Practical Workbook

CS-351/CS-418
COMPUTER COMMUNICATION NETWORKS
(TCIT / SE / EE)

Name : ___

Year : _____

Batch : _____

Roll No : _____

Department: _____

Department of Computer & Information Systems Engineering
NED University of Engineering & Technology

INTRODUCTION

The days of mainframe computing using dumb terminals are long gone. The present time is the era of very powerful personal computers, interconnecting with each other and even better equipped servers, sometimes connecting across continental boundaries.

Computer Communication Networks is a senior level undergraduate course in Computer and Information Systems Engineering, which covers various aspects of computer networks. It covers various classifications of computer networks and gives the students a good grasp on the various topics in computer networks. This laboratory manual aims to augment the classroom teaching of the course and to provide the students essential practical knowledge in the subject.

The first and second labs deal with learning IPv4 Addressing, Sub-netting & Variable Length Subnet Masking (VLSM).

The third lab deals with making crossover and straight-through UTP cables. This skill will come in very handy in various trades when the students go into practical life. It introduces some related standards and equipment used in this regard.

The fourth lab jumps into Cisco routers. It is a hands-on exercise using some commonly used Cisco IOS commands. In this lab, the students will learn how to connect to and interact with Cisco routers.

The fifth lab is about connecting different IP networks by defining static routes all around.

Sixth lab introduces dynamic routing using a simple routing protocol, namely RIP (Routing Information Protocol) and its later version called RIP version 2. In following two labs configuration and debugging of two more dynamic routing protocols are explored, that are OSPF and EIGRP.

The ninth lab teaches task of everyone's interest, i.e. connecting to internet using PPP

Labs through ten to fourteen are based on switching and cover basic LAN switch operation, loop avoidance using Spanning Tree Protocol and Virtual LANs and reducing administration overhead by using VLAN Trunking Protocol in switched network.

As careful as one might be, the disaster of lost, forgotten or stolen password will, nonetheless, strike sooner or later. Fifteenth, the last lab teaches how to do disaster recovery on a Cisco router in terms of recovering a forgotten password.

CONTENTS

Lab Session 01

OBJECT

Learning IPv4 Addressing & Sub-netting (Class C Addresses)

THEORY

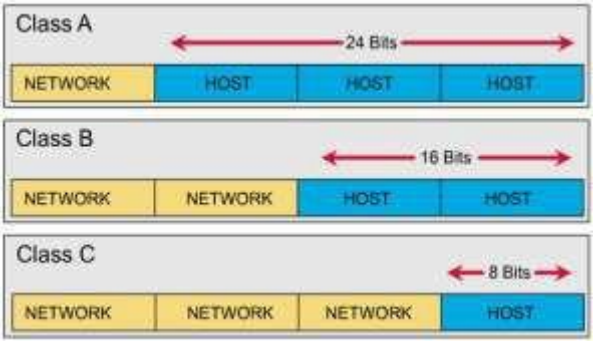
IP ADDRESS & SUBNET MASK

An IP (Internet Protocol) address uniquely identifies a node or host connection to an IP network. System administrators or network designers assign IP addresses to nodes. IP addresses are configured by software and are not hardware specific. An IP address is a 32 bit binary number usually represented as four fields each representing 8 bit numbers in the range 0 to 255 (sometimes called octets) separated by decimal points.
For example: 150.215.17.9

It is sometimes useful to view the values in their binary form.

150.215.17.9
10010110.11010111.00010001.00001001

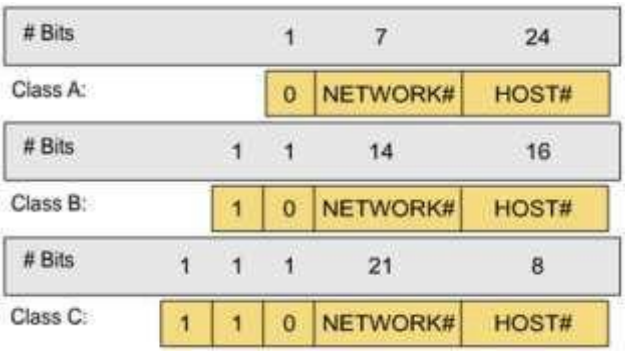
An IP address consists of two parts, one identifying the network and one identifying the node. The class of the address determines which part belongs to the network address which part belongs to the node address.



An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>)
A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.

CLASSFUL ADDRESSING

IPv4 addressing used the concept of classes. This architecture is called classful addressing. The address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.



We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class

of the address. If the address is given in decimal-dotted notation, the first byte defines the class.

Class	Starts with	Binary range	Decimal Value range	Maximum subnets	Maximum hosts	Routing mask
A	0	00000000-01111111	0-127*	127	16,777,214	255.0.0.0
B	10	10000000-10111111	128-191	16,384	65,534	255.255.0.0
C	110	11000000-11011111	192-223	2,097,152	254	255.255.255.0
D	1110	11100000-11101111	224-239			
E	1111	11110000-11111111	240-255			

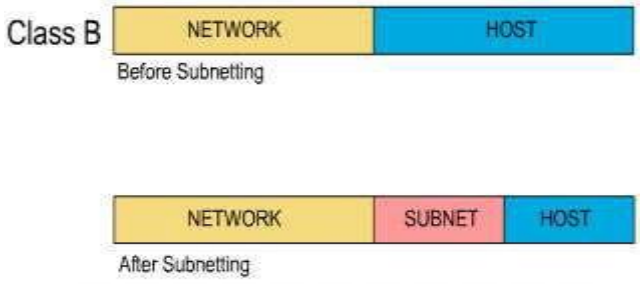
* The 0 octet is forbidden in the RFC, and 127 is reserved for loopback testing.

Network & Broadcast Addresses

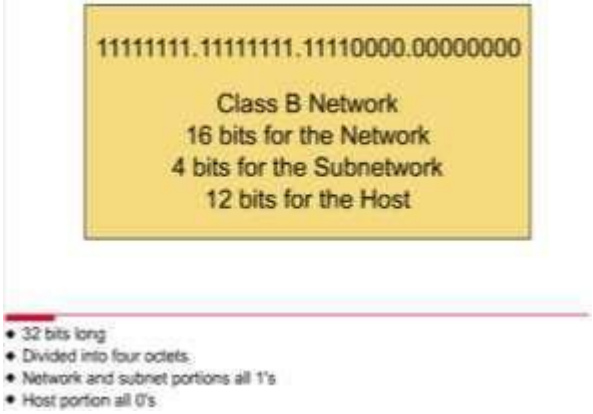
- An IP address such as 176.10.0.0 that has all binary 0s in the host bit positions is reserved for the network address.
- An IP address such as 176.10.255.255 that has all binary 1s in the host bit positions is reserved for the broadcast address.

SUB-NETTING

To create a subnet address, a network administrator borrows bits from the original host portion and designates them as the subnet field.



Consider the following example:



Sub-netting Class C Addresses

In a Class C address, only 8 bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

Binary (4th Octect)	Decimal (4th Octect)	CIDR (Classless Inter-Domain Routing) or slash notation
10000000	128	/25
11000000	192	/26
11100000	224	/27
11110000	240	/28
11111000	248	/29
11111100	252	/30

Now determine the following:

How many subnets? 2^x = number of subnets. *x* is the number of masked bits, or the 1s. For example, in 11000000, the number of ones gives us 2^2 subnets. In this example, there are 4 subnets.

How many hosts per subnet? $2^y – 2$ = number of hosts per subnet. *y* is the number of unmasked bits, or the 0s. For example, in 11000000, the number of zeros gives us $2^6 – 2$ hosts. In this example, there are 62 hosts per subnet. You need to subtract two for the subnet address and the broadcast address, which are not valid hosts.

What are the valid subnets? 256 – Subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64, 128, 192.

What's the broadcast address for each subnet? Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128, etc. The broadcast of the last subnet is always 255 for Class C.

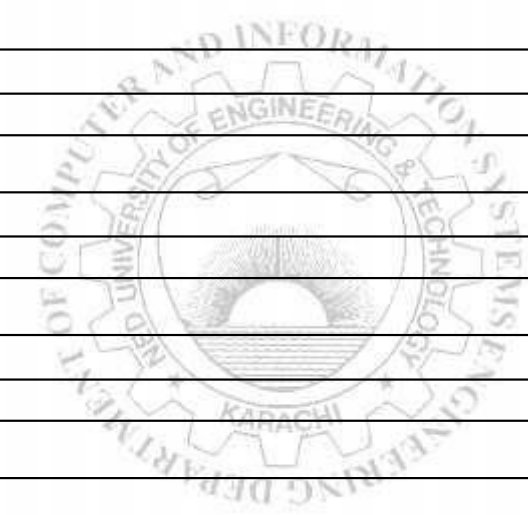
What are the valid hosts? Valid hosts are the numbers between the subnets, omitting all the 0s and all 1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range—it's *always* the numbers between the subnet address and the broadcast address.

EXERCISES

1. ***Find the class of each address.***
   - ***a.*** **00000001 00001011 00001011 11101111**
   - ***b.*** **11000001 10000011 00011011 11111111**
   - ***c.*** **14.23.120.8**
   - ***d.*** **252.5.15.111**

2. **Subnets the following addresses and verify your results using any *online IPv4 Addressing & Sub-netting Calculator and attach their screen shots.***

   - ***a. 192.168.10.0 (/26)***
   - ***b. 192.168.10.0 (/27)***


COMPUTER AND INFORMATION SYSTEMS ENGINEERING DEPARTMENT OF
NED UNIVERSITY OF ENGINEERING & TECHNOLOGY
KARACHI

Lab Session 02

OBJECT

Learning Sub-netting (Class B & A addresses) & VLSM

THEORY

Sub-netting Class B Addresses

Binary (3rd and 4thOctet)	Decimal (All Octets)	CIDR (Classless Inter-Domain Routing) or slash notation
10000000 00000000	255.255.128.0	/17
11000000 00000000	255.255.192.0	/18
11100000 00000000	255.255.224.0	/19
11110000 00000000	255.255.240.0	/20
11111000 00000000	255.255.248.0	/21
11111100 00000000	255.255.252.0	/22
11111110 00000000	255.255.254.0	/23
11111111 00000000	255.255.255.0	/24
11111111 10000000	255.255.255.128	/25
11111111 11000000	255.255.255.192	/26
11111111 11100000	255.255.255.224	/27
11111111 11110000	255.255.255.240	/28
11111111 11111000	255.255.255.248	/29
11111111 11111100	255.255.255.252	/30

Then determine all the parameters discussed in Lab 01 in Sub-netting Class C Address section.

Sub-netting Class A Addresses

Note that the Class A addresses can be sub-netted in the same way as for Class C & B. However, in that case we have sub-netting possible in 3 octets as opposed to 1 or 2 subnets as in Class C or B respectively.

VARIABLE LENGTH SUBNET MASKING (VLSM)

Variable Length Subnet Masking (VLSM) is a way of further sub-netting a subnet. Using Variable Length Subnet Masking (VLSM) we can allocate IP addresses to the subnets by the exact need (*in the power f 2*).
Variable Length Subnet Masking (VLSM) allows us to use more than one subnet mask within the same network address space.
If we recollect from the previous lessons, we can divide a network only into subnets with equal number of IP addresses. Variable Length Subnet Masking (VLSM) allows creating subnets from a single network with unequal number of IP addresses.

Example: We want to divide 192.168.10.0, which is a Class C network, into four networks, each with unequal number of IP address requirements as shown below.
Subnet A : 126 IP Addresses
Subnet B : 62 IP Addresses
Subnet C : 30 IP Addresses
Subnet D : 30 IP Addresses

Original Network (Network to be subnetted) – 192.168.10.0/24

(VLSM) - First Division

Divide the two networks equally with 128 IPv4 addresses (126 usable IPv4 addresses) in each network using 255.255.255.128subnet mask (192.168.10.0/25).

We will get two subnets each with 128 IPv4 addresses (126 usable IPv4 addresses).

1) 192.168.10.0/25, which can be represented in binaries as below.

11000000.10101000.00001010.00000000
11111111.11111111.11111111.10000000

2) 192.168.10.128/25, which can be represented in binaries as below.

11000000.10101000.00001010.10000000
11111111.11111111.11111111.10000000

(VLSM)- Second Division

Divide second subnet (192.168.10.128/25) we got from the first division again into two Networks, each with 64 IP Addresses (62 usable IPv4 addresses) using 255.255.255.192 subnet mask.

We will get two subnets each with 64 IPv4 addresses (62 usable IPv4 addresses).

1) 192.168.10.128/26, which can be represented in binaries as below.

11000000.10101000.00001010.10000000
11111111.11111111.11111111.11000000

2) 192.168.10.192/26

11000000.10101000.00001010.11000000
11111111.11111111.11111111.11000000

(VLSM) - Third Division

Divide 192.168.10.192/26 Network again into two Networks, each with 32 IPv4 addresses (30 usable IPv4 addresses) using 255.255.255.224 subnet mask

We will get two subnets each with 32 IPv4 addresses (30 usable IPv4 addresses).

1) 192.168.10.192/27, which can be represented in binaries as below.

11000000.10101000.00001010.11000000
11111111.11111111.11111111.11100000

2) 192.168.10.224/27, which can be represented in binaries as below.

11000000.10101000.00001010.11100000
11111111.11111111.11111111.11100000

Now we have split the 192.168.10.0/24 network into four subnets using Variable Length Subnet Masking (VLSM), with unequal number of IPv4 addresses as shown below. Also note that when you divide a network using Variable Length Subnet Masking (VLSM), the subnet masks are also different.

1)	192.168.10.0	-	255.255.255.128	(126	(128-2)	usable IPv4 addresses)
2)	192.168.10.128	-	255.255.255.192	(62	(64-2)	usable IPv4 addresses)
3)	192.168.10.192	-	255.255.255.224	(30	(32-2)	usable IPv4 addresses)
4)	192.168.10.224	-	255.255.255.224	(30	(32-2)	usable IPv4 addresses)

EXERCISES

1. **Subnets the following addresses and verify your results using any *online IPv4 Addressing & Sub-netting Calculator and attach their screen shots.***
   a. ***172.16.0.0 (/19)***
   b. ***10.0.0.0 (/10)***

2. Given a Class C network address **192.168.10.0 (/24)**. Divide it into three sub-networks each with unequal number of hosts' requirement as shown below:
   Subnet A: 90 Hosts, Subnet B: 23 Hosts, Subnet C: 7 Hosts.

Summarize the results in a table. *(For each subnet, list required hosts, possible hosts and N/W Address)*

Lab Session 03

OBJECT

Making the following kinds of UTP cables:

1. ***Straight through cable***
2. ***Cross cable***

THEORY

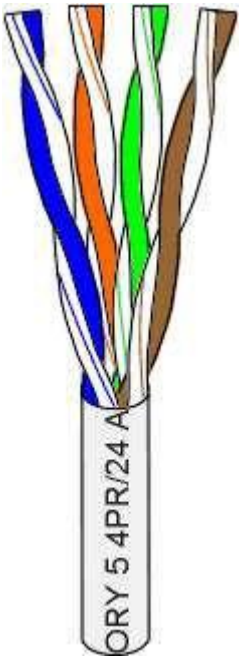


Figure 3.1: UTP cable

There are several classifications of twisted pair cable. Let's skip right over them and state that we'll use Category 5 (or CAT 5) cable for all new installations. Likewise, there are several fire code classifications for the outer insulation of CAT 5 cable. We'll use CMR cable, or "riser cable," for most of the wiring we do. You should also be aware of CMP or plenum cable (a plenum is used to distribute air in a building) you may be required by local or national codes to use the more expensive plenum-jacketed cable if it runs through suspended ceilings, ducts, or other areas, if they are used to circulate air or act as an air passage from one room to another. If in doubt, use plenum. CMR cable is generally acceptable for all applications not requiring plenum cable.

CAT 5 cable is available in reel-in-box packaging. This is very handy for pulling the wire without putting twists in it. Without this kind of package or a cable reel stand, pulling wire is a two-person job. Before the advent of the reel-in-box, we used to put a reel of wire on a broom handle to pull it. One person would hold the broom handle and the other would pull broom handle to pull it. You will produce a tangled mess, if your pull the wire off the end of the reel alone.

Standard wire patch cables are often specified for cable segments running form a wall jack to a PC and for patch panels. They are more flexible than solid core wire. However, the rationale for using it
is that the constant flexing of patch cables may wear-out solid core cable and break it. This is not a real concern in the average small network.

Most of the wiring we do simply connects computers directly to other computers or hubs. Solid core cable is quite suitable for this purpose and for many home and small business network. It is also quite acceptable for use as patch cables. You might consider a stranded wire patch cable if you have a notebook computer you are constantly moving around.

CAT 5 cable has four twisted pairs of wire for a total of eight individually insulated wires. Each pair is color coded with one wire having solid color (blue, orange, green, or brown) twisted around a second wire with a white background and a stripe of the same color. The solid color may have white stripe in some cables. Cable colors are commonly described using the background color followed by the color of the stripe; e.g; white-orange is a wire with a white background and an orange stripe.

Connectors

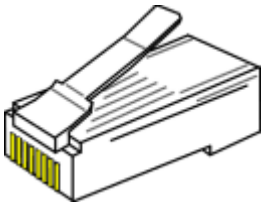


Figure 3.2: RJ-45 Connector

The straight through and cross-over patch cables are discussed in this article which are terminated with CAT 5 RJ-45 modular plugs. RJ-45 plugs are similar to those you'll see on the end of your telephone cable except they have eight as opposed to four or six contacts on the end of the plug and they are about twice as big. Make sure they are rated for CAT 5 wiring. (RJ stands for "Registered Jack"). Also, there are RJ-45 plugs designed for both solid core wire and stranded wire. Others are designed specifically for one kind of wire or the other. Be sure you buy plugs appropriate for the wire you are going to use. We normally use plugs designed to accommodate both kinds of wire.

Network cabling tools

1. Modular Plug Crimp Tool

Figure 3.3: Modular plug crimp tool

You will need a modular crimp tool. This is very similar to the ones which have been used for many years for all kinds of telephone cable work and it works just fine for Ethernet cables. You don't need a lot of bells and whistles, just a tool which will securely crimp RJ-45 connectors. Some crimpers have cutters which can be used to cut the cable and individual wires, and possibly stripping the outer jacket.

2. Universal UTP Stripping Tool (Eclipse)

It makes a much neater cut. It is highly recommending for anyone who will make a lot of cables.

Figure 3.4: Eclipse

3. Diagonal Cutters

It is easier to use diagonal cutters ("diags" or "dikes") to cut the cable off at the reel and to fine-tune the cable ends during assembly. Also, if you don't have a stripper, you can strip the cable by using a small knife to carefully slice the outer jacket longitudinally and use the diags to cut it off around the circumference.

Figure 3.5: Diagonal cutters

UTP basics

The 10BASE-T and 100BASE-TX Ethernet consist of two transmission lines. Each transmission line is a pair of twisted wires. One pair receives data signals and the other pair transmits data signals. A balanced line driver or transmitter is at one end of one of these lines

and a line receiver is at the other end. A (much) simplified schematic for one of these lines and its transmitter and receiver follows:

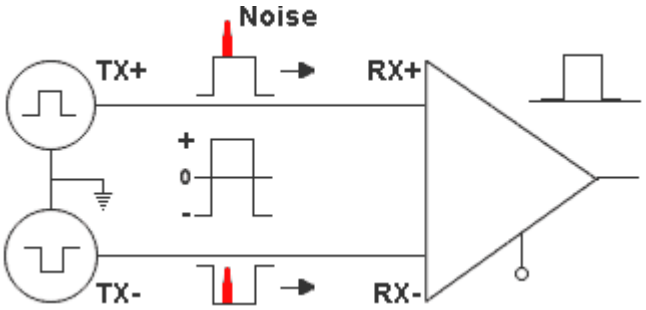


Figure 3.6: Schematic diagram of transmission line

Pulses of energy travel down the transmission line at about the speed of light (186,000 miles/second). The principal components of these pulses of energy are the potential difference between the wires and the current flowing near the surface of the wires. This energy can also be considered as residing in the magnetic field which surrounds the wires and the electric field between the wires. In other words, an electromagnetic wave which is guided by, and travels down the wires.

The main concern are the transient magnetic fields which surround the wires and the magnetic fields generated externally by the other transmission lines in the cable, other network cables, electric motors, fluorescent lights, telephone and electric lines, lightning, which may literally bury the Ethernet pulses, the conveyor of the information being sent down the line.

The twisted-pair Ethernet employs two principal means for combating noise. The first is the use of balanced transmitters and receivers. A signal pulse actually consists of two simultaneous pulses relative to ground: a negative pulse on one line and a positive pulse on the other. The receiver detects the total difference between these two pules. Since a pulse of noise usually produces pulses of the same polarity on both lines, it is essentially canceled out at the receiver. Also, the magnetic field surrounding one wire from a signal pulse is a mirror of the one on the other wire. At a very short distance from the two wires the magnetic fields are opposite and have a tendency to cancel the effect of each other out. This reduces the line's impact on the other pairs of wires and the rest of the world.

The second and the primary means of reducing cross-talk (the term cross-talk came from the ability to overhear conversations on other lines on your phone) between the pairs in the cable, is the double helix configuration produced by twisting the wires together. This configuration produces symmetrical (dentinal) noise signals in each wire. Ideally, their difference as detected at the receiver, is zero. In actuality it is much reduced.

Straight through and cross over cable

Again, the wire with colored backgrounds may have white stripes and may be denoted that way in diagrams found elsewhere. For example, the green wire may be labeled Green-White. The background color is always specified first.

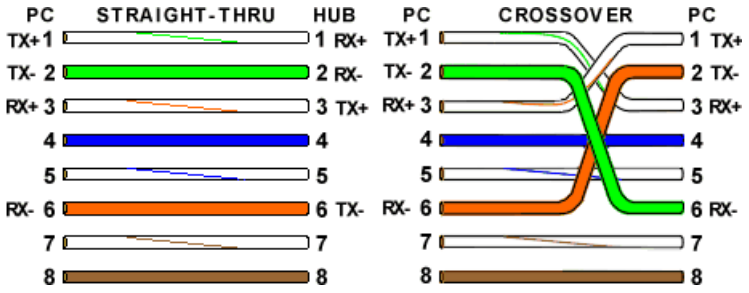


Figure 3.7: Straight through and crossover cable wire scheme

A Straight-through cable has identical ends, whereas a Crossover cable has different ends.

EIA/TIA 568A and 568B standards

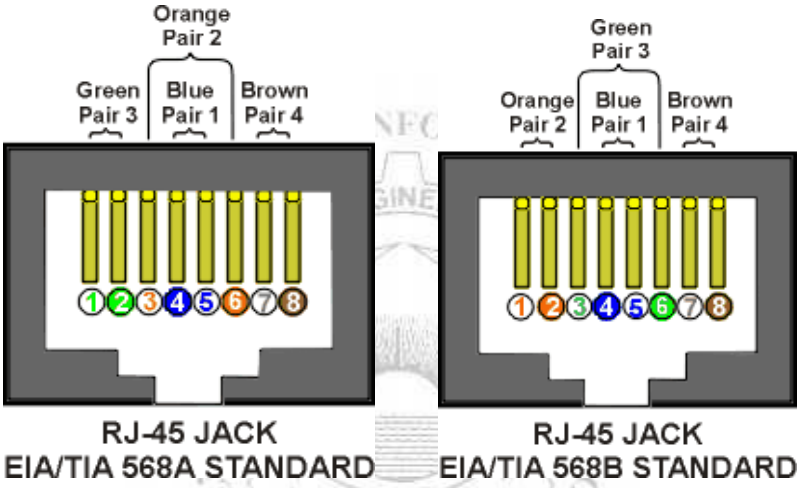


Figure 3.8: Cable connector standard ordering

It makes no functional difference which standard you use for a straight-through cable. Your can start a crossover cable with either standard as long as the other end is the other standard. It makes no functional difference which end is which. Despite what you may have read elsewhere, a 568A patch cable will work in a network with 568B wiring and 568B patch cable will work in a 568A network. The electrons couldn't care less.

Figure 3.9: EIA/TIA 568A and 568B

PROCEDURE

To Make Cable

1. Pull the cable off the reel to the desired length and cut the total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet or about the length of a football field) for 100BASE-TX and 300 Meters for 100BASE-T.

2. Strip one end of the cable with the stripper or a knife and diags. If you are using the stripper, place the cable in the groove on the blade (left) side of the stripper and align the end of the cable with the right side of the stripper. This will strip about ½" of the jacket off the cable. Turn the stripper about 1 ¼ turn and pull. If you turn it more, you will probably nick the wires. If you are using knife and diags, carefully slit the cable for about an inch or so and neatly trim around the circumference of the cable with diags to remove the jacket.

3. Inspect the wires for nicks. Cut off the end and start over if you see any. You may have to adjust the blade with the screw at the front stripper. Cable diameters and jacket thicknesses vary.

4. Spread and arrange the pairs roughly in the order of the desired cable end.

5. Untwist the pairs and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another.
   It is very important that the unstripped (untwisted) end be slightly less than ½" long. If it is longer than ½" it will be out-of-spec and susceptible to crosstalk. If it is less than ½" it will not be properly clinched when RJ-45 plug is crimped on. Flatten again. There should be little or no space between the wires.

6. Hold the RJ-45 plug with the clip facing down or away from you. Push the wire firmly into the plug. **Now, inspect before crimping and wasting the plug!** Looking through the bottom of the plug, the wire on the far-left side will have a white background. The wires should alternative light and dark from left to right. The furthest right wire is brown. The wires should all end evenly at the front of the plug. The jacket should end just about where you see it in the diagram-right on the line.

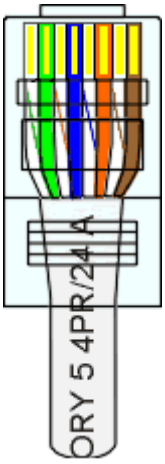


Figure 3.10:
Preparing the RJ-45 Connector

ALL ABOUT CRIMPING

7. Hold the wire near the RJ-45 plug with the clip down and firmly push it into the left side of the front of the Crimper (it will only go in one way). Hold the wire in place and squeeze the crimper handles quite firmly. This is what will happen:

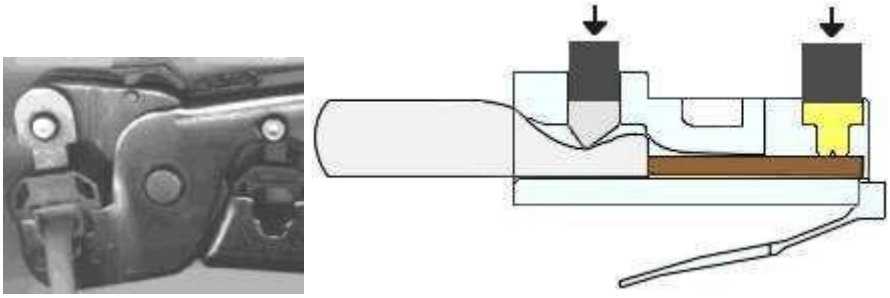


Figure 3.11: Crimping

(Crimp it once). The crimper pushes two plungers down on the RJ-45 plug. One forces, what amounts to, a cleverly designed plastic plug/wedge onto the cable jacket and very

firmly clinches it. The other seats the "pins", each with two teeth at its end, through the insulation and into the conductors of their respective wires.

8. Test the crimp… if done properly an average person will not be able to pull the plug off the cable with his or her bare hands. And that quite simply, besides lower cost, is the primary advantage of twisted-pair cables over the older thin wire, coaxial cables. In fact, the ease of installation and the modular RJ-45 plug is the main reason coaxial cable is no longer widely used for small Ethernet. But, don't pull that hard on the plug. It could stretch the cable and change its characteristics. Look at the side of the plug and see if it looks like the diagram and give it a fairly firm tug to make sure it is crimped well.

9. Prepare the other end of the cable so it has the desired end and crimp.

10. If both ends of the cable are within reach, hold them next to each other and with RJ-45 clips facing away. Look through the bottom of the plugs. If the plugs are wired correctly, and they are identical, it is a straight-through cable. If they are wired correctly and they are different, it is a crossover cable.

PRECAUTIONS

1. Try to avoid running cables parallel to power cables.

2. If you bundle a group of cables together with cable ties (zip ties), do not over-clinch them. It's okay to snug them together firmly; but don't tighten them so much that you deform the cables.

3. Keep cables away from devices which can introduce noise into them. Here's a short list: electric heaters, loud speakers, printers, TV sets, fluorescent light, copiers, welding machines, microwave ovens, telephones, fans, elevator motors, electric ovens, dryers, washing machines, and shop equipment.

4. Avoid stretching UTP cables (the force should not exceed 24 LBS).

5. Do not use a stapler to secure UTP cables. Use telephone wire hangers, which are available at most hardware stores.

EXERCISES

1. Give the reason why it is not advisable to bend UTP cables more than four times the diameter of the cable.

_____

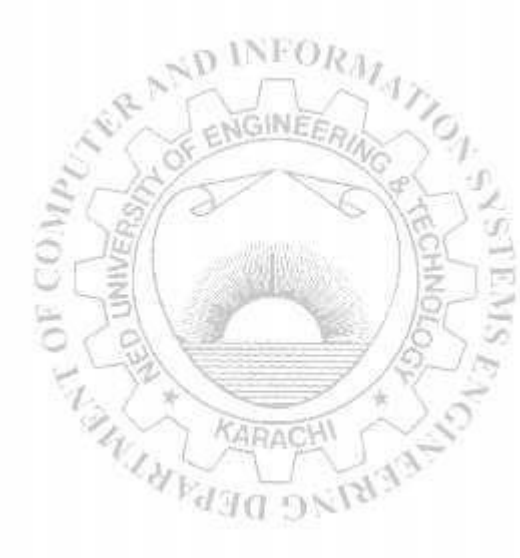
_____

_____

_____

_____

2. Why is it not advisable to run UTP cable outside of a building?



Lab Session 04

OBJECT

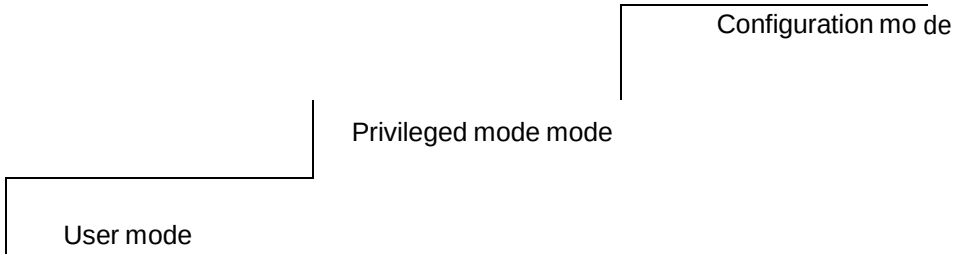
Practicing some basic commands to interact with the Cisco IOS (Internetwork Operating System) CLI Software

THEORY

Welcome to "hands on routing." The goal of this lab is to introduce you to Cisco routers and other equipment that you will be using throughout the semester. In order to do well in the labs, we need to understand the basic set-up of the lab.

- The lab has one rack, which is connected to a PC. You will be using the PC as a terminal to talk to the routers.
- The routers are labeled alphanumerically (Example R1, R2…)
- Each rack has two patch panels. One of them has RJ-45 connectors and the other has serial connectors. Ethernet ports are pre-connected to the RJ-45 patch panel. Serial ports are pre-connected to the serial patch panel. The ports are labeled on their left.
- To connect the PC to a specific router, connect the PC's console cable to the appropriate console port on the patch panel in the rack. You will find the console cable as a UTP cable with one of its ends connected through a small devices to a serial port on the PC.

Cisco routers support different modes of operation. When you access a router, it will typically be in the "user" mode. User mode gives a user access to simple "show commands." From user mode the next step is "Privileged mode." In the "Privileged mode" a user can have full access to all the databases maintained by the router. Cisco routers use many other modes, but let us keep it simple for now.



PROCEDURE

It is time to have fun:

1. Connect the PC to R1.

2. Press "`enter`" a few times and you should get a prompt that looks like: `router>`

3. You are now in the "user mode".

4. Type "`?`". Question mark lists commands that can be used in a certain context.

   First type "`help`"
   Try typing these commands:
   `p?`
   `pi?`

5. The IOS will complete commands for you with the help of the TAB key.

   Type `sh<TAB>`
   Finish the command with a "`?`" to see what commands you can use with show. (`show ?`)

6. You don't have to type a complete command for the IOS to execute it. You only need to type enough of a command to differentiate it from all other commands.

7. We have been operating in User Mode (identified by the prompt ending in >), now we want to go into the Privileged Mode:

   Type "`enable`" or "`en`"
   The prompt should end with a # (`Router#`)

   Type "`?`" to see all the commands possible from this mode

8. One of the most useful commands in the Cisco IOS is "`show.`" Try these variations:

   "`show configuration`" – shows saved router configuration
   "`show version`" - shows IOS statistics
   "`show startup-config`" – shows the configuration during startup
   "`show running-config`" – shows the dynamic configuration
   "`show flash`" – gives details of flash memory where IOS is stored
   "`show protocols`" – shows protocol and interface statistics
   "`show interface`" – gives detailed statistics on each interface
   "`show interface s0`" - Try this command with some other interfaces as well.

9. Now let's move to configuration mode. Type the following commands:

`configure terminal`
This will take you to configuration mode. The prompt ends with (`router-config`)`#?`
; to see the available commands

10. Next we will change the name of router to R1

11. Go into configuration mode and type the following commands:

```
hostname R1          ;this command will change name.
ctrl+Z               ;this is to come out of privilege mode
```

Now we want to set up an interface for a TCP/IP network.

Type these commands:

```
config t

interface Ethernet 0
```

This puts you in interface mode. Now you can configure interface Ethernet0.

```
ip address 130.10.20.5 255.255.255.0
```

This gives the interface an IP address and subnet mask.

```
no shutdown
```

By default all interface are administratively down. This command will bring them up.

```
ctrl+Z
```

This is to come out of privilege mode. Now type the following command:

```
sh interface e0
```

Observe and record carefully what you see.

Now connect a cable from router R1`s Ethernet 'e0' interface to a hub or switch. Again type this command:

```
sh interface e0
```

Again observe and record carefully what you see.

Note: Cisco commands are not case-sensitive.

EXERCISES

1. Determine which mode you operate in when you first access the router.

_____

_____

2. Start-up configuration is stored in NVRAM (true or false).
3. Running-configuration is stored in_____.
4. The command used to save changes made in the running configuration to start-up configuration is:

   _____

5. List the interfaces on three routers of your choice. Be sure to indicate the router number.

   _____

   _____

   _____

   _____

   _____

6. Elaborate on the information presented by the command "`show version`."

7. Which of the condition(s) are possible for an interface:

    a. administratively down, line protocol down
    b. administratively down, line protocol up
    c. administratively up, line protocol up
    d. administratively up, line protocol down

Lab Session 05

OBJECT

Configuring static routes on Cisco routers

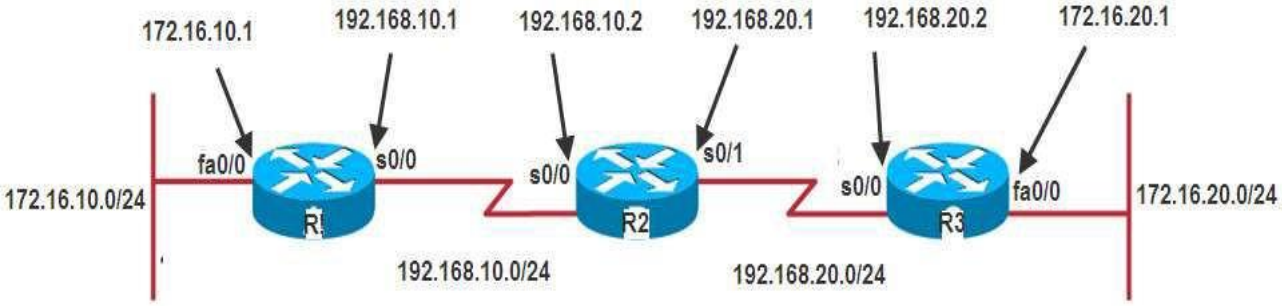


Figure 5.1: Scenario for static routes

THEORY

Routed & Routing Protocols

- A **Routed Protocol** is a protocol by which data can be routed. Routed protocols are IP, AppleTalk, and IPX. In this kind of protocols we require an addressing scheme and sub netting. Addressing scheme will be used to determine the network to which a host belongs and to identifying that host on that particular network. All hosts on an internetwork use the services of a routed protocol.
- A **Routing Protocol** is different and is only used between routers. It makes possible for routers to build and maintain routing tables. There are three classes of routing protocols-
  1) Distance Vector,
  2) Link State,
  3) Hybrid

Static & Dynamic Routing

The simplest method to route packets on a network is static routes. Although dynamic routing protocols are flexible and adjust to network changes, they do have associated network traffic which competes for network bandwidth with the user data traffic.

Configuring Static Routes

Static routes specify a fixed route for a certain destination network. They need to be configured on any router that needs to reach a network that it is not directly connected to. The IOS command used to configure static routes is `ip route`. The syntax is:

`ip route` *destination-address subnet-mask* **{***ip-address* | *outgoing-interface***}** [*distance*] [**tag** *tag*] [*permanent*]

where:

- *destination-address* is the destination address prefix for the network that we would like the router to reach
- *subnet-mask* is the subnet mask to be used on the address prefix to match for destination addresses. Multiple networks may be combined such that the destination-address and subnet-mask combination matches all hosts on those networks.
- *ip-address* specifies what ip address to forward a packet to if an IP packet arrives with a destination address that matches the destination-address subnet-mask pair specified in this command.
- Alternatively *outgoing-interface* specifies which interface the packet should be sent out of. Adding a static route to an Ethernet or other broadcast interface (for example, `ip route 0.0.0.0 0.0.0.0 Ethernet 1/2`) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send ARP requests to any destination addresses that route through the static route.
- *distance* is the optional administrative distance value for the route. If unspecified the default value is 1.
- *tag* value can be used as a "match" value for controlling redistribution via route maps.
- *permanenet* specifies that the route will not be removed even if the interface shuts down.

DTE/DCE

DCE and DTE are the interfaces. The DCE-DTE connection between routers is referred to as a null serial cable DCE(data communication equipment) and DTE (Data terminal equipment). DCE is located at the service provider end while the DTE is attached device.

The services that are given to the DTE is often accessed via modems or channel service unit/data service unit(CSU/DSU). DCE provides clocking and DTE receives the clock

PROCEDURE

1. Connect the network as shown in the network diagram.

2. Configure appropriate ip addresses and clock rates(if needed) on the router interfaces as specified in the network diagram.

3. For R1, enter the following static routes
   ip route 172.16.20.0 255.255.255.0 192.168.10.2
   ip route 192.168.20.0 255.255.255.0 192.168.10.2

4. On R2 enter:
   ip route 172.16.10.0 255.255.255.0 192.168.10.1
   ip route 172.16.20.0 255.255.255.0 192.168.20.2

5. On R3 enter:

ip route 172.16.10.0 255.255.255.0 192.168.20.1
ip route 192.168.10.0 255.255.255.0 192.168.20.1

6. After that verify the static routes by entering the following commands in the privilege mode:

router# sh ip route

EXERCISES

1. Run the command show IP route and write its output.

1. What is the default administrative distance of static route? Write the IP route command to modify the same.

3. Create a loop back interface on R3 and assign an IP address 10.1.0.1 /16 to it. Now add static routes to each of the other routers to reach this interface. Verify your work by pinging the newly created interface from routers R1 and R2 respectively.

Lab Session 06

OBJECT

Configuring RIP (Routing Information Protocol) and RIP version 2

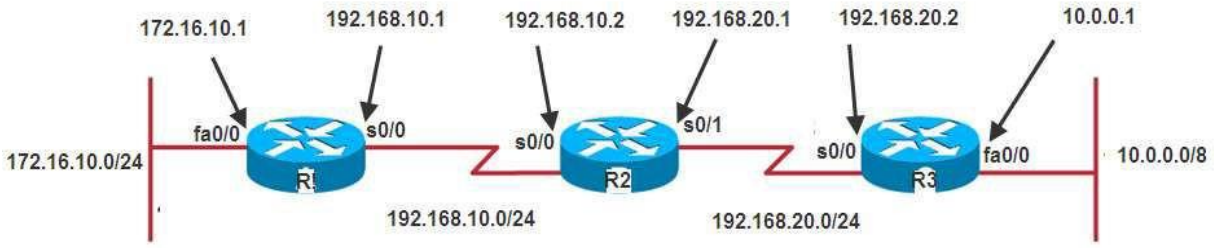


Figure 6.1: Scenario for RIP

THEORY

Distance Vector Routing Protocols

- Broadcast their entire routing table to each neighbor router at predetermined intervals
- The actual interval depends on the distance-vector routing protocol in use
- Varies between 30 and 90 seconds
- Sometimes referred to as *routing by rumor*
- Suffer from slow time to *convergence*
- *Convergence* is an state where all routers on the internetwork share a common view of the internetwork routes

Routing Information Protocol (RIP)

A distance-vector protocol, RIP was designed to work with small to medium-sized networks. RIP is an Interior Gateway Protocol (IGP), meaning it is used within an autonomous system. An autonomous system is a collection of networks under a single administration, sharing a common routing strategy.

RIP is easy to implement, compared to newer IGPs, and has been implemented in networks around the world. Advantage of using RIP, especially in small networks, is that there is very little overhead, in terms of bandwidth used and configuration and management time.

RIP Timers

RIP uses timers both to regulate its performance and to help prevent routing loops. All routers that use RIP send an update message to all of their neighbors approximately every 30 seconds; this process is termed *advertising*. The Cisco implementation sends updates every 30 seconds minus up to 15 percent, or 4.5 seconds.

If a neighbor has not responded in 180 seconds, it is assumed that the neighboring router is unavailable or the network connecting it to the router has become unusable. When the neighbor has not responded for 180 seconds, the route is marked invalid; 180 seconds is long enough that a route won't be invalidated by a single missed update message. The neighbor is shown to be unreachable by sending a normal update message with a metric of "infinity;" in the case of RIP, this number is 16. If an advertisement is received from a neighbor with a metric of infinity, then the route is placed into hold-down state, advertised with a distance of 16, and kept in the routing table. No updates from other neighbors for the same route are accepted while the route is in hold-down state. If other neighbors are still advertising the same route when the hold-down timer expires, then their updates will then be accepted. The route will be advertised with infinity metric for a period of time after the hold-down state if no alternate paths are found.

The actual timers used to accomplish the above tasks are a *routing-update timer*, a *route-invalid timer*, a *route-hold-down timer*, and a *route-flush* timer. The RIP routing-update timer is generally set to 30 seconds, ensuring that each router will send a complete copy of its routing table to all neighbors every 30 seconds. The route-invalid timer determines how much time must expire without a router having heard about a particular route before that route is considered invalid. When a route is marked invalid or put in hold-down state, neighbors are notified of this fact. This notification must occur prior to expiration of the route-flush timer. When the route flush-timer expires, the route is removed from the routing table. Typical initial values for these timers are 180 seconds for the route-invalid and route-holddown timers and 240 seconds for the route-flush timer. The values for each of these timers can be adjusted with the `timers basic` router configuration command.

Several Stability Features

To adjust for rapid network-topology changes, RIP specifies numerous stability features that are common to many routing protocols. RIP implements split horizon with poison-reverse and hold-down mechanisms to prevent incorrect routing information from being propagated. Split horizon prevents incorrect messages from being propagated by not advertising routes over an interface that the router is using to reach the route. Implementing split horizon helps avoid routing loops. Poison reverse operates by advertising routes that are unreachable with a metric of infinity back to the original source of the route. Hold-down is a method of marking routes invalid (expired). As discussed above, no updates from other neighbors for the same route are accepted while the route is in hold-down state.

Triggered updates are also an included convergence and stability feature. Updates are triggered whenever a metric for a route changes. Triggered updates may also contain only information regarding routes that have changed, unlike scheduled updates.

RIP version 2

RIPv2 is almost the same as the RIP version 1. RIPv2 also sends its complete routing table to its active interfaces at periodic time intervals. The timers, loop avoidance schemes and administrative distance are the same as Rip version 1.But RIPv2 is considered classless routing protocol because it also sends subnet information’s with each router. It also allows authentication using MD5 encryption scheme. And it also supports dis-contiguous networks. Configuring RIP version 2 on a router is very simple; it just requires one additional command.

PROCEDURE

Configuring RIP

1. Cable up the network as shown in the diagram.

2. Assign the IP address as shown in the diagram to the appropriate interfaces. For the serial links, has been used to indicate a DCE port.

3. Issue RIP routing commands on all the routers starting from the global config mode.

4. On R1:

```
router rip
network 172.16.10.0
network 192.168.10.0
```

   On R2

```
router rip
network 192.168.10.0
network 192.168.20.0
```

   On R 3

```
router rip
network 10.0.0.0
network 192.168.20.0
```

5. To verify the working of RIP ping one host, say H2, on LAN connected to R3 from the host, say H1, on LAN connected to R1. Also run some other debugging command to explore more.

Configuring RIP version 2

1. Issue the following commands on R1.

```
router rip
version 2
network 172.16.10.0
network 192.168.10.0
```

2. Repeat the same for R2 and R3.
3. Verify and debug, as you did earlier for RIP.

EXERCISES

1. Configure RIP on all three routers, note down routing table of router R1, and run command Debug ip rip to note the address on which updates are sent.

2. Write commands to modify the default update and hold-down timers.

3. Repeat exercise #1 for RIPv2 and note down the multicast address on which RIPv2 forwards the updates.

4. Write down the source IP address for the ping packets when you ping H1 from R1.

5. While working on R1, how could you check if H1 can reach the loopback interface? In other words, how can you verify if a ping from H1 to loopback of R1 is successful?

Lab Session 07

OBJECT

Configuring OSPF (Open Shortest Path First) Single Area

THEORY

Open Shortest Path First (OSPF) was developed by the Internet Engineering Task Force (IETF) as a replacement for the problematic RIP and is now the IETF-recommended Interior Gateway Protocol (IGP). OSPF is a link state protocol that, as the name implies, uses Dijkstra's Shortest Path First (SPF) algorithm. It is an open standards protocol—that is, it isn't proprietary to any vendor or organization. Link-state routing protocols perform the following functions:

- Respond quickly to network changes
- Send triggered updates only when a network change has occurred
- Send periodic updates known as *link-state refreshes*
- Use a *hello mechanism* to determine the reachability of neighbors
  - Each router keeps track of the state or condition of its directly connected neighbors by multicasting hello packets
- Each router also keeps track of all the routers in its network or area of the network by using *link-state advertisements (LSAs).*

Like all link state protocols, OSPF's major advantages over distance vector protocols are fast convergence, support for much larger internetworks, and less susceptibility to bad routing information. Other features of OSPF are:

- The use of areas, which reduces the protocol's impact on CPU and memory, contains the flow of routing protocol traffic, and makes possible the construction of hierarchical internetwork topologies
- Fully classless behavior, eliminating such class-full problems as dis-contiguous subnets. Support of classless route table lookups, VLSM, and super-netting for efficient address management
- A dimensionless, arbitrary metric
- Equal-cost load balancing for more efficient use of multiple paths
- Support of authentication for more secure routing
- The use of route tagging for the tracking of external routes

Characteristics of OSPF

Characteristic	OSPF
VLSM support	Yes
Manual summarization	Yes

Type of protocol	Link state
Classless support	Yes
Auto-summarization	No
Dis-contiguous support	Yes
Route propagation	Multicast on change
Hop count limit	None
Convergence	Fast
Peer authentication	Yes
Hierarchical network Updates/ Route computation	Event triggered/ Dijkstra

DR and BDR

DR (Designated Routers)

DR has the following duties:

- To represent the multi-access network and its attached routers to the rest of the internetwork
- To manage the flooding process on the multi-access network.
- The concept behind the DR is that the network itself is considered a "pseudo node," or a virtual router. Each router on the network forms an adjacency with the DR which represents the pseudo-node. Only the DR will send LSAs to the rest of the internetwork.

Note: router might be a DR on one of its attached multi-access networks, and it might not be the DR on another of its attached multi-access networks. In other words, the DR is a property of a router's interface, not the entire router.

BDR(Backup Designated Router):

A *Backup Designated Router (BDR)* is a hot standby for the DR on multi-access links. The BDR receives all routing updates from OSPF adjacent routers but doesn't flood LSA updates.

Note: if the router interface priority value is set to zero then that router won't participate in the DR or BDR elections on that interface.

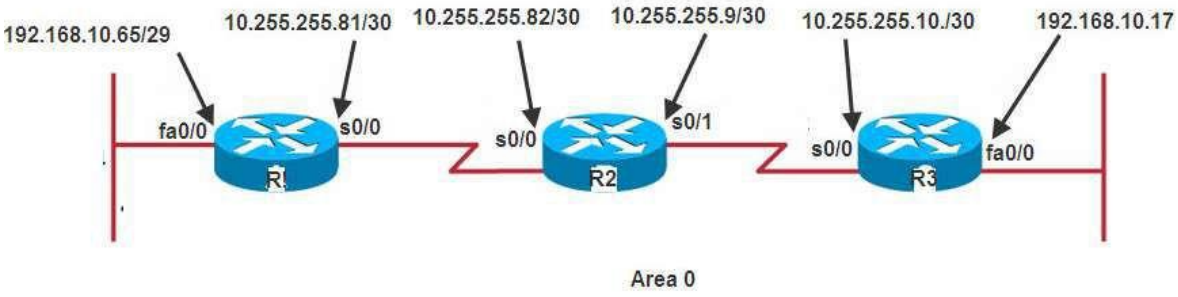


Fig 8.1: Scenario for OSPF implementation

After assigning ip addresses to interfaces of the routers the following IP Routing commands of OSPF on each other will be given as below.

```
Router A:

Router_A#config t
Router_A(config)#router ospf 1
Router_A(config-router)#network 192.168.10.64 0.0.0.7 area 0
Router_A(config-router)#network 10.255.255.80 0.0.0.3 area 0
```

The Router_A is using a /29 or 255.255.255.248 mask on the fa0/0 interface. This is a block size of 8, which is a wildcard of 7. The s0/0 interface is a mask of 255.255.255.252 block size of 4, with a wildcard of 3. Similarly the other subnet ,mask, and wildcard can be determined by looking at the IP address of an interface.

```
Router B:

Router_B#config t
Router_B(config)#router ospf 1
Router_B(config-router)#network 10.255.255.80 0.0.0.3 area 0
Router_B(config-router)#network 10.255.255.8 0.0.0.3 area 0

Router C:
Router_C#config t
Router_C(config)#router ospf 1
Router_C(config-router)#network 192.168.10.16 0.0.0.7 area 0
Router_C(config-router)#network 10.255.255.8 0.0.0.3 area 0
```

EXERCISES

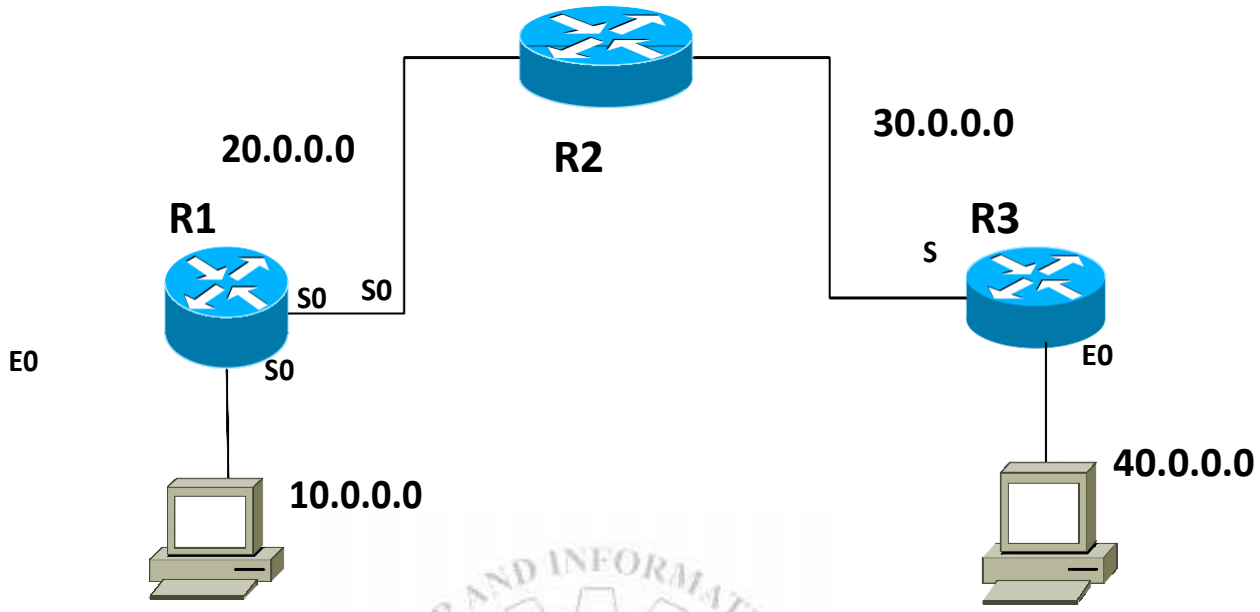


Fig 8.2: Scenario for exercise problems

Configure the network shown above on the routers in the lab. Assign appropriate IP addresses on the interfaces and configure OSPF on the routers. Write down the configuration commands entered on all three routers for configuration of OSPF.

1. Router 1:

2. Router 2:

3. Router 3:

Configure the network shown above on the routers in the lab. Assign appropriate IP addresses on the interfaces and configure EIGRP on the routers. Write down the configuration commands entered on all three routers for configuration of EIGRP.

1. Router 1:

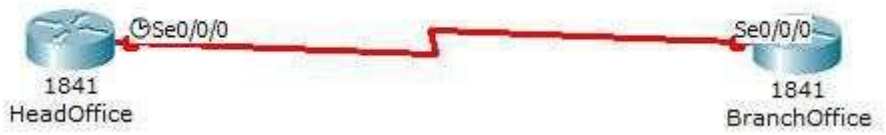
2. Router 2:

3. Router 3:

Lab Session 08

OBJECT

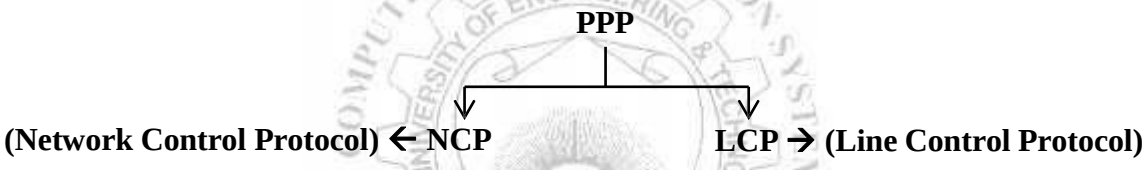
Connecting two routers (Branch office and Head office) with the help of PPP



THEORY

PPP (Point-To-Point Protocol)

Short for **P***oint-to-***P***oint* **P***rotocol*, PPP is a method of connecting a computer to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features. Working in the data link layer of the OSI model, PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet.



NCP

A Network Control Protocol is a protocol that runs atop the Point-to-Point Protocol (PPP) and that is used to negotiate options for a network layer protocol running atop PPP. Network Control Protocols include the Internet Protocol Control Protocol for the Internet Protocol, the Internetwork Packet Exchange Control Protocol for the Internet Packet Exchange protocol, and the AppleTalk Control Protocol for AppleTalk. This protocol operates on the data link layer.

LCP

Short for Link Control Protocol, a protocol that is part of the PPP. In PPP communications, both the sending and receiving devices send out LCP packets to determine specific information that will be required for the data transmission. The LCP checks the identity of the linked device and either accepts or rejects the peer device, determines the acceptable packet size for transmission, searches for errors in configuration and can terminate the link if the parameters are not satisfied. Data cannot be transmitted over the network until the LCP packet determines that the link is acceptable.

Authentications methods of PPP

PAP and CHAP are two methods that PPP uses for authentication.

PAP (Password Authentication Protocol)

Short for Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP. The main weakness of PAP is that both the username and password are transmitted "in the clear" -- that is, in an unencrypted form. It's a two way hand shake method.

CHAP (Challenge Handshake Authentication Protocol)

Short for Challenge Handshake Authentication Protocol, CHAP is a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated .By transmitting only the hash, the secret can't be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks. It's a three way hand shake method.

PROCEDURE

1. Change Hostname and assign Username and password on both routers. Assign the username of Branch Office Router in Head Office Router and Head Office Router username initialized on Branch Office Router but Password must be same on both Routers.

   HeadOffice Router:

```
Router(config)#hostname FasiRehman
FasiRehman(config)#usernam
FasiRehman(config)#username FasiRehmanCisco pas
FasiRehman(config)#username FasiRehmanCisco password 123
FasiRehman(config)#
```

   BranchOffice Router:

```
Router(config)#hostname FasiRehmanCisco
FasiRehmanCisco(config)#use
FasiRehmanCisco(config)#username FasiRehman pas
FasiRehmanCisco(config)#username FasiRehman password 123
```

2. Issue PPP debugging commands in privileged mode of both routers.

   - **debug ppp authentication:** The most common reasons for failed dial backup calls are incorrect dial strings and PPP authentication problems. You can easily diagnose both of these problems with this command.

- **debug ppp negotiation:** Displays PPP packets related to the negotiation of the PPP link.

```
FasiRehman#deb
FasiRehman#debug p
FasiRehman#debug ppp a
FasiRehman#debug ppp authentication
PPP authentication debugging is on
FasiRehman#de
FasiRehman#deb
FasiRehman#debug p[
FasiRehman#debug pp
FasiRehman#debug ppp n
FasiRehman#debug ppp negotiation
PPP protocol negotiation debugging is on
```

3. Assingning IP addresses on serial interfaces and enabling PPP on both routers

- **encapsulation ppp:** Change encapsulation from default HDLC to PPP

- **ppp authentication chap pap:** Define that the Link will use PAP authentication, but will try CHAP if PAP fails or is rejected by other side.

HeadOffice Router:

```
FasiRehman(config)#interface se
FasiRehman(config)#interface serial 0/0/0
FasiRehman(config-if)#ip ad
FasiRehman(config-if)#ip address 10.0.0.1 255.0.0.0
FasiRehman(config-if)#no shu
FasiRehman(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
FasiRehman(config-if)#c;lo
FasiRehman(config-if)#clo
FasiRehman(config-if)#clock ra
FasiRehman(config-if)#clock rate 64000
FasiRehman(config-if)#en
FasiRehman(config-if)#encapsulation pp
FasiRehman(config-if)#encapsulation ppp
FasiRehman(config-if)#
Serial0/0/0 PPP: Using default call direction
Serial0/0/0 PPP: Treating connection as a dedicated line
Serial0/0/0 PPP: Phase is ESTABLISHING, Active Open

FasiRehman(config-if)#ppp
FasiRehman(config-if)#ppp a
FasiRehman(config-if)#ppp authentication c
FasiRehman(config-if)#ppp authentication chap p
FasiRehman(config-if)#ppp authentication chap pap
```

BranchOffice Router:

```
FasiRehmanCisco(config)#interface serial 0/0/0
FasiRehmanCisco(config-if)#ip ad
FasiRehmanCisco(config-if)#ip address 10.0.0.2 255.0.0.0
FasiRehmanCisco(config-if)#no shu
FasiRehmanCisco(config-if)#no shutdown

FasiRehmanCisco(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

FasiRehmanCisco(config-if)#en
FasiRehmanCisco(config-if)#encapsulation p
FasiRehmanCisco(config-if)#encapsulation ppp
FasiRehmanCisco(config-if)#
Serial0/0/0 PPP: Using default call direction
Serial0/0/0 PPP: Treating connection as a dedicated line
Serial0/0/0 PPP: Phase is ESTABLISHING, Active Open

Serial0/0/0 LCP: State is Open

Serial0/0/0 PPP: Phase is AUTHENTICATING

Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0/0 IPCP: I CONFACK [Closed] id 1 len 10

Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0/0 IPCP: I CONFACK [REQsent] id 1 len 10

Serial0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0/0 Phase is ESTABLISHING, Finish LCP
```

```
FasiRehmanCisco(config-if)#ppp authentication chap p
FasiRehmanCisco(config-if)#ppp authentication chap pap
FasiRehmanCisco(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn

Serial0/0/0 LCP: State is Open

Serial0/0/0 PPP: Phase is AUTHENTICATING

Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0/0 IPCP: I CONFREQ [Closed] id 1 len 10

Serial0/0/0 IPCP: O CONFACK [Closed] id 1 len 10

Serial0/0/0 IPCP: I CONFACK [Closed] id 1 len 10

Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial0/0/0 IPCP: I CONFREQ [REQsent] id 1 len 10

Serial0/0/0 IPCP: O CONFACK [REQsent] id 1 len 10

Serial0/0/0 IPCP: I CONFACK [REQsent] id 1 len 10

Serial0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0/0 Phase is UP
```

EXERCISES

1. Run the command show ppp authentication and write its output.

2. Write down the difference between chap and pap

3. Write down the command to use chap and pap as a fall back method to one another

Lab Session 09

OBJECT

Studying and configuring Access Lists

THEORY

An access list is essentially a list of conditions that categorize packets. One of the most common and easiest to understand uses of access lists is filtering unwanted packets when implementing security policies. Access lists can even be used in situations that don't necessarily involve blocking packets.

There are a few important rules that a packet follows when it's being compared with an access list:

Rule#1
It's always compared with each line of the access list in sequential order—that is, it'll always start with the first line of the access list, then go to line 2, then line 3, and so on.

Rule#2
It's compared with lines of the access list only until a match is made. Once the packet matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.

Rule#3
There is an implicit "deny" at the end of each access list—this means that if a packet doesn't match the condition on any of the lines in the access list, the packet will be discarded. Each of these rules has some powerful implications when filtering IP packets with access lists, so keep in mind that creating effective access lists truly takes some practice.

There are two main types of access lists:

1. Standard access lists
2. Extended access lists

Standard access lists

These use only the source IP address in an IP packet as the condition test. All decisions are made based on the source IP address. This means that standard access lists basically permit or deny an entire suite of protocols. They don't distinguish between any of the many types of IP traffic such as web, Telnet, UDP, and so on.

Its command syntax is

```
access-list <number> {permit| deny} <destination> [log]
```

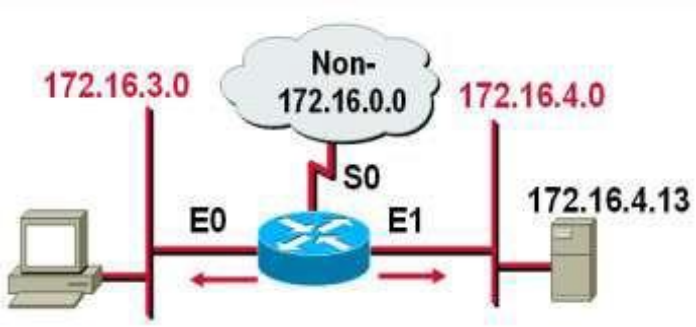


Fig 12.1: Standard Access list to allow my network

Commands on router will be

```
R1(config)#aaccess-list 1 permit 172.16.0.0 0.0.255.255
R1(config)#interface ethernet 0
R1(config)#ip access-group 1 out
R1(config)#interface ethernet 1
R1(config)#ip access-group 1 out
```

The above commands will permit the network 172.16.0.0 only and will block other network through the router on its ethernet interfaces in its out side directions

Extended access lists

Extended access lists can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when controlling traffic.

Its command syntax is

```
access-list <number> {permit| deny}
<protocol><source>[<ports>]<destination>[ports][<options>]
```

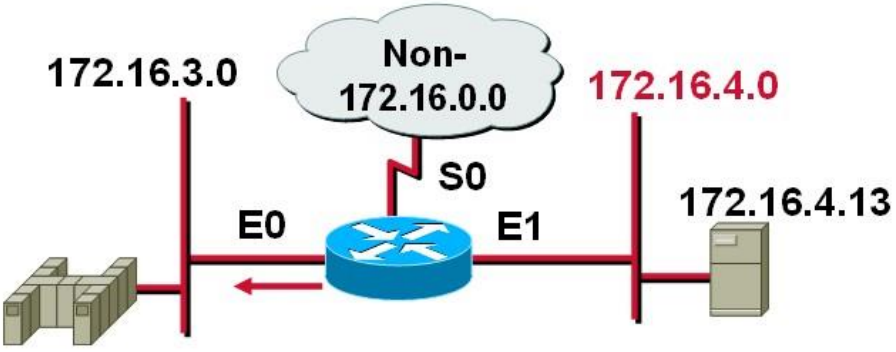


Fig 12.2: Extended access list

Commands on the router will be:

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
access-list 101 permit ip any any
interface ehternet 0
ip access-group 101 out
```

The above commands will Deny only the Telent from subnet 172.16.40.0 out of E0 and will permit all other traffic.

EXERCISE

Give commands to enable logging for the given access list and to show the entries that have been blocked

Lab Session 10

OBJECT

Studying basic LAN switch operation.

THEORY

LAN switch performs 3 operations

- Address learning
- Forward filter decision
- Loop avoidance

In this session, we will explore how an Ethernet switch learns addresses of the attached hosts.

Address learning

A new switch has empty MAC address table. As each frame transits switch, it learns source MAC address against the source port. As the switch does not know to which port the destination is attached, it initially transmits the frame to all ports. This process is called flooding. As the responses are received, the MAC address table is further populated.

PROCEDURE

Consider the following scenario

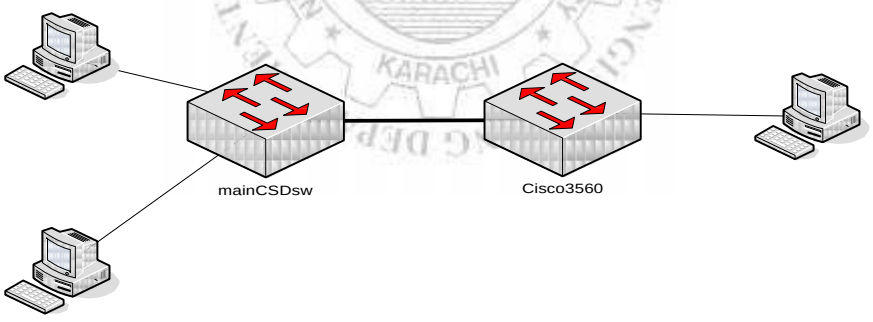


Fig 13.1: Scenario for LAN switch operation

Initially the MAC database of Cisco3560 will be

```
Switch#sh mac-address-table

          Mac Address Table
        -------------------------------------------

        Vlan    Mac Address       Type        Ports
        ----    -----------       --------    -----

           1    0006.2a75.100c    DYNAMIC     Fa0/1
Switch#
```

And that of mainCISDsw is;

```
mainCISDsw#sh mac-address-table

        Mac Address Table
      ------------------------------------------

      Vlan    Mac Address       Type        Ports
      ----    -----------       --------    -----

         1    0060.471b.ae01    DYNAMIC     Eth0/1

mainCISDsw#
```

Now as any of the computers generates ping for any of the remaining computers, the MAC address table will grow

```
Switch#sh mac-address-table

      Mac Address Table
      ------------------------------------------

      Vlan    Mac Address       Type        Ports
      ----    -----------       --------    -----

         1    0006.2a75.100c    DYNAMIC     Fa0/1
         1    0040.0ba5.183a    DYNAMIC     Fa0/1
         1    00e0.f7a4.475c    DYNAMIC     Fa0/2
Switch#
```

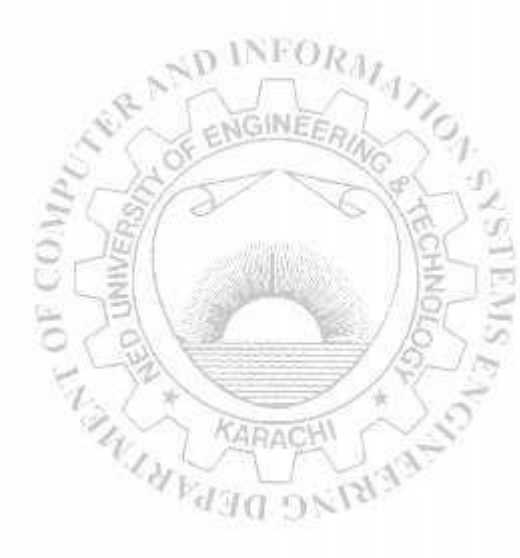
Also for mainCSDsw

```
mainCISDsw#sh mac-address-table

       Mac Address Table
      ------------------------------------------

      Vlan    Mac Address       Type        Ports
      ----    -----------       --------    -----

         1    0040.0ba5.183a    DYNAMIC     Eth1/1
         1    0060.471b.ae01    DYNAMIC     Eth0/1
         1    00e0.f7a4.475c    DYNAMIC     Eth0/1
mainCISDsw#
```

EXERCISES

1. If a destination MAC address is not in the forward/filter table, what will the switch do with the frame?

2. If a frame is received on a switch port and the source MAC address is not in the forward/filter table, what will the switch do?



Lab Session 11

OBJECT

Learning Loop Avoidance with Spanning Tree.

THEORY

The **Spanning Tree Protocol** (**STP**) is a link layer network protocol that ensures a loop-free topology for any switched LAN. Thus, the basic function of STP is to prevent switching loops and ensuing broadcast radiation.

In the OSI model for computer networking, STP falls under the OSI layer-2. It is standardized as 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 switches (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of switch loops, or the need for manual enabling/disabling of these backup links. Switch loops must be avoided because they result in flooding the local network.

STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation.

Protocol Operation

The collection of switches in a LAN can be considered a graph whose nodes are the bridges and the LAN segments (or cables), and whose edges are the interfaces connecting the bridges to the segments. To break loops in the LAN while maintaining access to all LAN segments, the bridges collectively compute a spanning tree. The spanning tree is not necessarily a minimum cost spanning tree. A network administrator can reduce the cost of a spanning tree, if necessary, by altering some of the configuration parameters in such a way as to affect the choice of the root of the spanning tree.

The spanning tree that the bridges compute using the Spanning Tree Protocol can be determined using the following rules.

Select a root bridge. The *root bridge* of the spanning tree is the bridge with the smallest (lowest) bridge ID. Each bridge has a unique identifier (ID) and a configurable priority number; the bridge ID contains both numbers. To compare two bridge IDs, the priority is compared first. If two bridges have equal priority, then the MAC addresses are compared. For example, if switches A (MAC=0200.0000.1111) and B (MAC=0200.0000.2222) both have a priority of 10, then switch A will be selected as the root bridge. If the network administrators would like switch B to become the root bridge, they must set its priority to be less than 10.

Determine the least cost paths to the root bridge. The computed spanning tree has the property that messages from any connected device to the root bridge traverse a least cost path, i.e., a path from the device to the root that has minimum cost among all paths from the device to the root. The cost of traversing a path is the sum of the costs of the segments on the path. Different technologies have different default costs for network segments. An administrator can configure the cost of traversing a particular network segment.

The property that messages always traverse least-cost paths to the root is guaranteed by the following two rules.

Least cost path from each bridge. After the root bridge has been chosen, each bridge determines the cost of each possible path from itself to the root. From these, it picks one with the smallest cost (a least-cost path). The port connecting to that path becomes the *root port* (RP) of the bridge.

Least cost path from each network segment. The bridges on a network segment collectively determine which bridge has the least-cost path from the network segment to the root. The port connecting this bridge to the network segment is then the *designated port* (DP) for the segment.

Disable all other root paths. Any active port that is not a root port or a designated port is a *blocked port* (BP).

Bridge Protocol Data Units (BPDUs)

The above rules describe one way of determining what spanning tree will be computed by the algorithm, but the rules as written require knowledge of the entire network. The bridges have to determine the root bridge and compute the port roles (root, designated, or blocked) with only the information that they have. To ensure that each bridge has enough information, the bridges use special data frames called **Bridge Protocol Data Units** (BPDUs) to exchange information about bridge IDs and root path costs.

A bridge sends a BPDU frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00.

There are three types of BPDUs:

- Configuration BPDU (CBPDU), used for Spanning Tree computation
- Topology Change Notification (TCN) BPDU, used to announce changes in the network topology
- Topology Change Notification Acknowledgment (TCA)

BPDUs are exchanged regularly (every 2 seconds by default) and enable switches to keep track of network changes and to start and stop forwarding at ports as required.

When a device is first attached to a switch port, it will not immediately start to forward data. It will instead go through a number of states while it processes BPDUs and determines the topology of the network. When a host is attached such as a computer, printer or server the port

will always go into the forwarding state, albeit after a delay of about 30 seconds while it goes through the listening and learning states (see below). The time spent in the listening and learning states is determined by a value known as the forward delay (default 15 seconds and set by the root bridge). However, if instead another *switch* is connected, the port may remain in blocking mode if it is determined that it would cause a loop in the network. Topology Change Notification (TCN) BPDUs are used to inform other switches of port changes. TCNs are injected into the network by a non-root switch and propagated to the root. Upon receipt of the TCN, the root switch will set a Topology Change flag in its normal BPDUs. This flag is propagated to all other switches to instruct them to rapidly age out their forwarding table entries.

Spanning Tree port states:

- **Blocking** - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- **Listening** - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- **Learning** - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- **Forwarding** - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port

Now consider the following topology

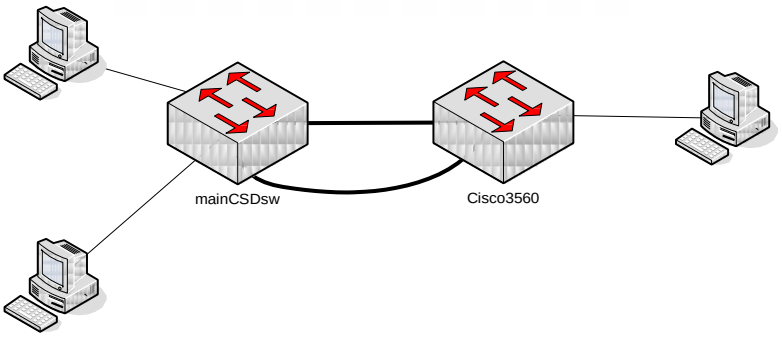


Fig 14.1: Scenario for implementing spanning tree

Here a physical loop can be observed

Now observe the spanning tree calculations for **mainCSDsw** first

```
mainCISDsw#sh spanning-tree
VLAN0001
```

```
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0010.1100.58CE
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0010.1100.58CE
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface         Role Sts Cost      Prio.Nbr Type
----------------- ---- --- --------- -------- --------------------------------
--
Et3/1             Desg FWD 100       128.4    P2p
Et2/1             Desg FWD 100       128.3    P2p
Et0/1             Desg FWD 100       128.1    P2p
Et1/1             Desg FWD 100       128.2    P2p

For cisco3560 the calculations will be

Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0010.1100.58CE
              Cost        100
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B02B.5EA0
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface         Role Sts Cost      Prio.Nbr Type
----------------- ---- --- --------- -------- --------------------------------
--
Fa0/1             Root FWD 100       128.1    P2p
Fa0/3             Altn BLK 100       128.3    P2p
Fa0/2             Desg FWD 19        128.2    P2p
```

Modifying priorities and other parameters

To change default priority one can use the following command.

```
mainCISDsw(config)#spanning-tree vlan 1 priority 36864
```

Now see what happens to the root bridge.

```
mainCISDsw#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     00E0.B02B.5EA0
              Cost        100
              Port        1(Ethernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority     36865  (priority 36864 sys-id-ext 1)
             Address      0010.1100.58CE
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   20

Interface         Role Sts Cost      Prio.Nbr Type
----------------- ---- --- --------- -------- --------------------------------
--
Et3/1             Altn BLK 100       128.4    P2p
Et2/1             Desg FWD 100       128.3    P2p
Et0/1             Root FWD 100       128.1    P2p
Et1/1             Desg FWD 100       128.2    P2p
```

Other details on STP can be observed through the following set of commands under spanning tree.

```
Switch#sh spanning-tree ?
  active      Report on active interfaces only
  detail      Detailed information
  interface   Spanning Tree interface status and configuration
  summary     Summary of port states
  vlan        VLAN Switch Spanning Trees
  <cr>
```

EXERCISES

1. What is used to prevent switching loops in a network with redundant switched paths?

2. When is STP considered said to be converged?

Lab Session 12

OBJECT

Configuring Virtual LANs

THEORY

A **virtual LAN**, commonly known as a **VLAN**, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

To physically replicate the functions of a VLAN, it would be necessary to install a separate, parallel collection of network cables and switches/hubs which are kept separate from the primary network. However unlike a physically separate network, VLANs must share bandwidth; two separate one-gigabit VLANs using a single one-gigabit interconnection can both suffer reduced throughput and congestion. It virtualizes VLAN behaviors (configuring switch ports, tagging frames when entering VLAN, lookup MAC table to switch/flood frames to trunk links, and untagging when exit from VLAN.)

Implementation

A basic switch not configured for VLANs will either have VLAN functionality disabled, or will have it permanently enabled with what is known as a *default VLAN* which simply contains all ports on the device as members.

Configuration of the first custom VLAN port group usually involves subtracting ports from the default VLAN, such that the first custom group of VLAN ports is actually the second VLAN on the device, apart from the default VLAN. The default VLAN typically has an ID of 1.

If a VLAN port group were to only exist on the one device, all ports that are members of the VLAN group only need to be "untagged". It is only when the port group is to extend to another device that tagging is used. For communications to occur from switch to switch, an uplink port needs to be a tagged member of every VLAN on the switch that uses that uplink port, including the default VLAN.

Some switches either allow or require a name be created for the VLAN, but it is only the VLAN group number that is important from one switch to the next.

Where a VLAN group is to simply pass through an intermediate switch via two pass-through ports, only the two ports need to be a member of the VLAN, and are tagged to pass both the required VLAN and the default VLAN on the intermediate switch.

Management of the switch requires that the management functions be associated with one of the configured VLANs. If the default VLAN were deleted or renumbered without moving the

management to a different VLAN first, it is possible to be locked out of the switch configuration, requiring a forced clearing of the device configuration to regain control.

Switches typically have no built-in method to indicate VLAN port members to someone working in a wiring closet. It is necessary for a technician to either have management access to the device to view its configuration, or for VLAN port assignment charts or diagrams to be kept next to the switches in each wiring closet. These charts must be manually updated by the technical staff whenever port membership changes are made to the VLANs.

Remote configuration of VLANs presents several opportunities for a technician to accidentally cut off communications and lock themselves out of the devices they are attempting to configure. Actions such as subdividing the default VLAN by splitting off the switch uplink ports into a separate new VLAN can suddenly cut off all remote communication, requiring the technician to physically visit the device in the distant location to continue the configuration process.

When inside the world of VLANs there are two types of links. These links allow us to connect multiple switches together or just simple network devices e.g PC, that will access the VLAN network. Depending on their configuration, they are called Access Links, or Trunk Links.

Access Links
Access Links are the most common type of links on any VLAN switch. All network hosts connect to the switch's Access Links in order to gain access to the local network. These links are your ordinary ports found on every switch, but configured in a special way, so you are able to plug a computer into them and access your network.

Trunk Link
A Trunk Link, or 'Trunk' is a port configured to carry packets for any VLAN. These type of ports are usually found in connections between switches. These links require the ability to carry packets from all available VLANs because VLANs span over multiple switches.

PROCEDURE

VLAN 1 is the default

```
Switch #sh int vlan 1

Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 00e0.b02b.5ea0 (bia 00e0.b02b.5ea0)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Configuring IP on default VLAN

Switch(config)#int vlan 1
Switch(config-if)#ip address 172.16.68.2 255.255.248.0

Creating VLANs

```
Switch(config)#int vlan 2
```

Assigning ports to vlans

```
Switch(config)#int fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
```

Configuring trunk link

Consider the following topology

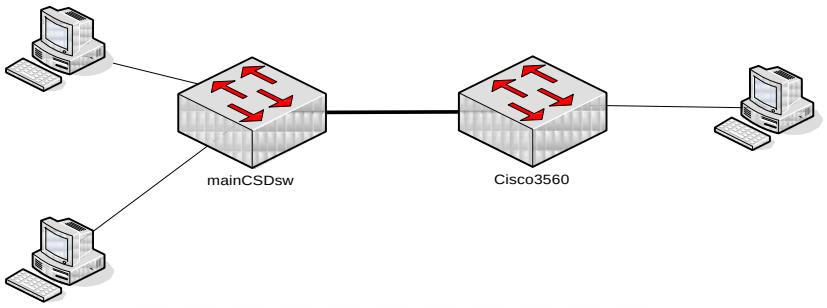


Fig 14.1: Scenario for implementing VLANs

Suppose mainCSDsw has two VLANs configured VLAN1 and VLAN2, whereas cisco3560 has only VLAN1. Now both switched must have at least one common trunk link connecting the two switches, so that the PCs which are in VLAN1 may communicate. Here we have interface fa 0/1 on each switch connected to the other. Hence the configuration would be

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode trunk
```

Verification of configurations

```
Switch#show interface switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
```

```
Appliance trust: none

Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
```

A more handy way of verifying VLAN memberships would be

```
mainCISDsw#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Eth2/1, Eth3/1, Eth4/1
2    VLAN0002                         active    Eth1/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

EXERCISES

1. What does trunking provide?

_____

_____

_____

2. What type of link is only part of one VLAN and is referred to as the “native VLAN” of the port?

_____

_____

_____

_____

Lab Session 13

OBJECT

To Configure VTP (VLAN Truncking Protocol) on Cisco Switches

THEORY

VTP

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products.

A switch using VTP can be configured in one of three modes: server, client, or transparent.

VTP Server Mode

- By default the switch is in this mode.
- VTP servers advertise the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain
- VTP servers store the VLAN information for the entire domain in NVRAM
- The server is where VLAN is created, deleted, or renamed for the domain
- Synchronized VLAN information

VTP Transparent Mode

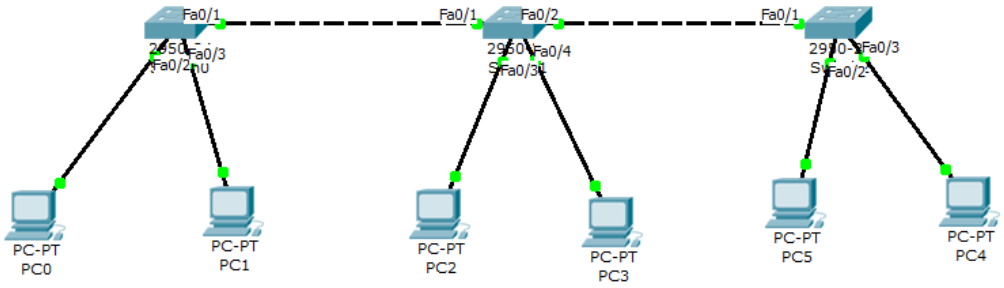
- VTP transparent advertise the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain.
- VTP transparent store the VLAN information for the entire domain in NVRAM
- The transparent is where VLAN is created, deleted, or renamed for the domain
- VLANs that are created, renamed, or deleted on transparent switches are local to that switch only, hence cannot synchronize VLAN information

VTP Client Mode

- VTP clients function the same way as VTP servers.
- VTP clients advertise the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain.
- VTP clients cannot store the VLAN information for the entire domain in NVRAM
- The client is where VLAN cannot be created, deleted, or renamed for the domain
- Synchronized VLAN information

PROCEDURE

1. Design a topology having 3 switches and 2 end devices in each switch. The figure shows the architecture of the topology.



2. Create trunk port in every switch's ports. Then create a VTP domain in the first switch named 'ahsandm', using command: '**vtp domain ahsandm**'. Now allocate a password to the switch by using command: '**vtp password abc**'. The below commands describes all the steps.

```
Switch(config)#hostname ahsan
ahsan(config)#inter
ahsan(config)#interface fa0/1
ahsan(config-if)#sw
ahsan(config-if)#switchport mode
ahsan(config-if)#switchport mode tr
ahsan(config-if)#switchport mode trunk
ahsan(config-if)#exit
ahsan(config)#vtp domain ahsandm
Changing VTP domain name from NULL to ahsandm
ahsan(config)#vtp password abc
Setting device VLAN database password to abc
```

3. Apply the same password on other two switches as well.

4. Now check the VTP status using command: '**show vtp status**' in all the switches

```
ahsan#shw
ahsan#sho
ahsan#show vt
ahsan#show vtp st
ahsan#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : ahsandm
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD2 0x64 0xE7 0xCB 0xBE 0x3A 0xF6 0x
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

5. Now create 3 new VLAN in the first switch

```
ahsan(config)#vlan 3
ahsan(config-vlan)#exit
ahsan(config)#vlan 4
ahsan(config-vlan)#exit
ahsan(config)#vlan 2
ahsan(config-vlan)#exit
ahsan(config)#
ahsan(config)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, 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
2    VLAN0002                          active
3    VLAN0003                          active
5    VLAN0005                          active
10   VLAN0010                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

6. Now change the mode of 2nd switch to transparent and the 3rd to client mode.

```
ahsan(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

```
ahsan(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

7. Create a VLAN 10 in the 1st switch (server mode switch) and then check it in the switch with transparent mode, the VLAN 10 does not exist satisfying that switch with this mode cannot synchronize VLAN information.

```
ahsan(config)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, 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
2    VLAN0002                          active
3    VLAN0003                          active
5    VLAN0005                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. Now to study the property of switch in client mode, create a VLAN in this switch using command: '**vlan 11**', you can see the VLAN will not be created.

```
ahsan(config)#valn 11
              ^
% Invalid input detected at '^' marker.
```

EXERCISES

1. Why passwords for VTP should be same on all switches in a same VTP domain.

2. Write down the observations of a switch in VTP Transparent mode.

3. Write down a command which convert server mode switch into client mode

Lab Session 14

OBJECT

Recovering lost router password.

THEORY

In this lab you will learn the procedures required to recover a lost login or enable password. The procedures differ depending on the platform and the software used, but in all cases, password recovery requires that the router be taken out of operation and powered down. Note:

1. Please use cisco as the password where necessary.

2. Please be prepared to do password recovery right away. The group before you might have set a password other than cisco.

3. Use `show version` command to determine the platform before you try the password recovery.

You will be working with the configuration register as part of this lab. The config-register is a 16 bit register. Look up information about the config-register on documentation CD, CISCO web site, or any other resources available to you.

Software Configuration Register Bits (What do they mean)

Bit Number	Value	Meaning
0 to 3	0x000**0** to 0x000**F**	Boot field
6	0x0040 (setting bit 6 to 1)	Causes system software to ignore NVRAM contents
8	0x0100	Break disabled
13	0x2000	Boot default Flash software if network boot fails

Explanation of Boot Field

Boot Field	Meaning
0x0000	Stays at the system bootstrap prompt
0xXXX1	Boots the first system image in onboard Flash memory
0xXXX2 0xXXXF	If you set the boot field value to 0x2 through 0xF and there is a valid **boot system** command stored in the configuration file, the router boots the system software as directed by that value. If there is no boot system command, the router forms a default boot filename for booting from a network server. If there is no network server configured, as is the case in our lab, the standard setup dialogue is started.

PROCEDURE

Assume you have been locked out of the router. You have access only to the user mode. Follow the instructions below from the user mode. Do not get into privileged mode.

1. Type `show version` and record the value of the configuration register.

2. Using the power switch, turn off the router and then turn it on.

3. Press CTRL+Break on the terminal keyboard within 60 seconds of the powerup to put the router into ROMMON mode.

4. This is where the procedure differs depending on the platform.

   For 25XX and 4000:

- Type `o/r 0x2142` or `0x42` at the > prompt to boot from flash without loading the configuration.
- Type `i` or `reset` at the > prompt. The router reboots but ignores its saved configuration.

For 2600, 3600, 4500, 4700:

- Type `confreg 0x2142` at the rommon 1> prompt to boot from Flash without loading the configuration.
- Type `reset` at the rommon 2> prompt. The router reboots but ignores its saved configuration.

5. Type no after each setup question or press Ctrl-C to skip the initial setup procedure.

6. Type `enable` at the Router> prompt. You'll be in enable mode and see the Router# prompt.

7. Type `config mem` or `copy start running` to copy the nonvolatile RAM (NVRAM) into memory. **Do not type config term.**

8. Type `config term` and make the changes. The prompt is now hostname(config)#.

9. Type `enable password <password>` to set the password to the new value or issue the command `no enable password`.

10. Type `config-register 0x2102`, or the value you recorded in step 1.

11. Type `write mem` or `copy running startup` to commit the changes.

12. Type `show version` and observe the configuration register setting carefully.

EXERCISES

1. Explain the setting when the configuration-register is set to 0x2542.

2. There are many different ways to access a router. Write down these ways.

3. Explain the need for step 7 in password recovery procedure.

4. Write down the difference between "`enable password`" and "`enable secret password`."

5. What happens if "`enable password`" and "`enable secret password`" are the same?

6. When you configure enable password and issue the command show running, you can see the password set for the privileged mode. Is there a method to prevent it from being visible?

7. Set the configuration-register to 0x2542. Reload the router. Does the break sequence work? Crosscheck with configuration-register settings and see if it matches with the settings. Is there any difference? Explain

DEPARTMENT OF COMPUTER & INFORMATION SYSTEMS ENGINEERING
BACHELORS IN COMPUTER SYSTEMS ENGINEERING

RUBRIC (Rubric Code: RUB-CS01)

Course Code: _____ Week #: _____ Lab #: _____

Assigned task: _____

_____

_____

CRITERIA AND SCALES			
Criterion 1: To what extent has the student organized the circuit components / hardware resources?			
0	1-2	3-4	
The circuit components / hardware resources have been laid in a haphazard manner	The circuit components / hardware resources have been partially organized	The circuit components/ hardware resources have been well organized	
Criterion 2: Is the student at ease with handling of the equipment?			
0	1-2	3-4	
The student is not confident with the handling of equipment	The student is confident to some extent with the handling of equipment	The student is confident with the use of equipment	
Criterion 3: How well has the student interconnected the circuit components / hardware resources?			
0	1-2	3-4	
Student has no idea how to connect the circuit components / hardware resources	Circuit components / hardware resources are not connected properly	Circuit components / hardware resources are properly connected	
Criterion 4: Has the student been able to achieve the desired outputs?			
0	1-2	3-4	
The task is incomplete, no outputs have been achieved	Task has partially been completed on time, the outputs are erroneous	Task has been completed on time, desired outputs have been achieved	
Criterion 5: How would you grade the interaction of the student with lab resources (lab personnel, participant students, equipment)?			
0	1-2	3-4	
The student took no notice of the lab resources	The student was aware of lab resources for a short period of time but was mostly unconcerned	The student effectively interacted with the lab resources	
Criterion 6: What is the student's level of confidence with the Simulation Tool Interface, if used?			
0	1-2	3-4	5
The student is unfamiliar with the tool	The student is familiar with the visible features of the tool	The student is familiar with the unexposed features of the tool	The student is proficient with the tool

DEPARTMENT OF COMPUTER & INFORMATION SYSTEMS ENGINEERING
BACHELORS IN COMPUTER SYSTEMS ENGINEERING

RUBRIC (Rubric Code: RUB-CS01)

Course Code: _____ Week #: _____ Lab #: _____

Assigned task: _____

_____

_____

CRITERIA AND SCALES			
Criterion 1: To what extent has the student organized the circuit components / hardware resources?			
0	1-2	3-4	
The circuit components / hardware resources have been laid in a haphazard manner	The circuit components / hardware resources have been partially organized	The circuit components/ hardware resources have been well organized	
Criterion 2: Is the student at ease with handling of the equipment?			
0	1-2	3-4	
The student is not confident with the handling of equipment	The student is confident to some extent with the handling of equipment	The student is confident with the use of equipment	
Criterion 3: How well has the student interconnected the circuit components / hardware resources?			
0	1-2	3-4	
Student has no idea how to connect the circuit components / hardware resources	Circuit components / hardware resources are not connected properly	Circuit components / hardware resources are properly connected	
Criterion 4: Has the student been able to achieve the desired outputs?			
0	1-2	3-4	
The task is incomplete, no outputs have been achieved	Task has partially been completed on time, the outputs are erroneous	Task has been completed on time, desired outputs have been achieved	
Criterion 5: How would you grade the interaction of the student with lab resources (lab personnel, participant students, equipment)?			
0	1-2	3-4	
The student took no notice of the lab resources	The student was aware of lab resources for a short period of time but was mostly unconcerned	The student effectively interacted with the lab resources	
Criterion 6: What is the student's level of confidence with the Simulation Tool Interface, if used?			
0	1-2	3-4	5
The student is unfamiliar with the tool	The student is familiar with the visible features of the tool	The student is familiar with the unexposed features of the tool	The student is proficient with the tool

DEPARTMENT OF COMPUTER & INFORMATION SYSTEMS ENGINEERING
BACHELORS IN COMPUTER SYSTEMS ENGINEERING

RUBRIC (Rubric Code: RUB-CS01)

Course Code: _____ Week #: _____ Lab #: _____

Assigned task: _____

_____

_____

CRITERIA AND SCALES			
Criterion 1: To what extent has the student organized the circuit components / hardware resources?			
0	1-2	3-4	
The circuit components / hardware resources have been laid in a haphazard manner	The circuit components / hardware resources have been partially organized	The circuit components/ hardware resources have been well organized	
Criterion 2: Is the student at ease with handling of the equipment?			
0	1-2	3-4	
The student is not confident with the handling of equipment	The student is confident to some extent with the handling of equipment	The student is confident with the use of equipment	
Criterion 3: How well has the student interconnected the circuit components / hardware resources?			
0	1-2	3-4	
Student has no idea how to connect the circuit components / hardware resources	Circuit components / hardware resources are not connected properly	Circuit components / hardware resources are properly connected	
Criterion 4: Has the student been able to achieve the desired outputs?			
0	1-2	3-4	
The task is incomplete, no outputs have been achieved	Task has partially been completed on time, the outputs are erroneous	Task has been completed on time, desired outputs have been achieved	
Criterion 5: How would you grade the interaction of the student with lab resources (lab personnel, participant students, equipment)?			
0	1-2	3-4	
The student took no notice of the lab resources	The student was aware of lab resources for a short period of time but was mostly unconcerned	The student effectively interacted with the lab resources	
Criterion 6: What is the student's level of confidence with the Simulation Tool Interface, if used?			
0	1-2	3-4	5
The student is unfamiliar with the tool	The student is familiar with the visible features of the tool	The student is familiar with the unexposed features of the tool	The student is proficient with the tool