected to the devices.

Step 5. **Testing connectivity:**

We are going to test for a valid connection by pinging PC-1 from PC-0.

1) To do this, click **PC-0**. Go to the **Desktop** tab and click **Command Prompt**. This acts very similar to a DOS prompt in a Windows OS.

2) To see the details of the computer's local network, we can type in i**pconfig**.

3) To ping PC-1 by typing in **ping 192.168.2.2** At first, the request might time-out, but you should get a reply after that.

Step 6. Testing for Connectivity using Simulation Mode

1) At the bottom right corner, click the "**stopwatch**" icon to activate **Simulation Mode**.

2) Click **Edit Filters**. Clear the selections. Select only **ICMP**.

3) Click anywhere to get out.

4) Look at the bar of items on the right hand side. Click the **Closed Envelope** + button. This will allow us to choose a source to test our network.

5) Click **PC-0** and then click **PC-1**.

6) Click **Auto Capture/Play** to begin simulation. You should now see an envelope going from **PC-0 to the Router to PC-1 and back**.

After that, you have successfully completed your network setup

LAB 2: BASIC NETWORK DEVICES CONFIGURATION

Learning Objectives:

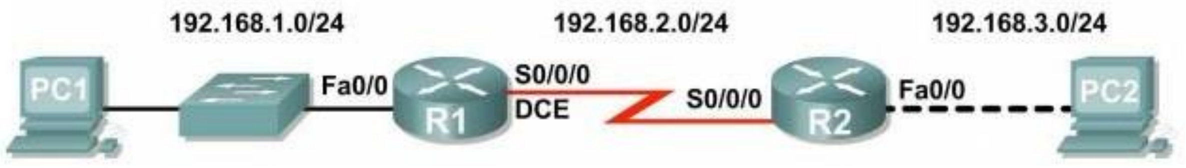
Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram.
- Perform basic configuration tasks on a router.
- Configure and activate Ethernet interfaces.
- Test and verify configurations.
- Reflect upon and document the network implementation.

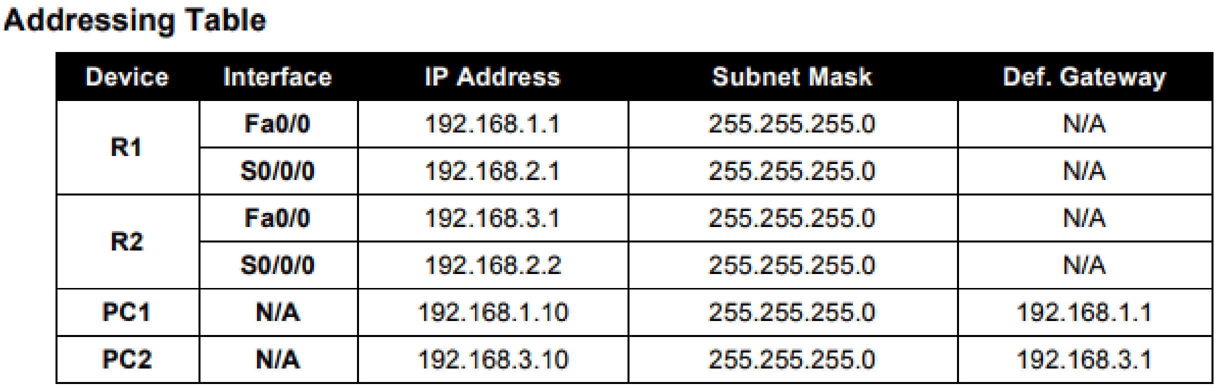
Scenario:

In this lab activity, you will create a network that is similar to the one shown in the below topology diagram. Begin by cabling the network as shown in the topology diagram. You will then perform the initial router configurations required for connectivity. Use the IP addresses that are provided in the topology diagram to apply an addressing scheme to the network devices. When the network configuration is complete, examine the routing tables to verify that the network is operating properly.

I. Topology Diagram



II. Addressing Table



Addressing Table

Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

TASK 1: CABLE THE NETWORK.

Cable a network that is similar to the one in the Topology Diagram. The output used in this lab is from 1841 routers. You can use any current router in your lab as long as it has the required interfaces as shown in the topology. Be sure to use the appropriate type of Ethernet cable to connect from host to switch, switch to router, and host to router. Be sure to connect the serial DCE cable to router R1 and the serial DTE cable to router R2.

Answer the following questions:

a) What type of cable is used to connect the Ethernet interface on a host PC to the Ethernet interface on a switch? Copper Straight-Through Cable

b) What type of cable is used to connect the Ethernet interface on a switch to the Ethernet interface on a router? Copper Straight-Through Cable

c) What type of cable is used to connect the Ethernet interface on a router to the Ethernet interface on a host PC? Copper Cross-Over Cable

TASK 2: PERFORM BASIC CONFIGURATION OF ROUTER R1.

Step 1: Establish a HyperTerminal session to router R1.

Step 2: Enter privileged EXEC (execute) mode.

```
 Router>enable

Router#
```

Step 3: Enter global configuration mode.

```
Router#configure terminal

 Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#
```

Step 4: Configure the router name as R1.

Enter the command hostname R1 at the prompt.

```
Router(config)#hostname R1 R1(config)#
```

Step 5: Disable DNS lookup. Disable DNS lookup with the no ip domain-lookup command.

```
R1(config)#no ip domain-lookup

R1(config)#
```

Answer these questions:

a) Why would you want to disable DNS lookup in a lab environment?
To prevent delays caused by mistyped commands triggering unnecessary DNS resolution.

b) What would happen if you disabled DNS lookup in a production environment?
Domain names would not resolve, potentially disrupting services dependent on DNS.

Step 6: Configure the EXEC mode password.

Configure the EXEC mode password using the enable secret password command. Use class for the password.

```
R1(config)#enable secret class

R1(config)#
```

Answer this question:

Why is it not necessary to use the enable password password command?
The enable password command stores the password in plain text, whereas enable secret encrypts it, making enable password redundant and less secure.

Step 7: Configure a message-of-the-day banner.

Configure a message-of-the-day banner using the banner motd command.

```
R1(config)#banner motd &

Enter TEXT message. End with the character '&'.

********************************

!!!AUTHORIZED ACCESS ONLY!!!

********************************

 &

 R1(config)#
```

Answer these questions:

a) When does this banner display?
The motd banner displays before login when someone accesses the router via console, Telnet, or SSH.

b) Why should every router have a message-of-the-day banner?
It provides a security warning to unauthorized users, indicating restricted access and discouraging misuse.

Step 8: Configure the console password on the router.

Use cisco as the password. When you are finished, exit from line configuration mode.

```
R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#
```

Step 9: Configure the password for the virtual terminal lines.

Use cisco as the password. When you are finished, exit from line configuration mode.

```
R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit R1(config)#
```

Step 10: Configure the FastEthernet0/0 interface.

Configure the FastEthernet0/0 interface with the IP address 192.168.1.1/24.

```
R1(config)#interface fastethernet 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

 R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#
```

Step 11: Configure the Serial0/0/0 interface. Configure the Serial0/0/0 interface with the IP address 192.168.2.1/24. Set the clock rate to 64000.

```
R1(config-if)#interface serial 0/0/0
```

```
R1(config-if)#ip address 192.168.2.1 255.255.255.0

R1(config-if)#clock rate 64000

R1(config-if)#no shutdown

R1(config-if)#
```

Note: The interface will be activated until the serial interface on R2 is configured and activated

Answer the following question:

What is the purpose of the clock rate command? The clock rate command sets the timing for data transmission on the DCE side of a serial link to synchronize communication between connected devices.

Step 12: Return to privileged EXEC mode. Use the end command to return to privileged EXEC mode.

```
 R1(config-if)#end

R1#
```

Step 13: Save the R1 configuration. Save the R1 configuration using the copy running-config startup-config command.

```
R1#copy running-config startup-config

Building configuration...

 [OK]

R1#
```

Answer this question:

What is a shorter version of this command? R1# write memory

TASK 3: PERFORM BASIC CONFIGURATION OF ROUTER R2.

Step 1: For R2, repeat Steps 1 through 9 from Task 2.

Step 2: Configure the Serial 0/0/0 interface.

Configure the Serial 0/0/0 interface with the IP address 192.168.2.2/24.

```
R2(config)#interface serial 0/0/0

R2(config-if)#ip address 192.168.2.2 255.255.255.0

R2(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#
```

Step 3: Configure the FastEthernet0/0 interface.

Configure the FastEthernet0/0 interface with the IP address 192.168.3.1/24.

```
R2(config-if)#interface fastethernet 0/0

R2(config-if)#ip address 192.168.3.1 255.255.255.0

R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#
```

Step 4: Return to privileged EXEC mode.

Use the end command to return to privileged EXEC mode.

```
R2(config-if)#end

R2#
```

Step 5: Save the R2 configuration. Save the R2 configuration using the copy running-config startup-config command.

```
R2#copy running-config startup-config

Building configuration... [OK]

R2#
```

TASK 4: CONFIGURE IP ADDRESSING ON THE HOST PCs.

Step 1: Configure the host PC1.

Configure the host PC1 that is attached to R1 with an IP address of 192.168.1.10/24 and a default gateway of 192.168.1.1.

Step 2: Configure the host PC2.

Configure the host PC2 that is attached to R2 with an IP address of 192.168.3.10/24 and a default gateway of 192.168.3.1.

TASK 5: VERIFY AND TEST THE CONFIGURATIONS.

Step 1: Verify that routing tables have the following routes using the show ip route command.

You can see that both R1 and R2 have two routes. Both routes are designated with a C. These are the directly connected networks that were activated when you configured the interfaces on each router. If you do not see two routes for each router as shown in the following output, proceed to Step 2.

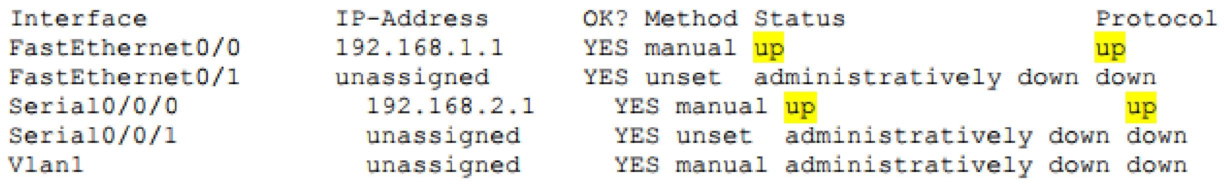
```
R1#show ip route

Codes:

C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1,
E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route


Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0/0
-----------------------------
```

```
R2#show ip route

Codes:

C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route


Gateway of last resort is not set

C 192.168.2.0/24 is directly connected, Serial0/0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/0
```

Step 2: Verify interface configurations.

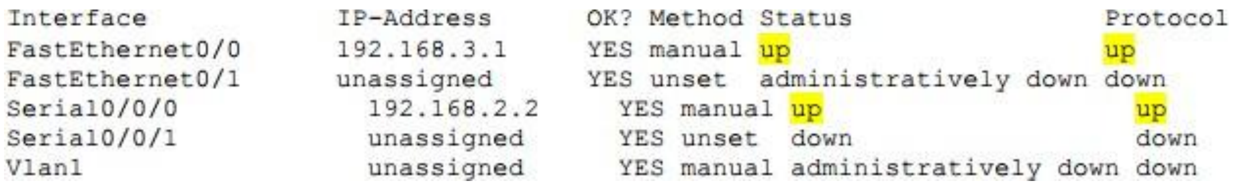
Another common problem is router interfaces that are not configured correctly or not activated. Use the show ip interface brief command to quickly verify the configuration of each router's interfaces. Your output should look similar to the following:

R1#show ip interface brief



```
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0              192.168.2.1     YES manual up                    up
Serial0/0/1              unassigned      YES unset  administratively down down
Vlan1                    unassigned      YES manual administratively down down
```

R2#show ip interface brief



```
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.3.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0              192.168.2.2     YES manual up                    up
Serial0/0/1              unassigned      YES unset  down                  down
Vlan1                    unassigned      YES manual administratively down down
```

If both interfaces are up and up, then both routes will be in the routing table. Verify this again by using the **show ip route** command

Step 3: Test connectivity.

Test connectivity by pinging from each host to the default gateway that has been configured for that host.

Questions:

From the host attached to R1, is it possible to ping the default gateway? ___yes___

From the host attached to R2, is it possible to ping the default gateway? ___yes___

If the answer is no for any of the above questions, troubleshoot the configurations to find the error using the following systematic process

1) Check the PCs.

Are they physically connected to the correct router? (Connection could be through a switch or directly.) ___yes___

Are link lights blinking on all relevant ports? ___yes___

2) Check the PC configurations.

Do they match the Topology Diagram? ___yes___

3) Check the router interfaces using the show ip interface brief command. Are the interfaces up and up? ___yes___

If your answer to all three steps is yes, then you should be able to successfully ping the default gateway.

Step 4: Test connectivity between router R1 and R2.

From the router R1, is it possible to ping R2 using the command ping 192.168.2.2? ____yes________

From the router R2, is it possible to ping R1 using the command ping 192.168.2.1? ____yes________

If the answer is no for the questions above, troubleshoot the configurations to find the error using the following systematic process:

1) Check the cabling.

Are the routers physically connected? ____yes________

Are link lights blinking on all relevant ports? ____yes________

2) Check the router configurations.

Do they match the Topology Diagram? ____yes________

Did you configure the clock rate command on the DCE side of the link? ____yes________

3) Check the router interfaces using the show ip interface brief command.

Are the interfaces “up” and “up”? ________yes____

If your answer to all three steps is yes, then you should be able to successfully ping from R2 to R1 and from R2 to R3.

TASK 6: REFLECTION

Step 1: Attempt to ping from the host connected to R1 to the host connected to R2. This ping should be unsuccessful.

Step 2: Attempt to ping from the host connected to R1 to router R2. This ping should be unsuccessful.

Step 3: Attempt to ping from the host connected to R2 to router R1. This ping should be unsuccessful. What is missing from the network that is preventing communication between these devices?

TASK 7: DOCUMENTATION

On each router, capture the following command output to a text (.txt) file and save for your report (to be included in your lab report)

- show running-config
- show ip route
- show ip interface brief

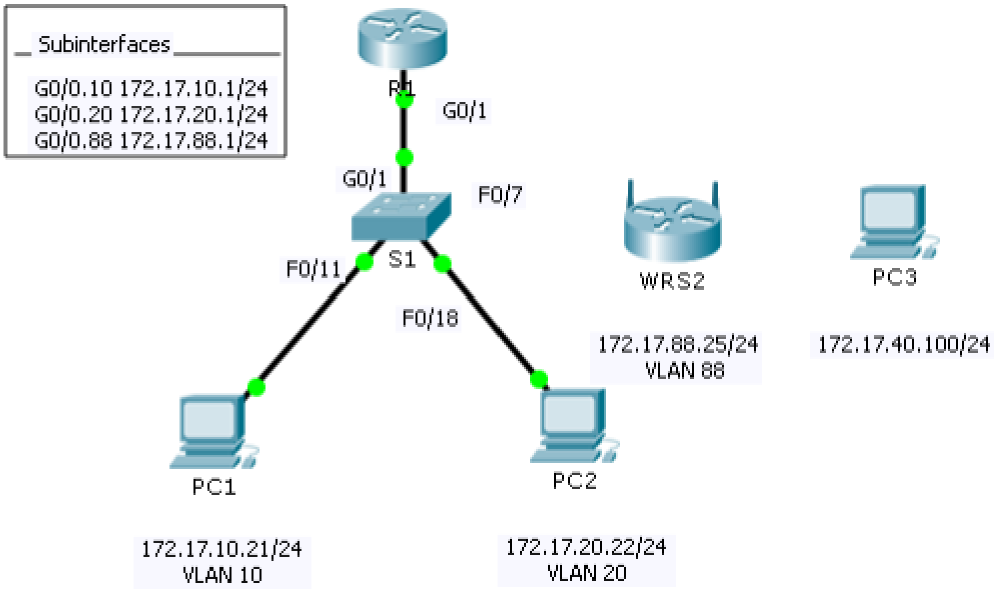
LAB3: CONFIGURING WIRELESS LAN ACCESS

Scenario:
In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WPA2 security. You will manually configure PC wireless connectivity by entering the Linksys router SSID and password.

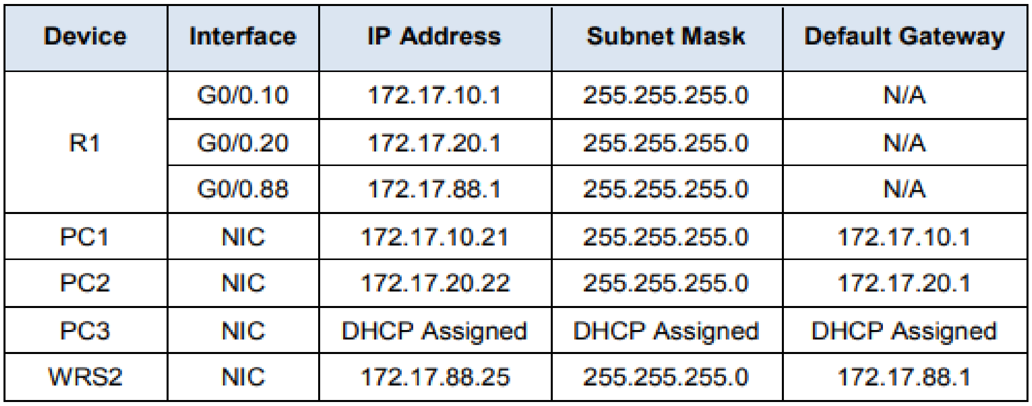
Objectives of Lab:

- Part 1: Configure a Wireless Router
- Part 2: Configure a Wireless Client
- Part 3: Verify Connectivity

1. Topology



2. Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.20	172.17.20.1	255.255.255.0	N/A
	G0/0.88	172.17.88.1	255.255.255.0	N/A
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
PC3	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
WRS2	NIC	172.17.88.25	255.255.255.0	172.17.88.1

Part 1: Configure a Wireless Router

- **Step 1**: Connect the Internet interface of WRS2 to S1.
  Connect the WRS2 Internet interface to the S1 F0/7 interface.
- **Step 2**: Configure the Internet connection type.
  a) Click WRS2 > GUI tab.
  b) Set the Internet Connection type to Static IP.
  c) Configure the IP addressing according to the Addressing Table.
- **Step 3:** Configure the network setup.
  a) Scroll down to Network Setup. For the Router IP option, set the IP address to 172.17.40.1 and the subnet mask to 255.255.255.0.
  b) Enable the DHCP server.
  c) Scroll to the bottom of the page and click Save Settings.
- **Step 4**: Configure wireless access and security.
  a) At the top of the window, click Wireless. Set the Network Mode to Wireless-N Only and change the SSID to WRS_LAN.
  b) Disable SSID Broadcast and click Save Settings.
  C) Click the Wireless Security option.
  d) Change the Security Mode from Disabled to WPA2 Personal.
  e) Configure cisco123 as the passphrase.
  f) Scroll to the bottom of the page and click Save Settings

Part 2: Configure a Wireless Client

- **Step 1:** Configure PC3 for wireless connectivity.

  Because SSID broadcast is disabled, you must manually configure PC3 with the correct SSID and passphrase to establish a connection with the router.

a) Click PC3 > Desktop > PC Wireless.
b) Click the Profiles tab.
c) Click New.
d) Name the new profile Wireless Access.
e) On the next screen, click Advanced Setup. Then manually enter the SSID of WRS_LAN on
Wireless Network Name. Click Next.
f) Choose Obtain network settings automatically (DHCP) as the network settings, and then
click Next.
g) On Wireless Security, choose WPA2-Personal as the method of encryption and click Next.
h) Enter the passphrase cisco123 and click Next.
i) Click Save and then click Connect to Network.

- **Step 2:** Verify PC3 wireless connectivity and IP addressing configuration. The Signal Strength and Link Quality indicators should show that you have a strong signal. Click More Information to see details of the connection including IP addressing information. Close the PC Wireless configuration window.

Part 3: Verify Connectivity

All the PCs should have connectivity with one another.

LAB4: CONFIGURING Virtual LANs (VLANs)

A Virtual Local Area Network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. By creating VLANs, you are able to create smaller broadcast domains within a switch by assigning different ports in the switch to different subnetworks. A VLAN is treated like its own subnet or broadcast domain. This means that frames broadcasted onto a network are only switched between ports in the same VLAN. Using virtual LANs, you're no longer confined to creating workgroups by physical locations. VLANs can be organized by location, function, department, or even the application or protocol used, regardless of where the resources or users are located.

In this Lab, we will review what a VLAN is and how VLAN memberships are used in a switched internetwork. Trunking FastEthernet links will also be discussed. Trunking allows you to send information about all VLANs across one link.

VLANs are typically created by an administrator, who then assigns switch ports to the VLAN. These are called static VLANs. If the administrator wants to do a little more work up front and assign all the host devices' hardware addresses into a database, the switches can be configured to assign VLANs dynamically. In this Lab we will discuss the static VLANs.

Static VLANs

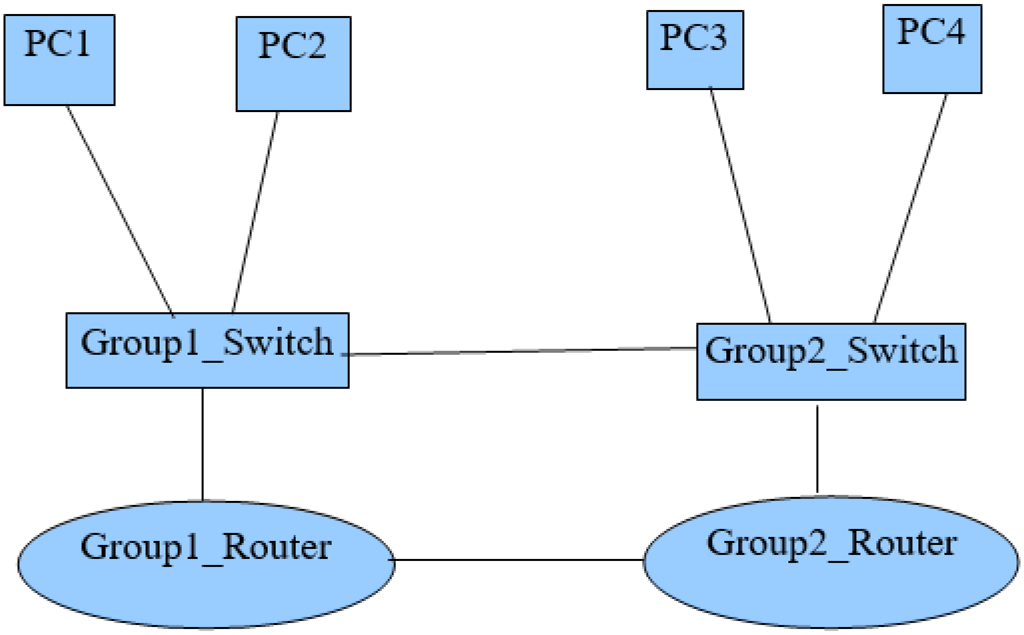
Static VLANs are the typical way of creating VLANs and the most secure. The switch port that you assign a VLAN association always maintains that association until an administrator changes the port assignment. This type of VLAN configuration is easy to set up and monitor, working well in a network where the movement of users within the network is controlled. The next sections will cover the following:

- Configuring VLANs
- Assigning Switch ports to VLANs
- Configuring trunk ports
- Configuring VTP (VLAN Trunking Protocol)
- Configuring Inter-VLAN Routing
-

Configuring VLANs

Configuring VLANs is the easy part of the job. It is trying to understand which users you want in each VLAN that is time consuming. Once you have decided the number of VLANs you want to create and the users that will be members of each VLAN, you can create your VLAN.

In our internetwork, we are going to use the following network setup:



In our internetwork, we have two 2960 switches ready to configure VLANs. We will follow the following instructions:

- We will create two (2) VLANs in each switch: ***vlan 2*** and ***vlan 3*** which will be named Group1_Switch and Group2_Switch respectively.
- ***vlan 2*** will have the subnet 192.168.20.0/24 and ***vlan 3*** will have the subnet 192.16.30.0/24.
- You are probably wondering why we Started with ***vlan 2*** instead of ***vlan 1?*** It is because VLAN1 is a native VLAN for all switches by default; i.e., all switch ports that are not part of any VLAN belong to ***vlan 1*** by default. In our internetwork, ***vlan 1*** will have the subnet 192.16.10.0/24.
- PC1 and PC3 belong to ***vlan 2*** while PC2 and PC4 belong to ***vlan 3***
- The two switches are connected through their respective FastEthernet 0/4 interfaces, while the FastEthernet 0/2 and 0/3 interfaces are connected to the PCs
- Group2_Switch will be the VTP server, the other switch(es) will be the client
- Group1_Router will be used to configure the inter-VLAN routing, through its FastEthernet 0/0 interface.

Let's start by adding hostnames, passwords, interface description and IP addresses to each switch: (eg: on Group1_Switch).

Switch(config)#hostname *Group1_Switch*

Group1_Switch(config)#enable secret *student*

Group1_Switch(config)# line con 0

```
Group1_Switch(config-line)#login

Group1_Switch(config-line)#password student

Group1_Switch(config-line)#line vty 0 15

Group1_Switch(config-line)#login

Group1_Switch(config-line)#password student

Group1_Switch(config)# int f0/1

Group1_Switch(config-if)#description connection to Router

Group1_Switch(config-if)# int  f0/4

Group1_Switch(config-if)#description connection to Group2_Switch

Group1_Switch(config-if)#int vlan 1

Group1_Switch(config-if)#ip address 192.16.10.2 255.255.255.0

Group1_Switch(config-if)#no shutdown

Group1_Switch(config)# ip default gateway 192.16.10.1 (this is the ip of f0/0 of Group1_router which is the port that will be used for inter-vlan routing)
```

To verify if your configurations are correct, use the ping command and check if all switches can talk to each other. If it is that case then proceed to next step, otherwise, re-check the configurations.

Now we can create our VLANS. Use the following commands:

```
switch(config)#vlan 2

switch(config-vlan)#name Group1

switch(config)#vlan 3

switch(config-vlan)#name Group2
```

Use the ***show vlan brief*** command to verify your VLAN information on your switches.

Assigning Switch ports to VLANs

```
swith(config)# interface fa0/2

swith(config-if)# switchport access [which VLAN?]
swith(config)# interface fa0/3
swith(config-if)# switchport access [which VLAN?]
```

Trunking

Now that the two switches are configured with all the basic administrative information and can ping each other, let's set the trunking on the ports connecting each switch together:

To enable the trunking, use the command ***switchport mode trunking:***

On Group_Switch1, we will enable trunking on 2 interfaces while on Group_Switch2, we will enable it on one interface. Which are these interfaces?

Use the ***show interface trunk*** command to verify your trunk information

VTP configuration

As mentioned in the instructions above, the Group1_switch will act as a VTP server and the Group2_switch will be the VTP client. 2960 switches (actually, all switches) are configured to be VTP servers by default. To configure VTP, first configure the domain name you want to use, all servers that need to share information must use the same Domain name and a switch can be in only one domain at a time.

Use these commands to configure VTP:

vtp domain [name]*: to set the name of the administration domain.*

vtp mode server**:** to enable routing on the router which is the server (swith1 in this case) and use the ***vtp mod client***: on the rest of the switches which will be the clients.

If you have done the vtp configs correctly, you will notice that on the second switch you will immediately have the VLANs information and yet you didn't create them there... That is the advantage of VTP, it allows an administrator to add, delete, and rename VLANs information that is then propagated to all other switches in the VTP domain. So, if we want to add more VLANs in our switches, we just need to create them only in the switch acting as VTP server and the rest of the switches will get information about those new VLANs through VTP.

Configuring Inter-VLAN Routing

Both Switches are completely configured, and we verified that it is all good. The hosts can communicate with hosts that are members of the same VLAN, right? Right. If we want to have all our hosts talking, we need a router or a layer 3 switch to make that happen.

In our internetwork, we are going to use Group1_Router to configure inter-VLAN communication. To do this, we are going to use the router approach; the router's interface (***fastEthernet 0/0*** in our case) is divided into logical interfaces; one for each VLAN. These are called ***subinterfaces*.**

Here is how you will configure this inter-vlan routing:

```
router(config)# int f0/0

router(config-if)# no ip address

router(config-if)# no shutdown

router(config-if)# int f0/0.1

router(config-subif)# int f0/0.1 ( notice how the prompt has changed to subinterface
                                   configuration mode!!!!)

router(config-subif)#encapuslation dot1q  1 [What is 1 in this command???]

router(config-subif)# ip address 192.168.10.1 255.255.255.0

router(config-subif)#int  f0/0.2

router(config-subif)#encapuslation dot1q  2 [What is 2 in this command???]

router(config-subif)#ip address 192.168.20.1 255.255.255.0 (Remember we said Vlan 2 will have
subnet 192.16.20.0 and VLAN3 will have 192.16.30.0)

router(config-subif)# outer(config-subif)#int  f0/0.3

router(config-subif)#encapuslation dot1q 3 [What is 3 in this command???]

router(config-subif)#ip address 192.168.30.1 255.255.255.0
```

When configuring this router, we created three sub-interfaces; one for each VLAN. Remember that the sub-interface number is not really important except for administration, but we did match the VLAN number so it is easy to remember.

At this point, if all went well, ours hosts should be able to talk to each other; try to ping a host that is not in the same VLAN, it should work. If not, re-check your configurations.