LABORATORY MANUAL

ECE-418

COMMUNICATION NETWORKS PROJECT LABORATORY

Name of the Student:……..
Registration Number/Roll No…….
Section and Group……

General Guidelines for students

1. Don't switch ON the power supply without confirming the connections from the lab instructor.
2. Be as neat as possible. Keep the work area and workbench clear of items not used in the experiment.
3. Always check to see that the power switch is OFF before plugging into the outlet. Also, turn instrument or equipment OFF before unplugging from the outlet.
4. When unplugging a power cord, pull on the plug, not on the cable.
5. When disassembling a circuit, first remove the source of power.
6. Report any damages to equipment, hazards, and potential hazards to the laboratory instructor.
7. Shoes must be worn at all times.
8. Observe polarity when connecting polarized components or test equipment into a circuit.
9. Keep soldering irons in their protective stand when not in use.
10. Double check circuits for proper connections and polarity prior to applying the power.
11. Food and drinks are prohibited in the lab area.
12. Do not work with wet hands or large amounts of metal jewellery.
13. Place the IC's properly in the bread board; Don't break the IC pins by forcefully inserting in bread board.
14. Always cut wire leads so the clipped wire falls on table top and not towards others.
15. Switch off the power supply when not in use.
16. Never change wiring with circuit plugged into power source.
17. Students are allowed in the laboratory only when the lab instructor is present.
18. Open drinks and food are not allowed near the lab benches.
19. Report any broken equipment or defective parts to the lab instructor. Do not open, remove the cover, or attempt to repair any equipment.
20. When the lab exercise is over, all instruments, except computers, must be turned off. Return substitution boxes to the designated location. Your lab grade will be affected if your laboratory station is not tidy when you leave.
21. University property must not be taken from the laboratory.
22. Do not move instruments from one lab station to another lab station.
23. Do not tamper with or remove security straps, locks, or other security devices.

Table of Contents

EXPERIMENT-1

AIM: To perform the router configuration using subnetting and VLSM concept on cisco packet tracer.

Software used: Cisco packet tracer

Learning Objective: To learn the subnetting and VLSM

Procedure:

1. Develop a topology by connecting three routers with each other.

2. Configure the routers by connecting serial cables between them.

3. By switching on the router enter into its config mode to configure the routers by following commands:

Simulation Commands

Router 1
Router# config t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#int fa0/0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Router(config-if)#ip address 192.168.1.1
255.255.255.240 Router(config-if)#no shut
Router2(config-if)#int fa0/1
Router(config-if)#ip address 192.168.1.17
255.255.255.240 Router(config-if)#no shut
Smilarly configure the third router by giving IP address.
The above configuration shows that the subnetting has been used in these configuration using class c addressing.

4. Configure the computers if you want to attach it to the routers. It is optional parameter.

5. After giving ip addresses check whether the routers are communicated with each other or not.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-2

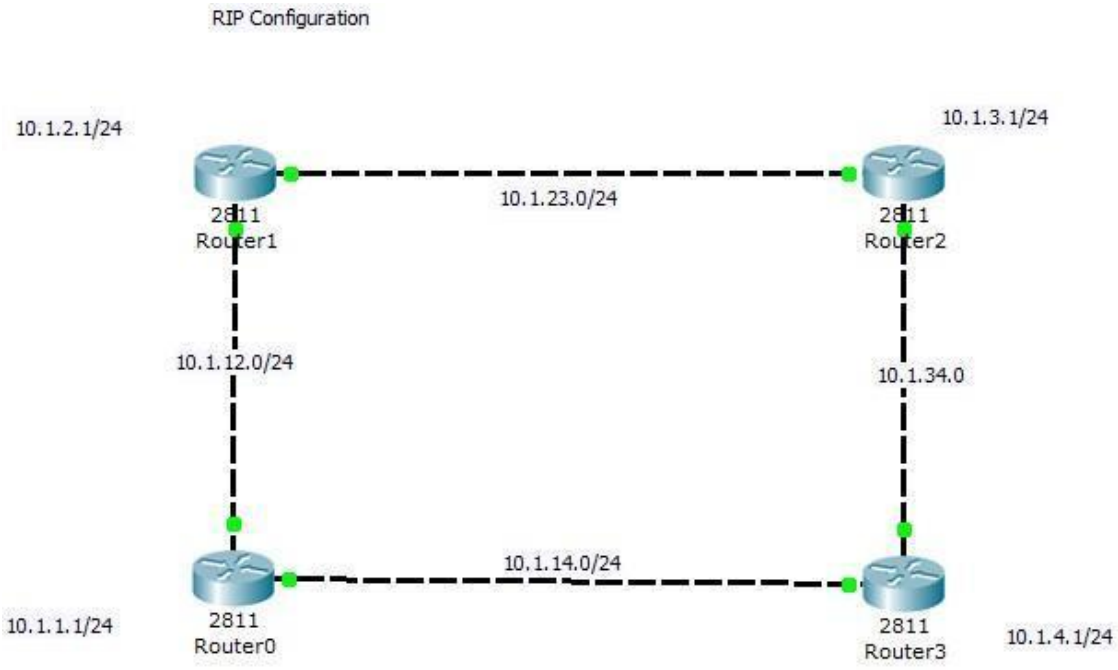
AIM: To implement Distance Vector Routing using RIP on packet tracer.

Software used: Packet tracer

Learning Objective: To learn the network protocol (RIP protocol)

Procedure:

1. Develop a Topology shown in figure given below.
2. Configure all Routers
3. Implement RIP protocols in Router to configure Network.



Router1 configuration.

Continue with configuration dialog? [yes/no]: no

Press RETURN to get

started! Router>
Router>en
Router#config t

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

Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#int fa0/1
Router(config-if)#ip address 192.168.2.1
255.255.255.0 no shut

After that use the router rip command by entering into config mode of router. Router(config)# router rip

network 192.168.1.0
network 192.168.2.0
exit

Similarly do all the steps for rest of the routers by changing their networks and IP addresses.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-3

AIM: To perform the distance vector routing on cisco routers.

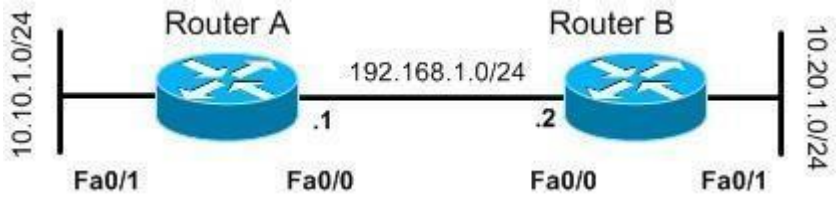
Hardware used: Three/Four Routers, Serial Cable, Two PC's(optional), Patch cords, Console cable

Learning Objective: To learn the distance vector routing with the help of routers.
Procedure: Following should be done to understand this practical.

Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) are examples of Distance Vector routing protocols. RIP is an open standard protocol while IGRP is a Cisco Proprietary protocol which has been discontinued by Cisco and replaced by an Advanced Distance Vector protocol named Enhanced Interior Gateway Routing Protocol (EIGRP).

Routing Information Protocol (RIP) is one of the oldest Interior Gateway Protocols and still used in networks today. There are two versions of RIP, version 1 and version 2. RIP uses Hop Count as the metric and used UDP port 520 to send and receive RIP messages. RIP is based on the Bellman-Ford Algorithm and therefore due to the routing by rumor approach it is not a very scalable protocol and used in small networks. RIP sends out routing advertisements every 30 seconds on all RIP enabled interfaces, it also employs several other timers such as the invalid and flush timers.

Configuration of RIP is very simple. Shown below is a two router network. RIP is being used to advertise the LANs attached to each router so that they are reachable with each other.



RIP Configuration Basic Configuration

RouterA(config)# router rip RouterA(config-router)#

version 2

RouterA(config-router)# no auto-summary

RouterA(config-router)# network 10.0.0.0

RouterA(config-router)# network 192.168.1.0

Modifying Updates

RIP uses hop count as the metric and we can only modify it using the offset-list feature which is covered in detail in Routing Filtering & Manipulation. It must be noted that offset-list feature is a protocol independent feature used for other routing protocols as well such as EIGRP. However, parameters and characteristics of a RIP routing update can be modified. By default, RIP version 2 updates are multicast and we can configure a Router to unicast these updates.

RouterA(config)# router rip

RouterA(config-router)# neighbor 192.168.1.2

RouterA(config-router)# passive-interface fa0/0

The neighbor commands instruct RIP to send unicast routing updates to the specified neighbor and the passive-interface command is used to suppress multicast updates out that interface. This is usually used when a router connects on multi-access segment and we want to exchange RIP information with only a specific neighbor.

We can also modify various timers associated with RIP such as the update timer which defines the rate in seconds at which RIP updates are sent. Below is the command syntax to modify various timers used by RIP.

RouterA(config)# router rip

RouterA(config-router) # timer basic *update invalid holddown flush*

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-4

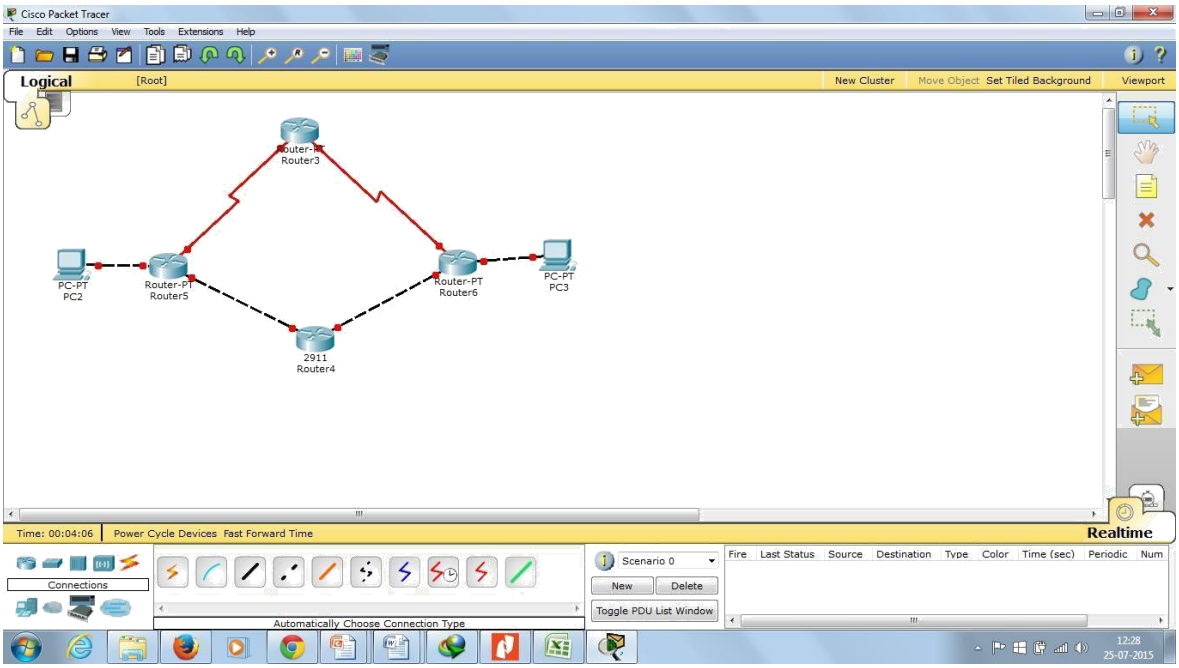
AIM: To implement link state routing using OSPF in packet tracer.

Software used: Packet tracer

Learning Objective: To learn the Link State Protocol

Procedure:

1. Develop a Topology shown in figure given below.
2. Configure the PC's by giving IP addresses.
3. Configure Router 0 by following commands: Router>enable
   Router# config t
   Router(config)# int fa0/0 (if fast Ethernet is using)
   Router(if-config)# ip address 192.168.1.1 255.255.255 no shut
   Configure Router 1(Serial Connection) Router>enable
   Router# config t
   Router(config)# int se0/0 (if serial cable is using)
   Router(if-config)# ip address 192.168.2.1 255.255.255 clock rate 64000
   no shutdown
   Similarly do for other two routers.
4. Now apply ospf protocol in all routers
5. Here we are showing for router 0 only. Similarly, you can apply for others routers. Go to router 0
   Router(config)#router ospf 1 network 192.168.1.0 0.0.0.255 area0 network 192.168.2.0 0.0.0.255 area0 network 192.168.3.0 0.0.0.255 area0
   Because in scenario three networks are attached to a router.
6. Similarly, you can configure all other routers by same method.


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Router-PT
Router3
PC-PT
PC2
Router-PT
Router5
Router-PT
Router6
PC-PT
PC3
2911
Router4
Time: 00:04:06
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
12:28
25-07-2015

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-5

AIM: To perform the link state routing on cisco routers.

Hardware used: Three/Four Routers, two serial cables, Two PC's(optional), Patch cords, Console cable

Learning Objective: To learn the link state routing with the help of routers.
Procedure: Following should be done to understand this practical.

Connect the routers with serial cable and configure it through the console cable. The OSPF protocol is sending the following packet types:

1. Hello – discover the neighbors,elect Designated Router(DR)
2. DBD – Database Description is used to check whether database is synchronized between the source and destination.
3. LSR – Link-State Request is used for requesting link state records.
4. LSU – Link-State Update packets are used to reply to LSRs and also use to announce the update in topology.
5. LSAack – Link-State Acknowledgement is the acknowledgement to LSU.

OSPF uses the Dijkstra's shortest path first algorithm (SPF) to create the SPF tree.

We can use the same scenario and configurations which we have used in experiment 3. Refer experiment three for configuration.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-6

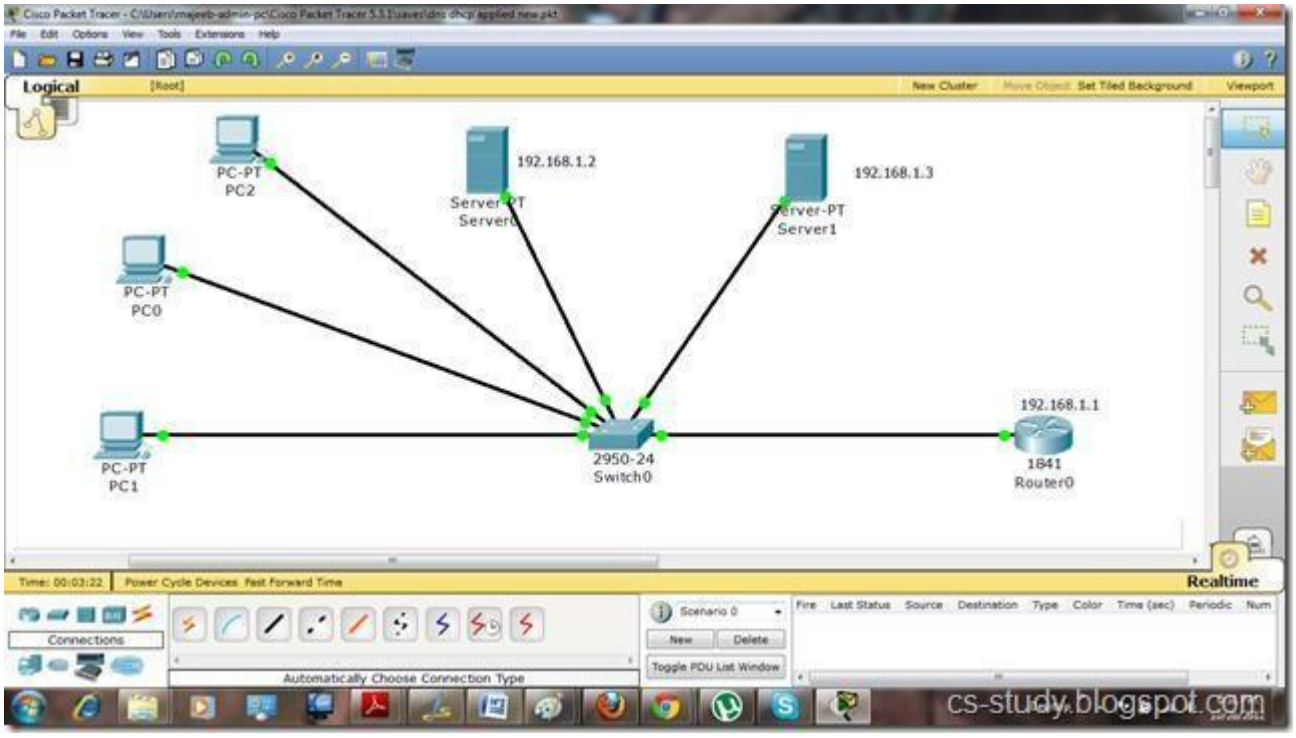
AIM: To create a DHCP and DNS server in packet tracer.

Software used: Packet Tracer

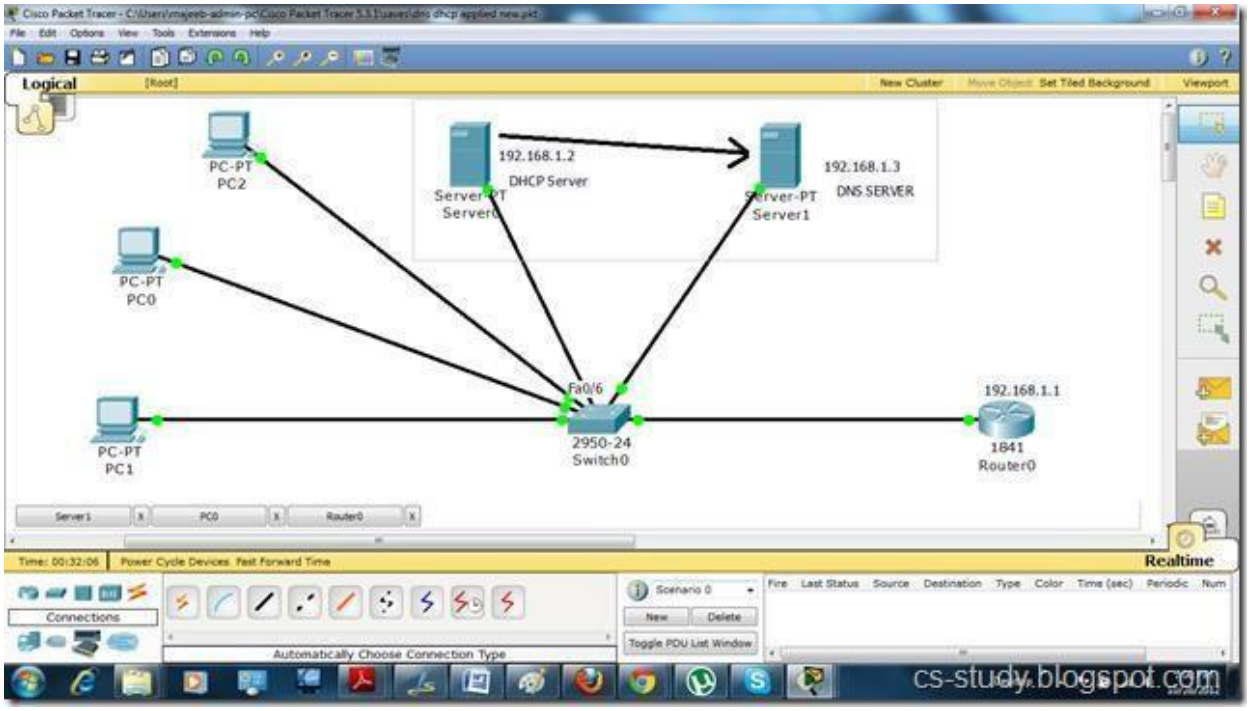
Learning Objective: To learn how to create a DNS in packet tracer.

Procedure:

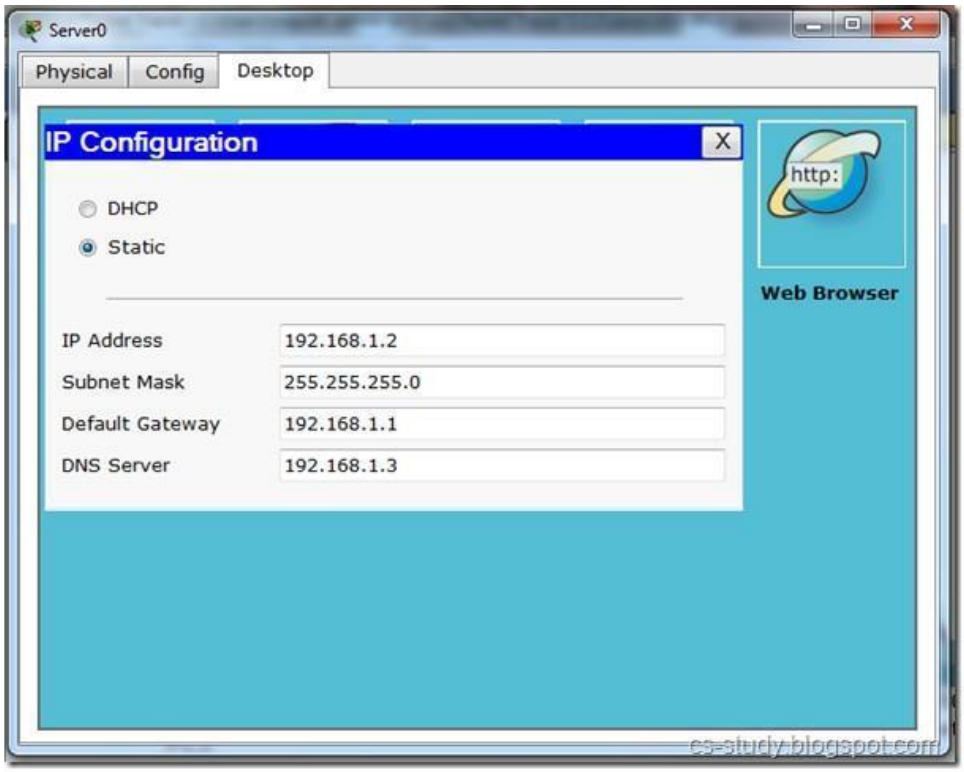
1. Make the topology as shown in figure below:



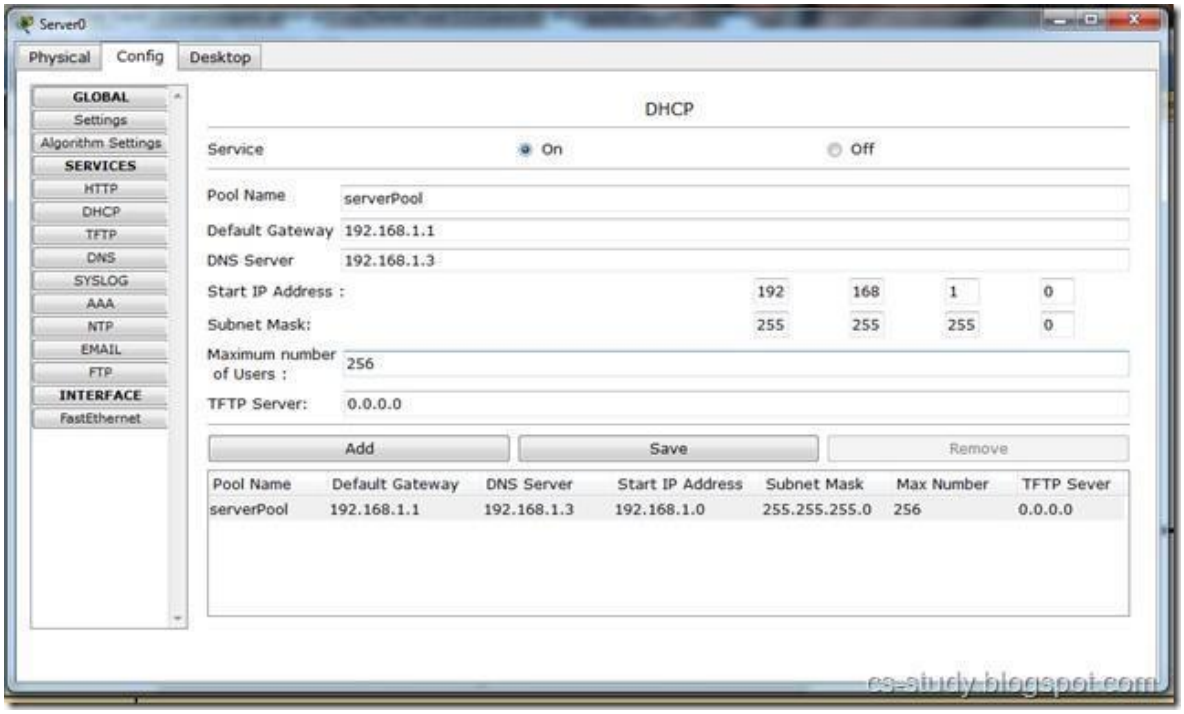
Server 0 in the above figure is DHCP server and Server 1 is the DNS server.



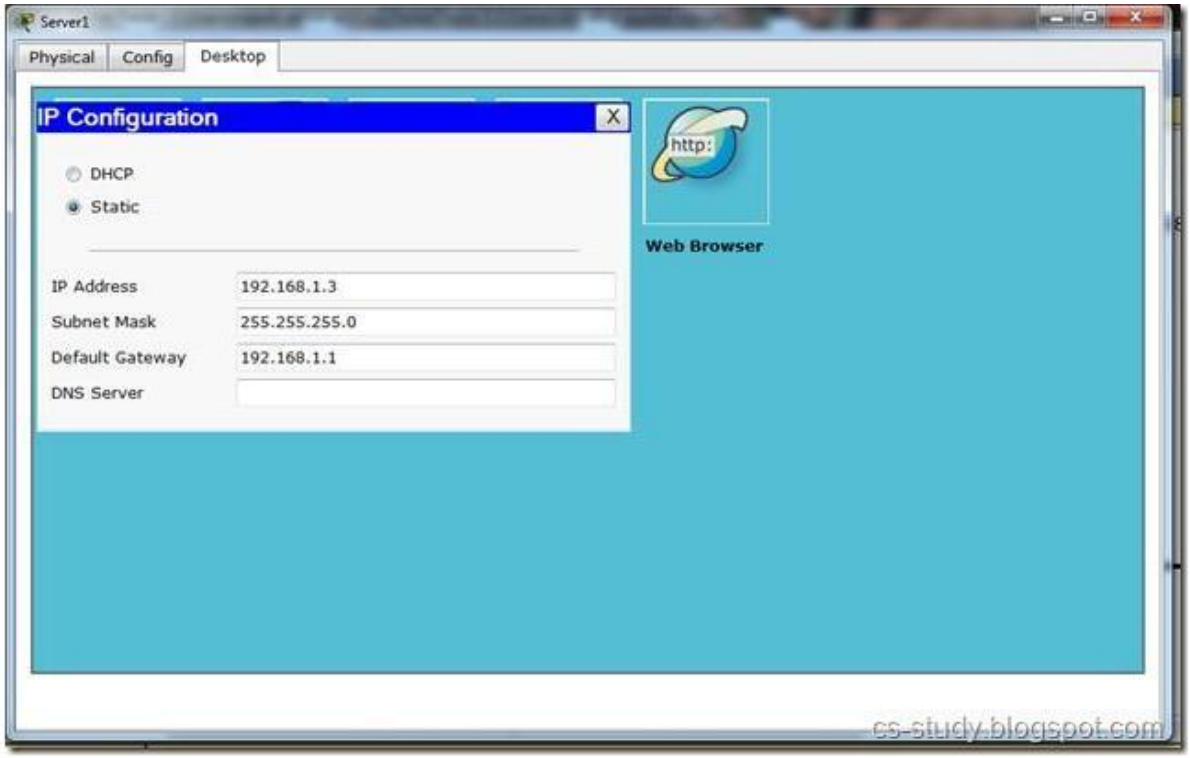
Configure the IP on server 0.



Configure the DHCP on server 0.

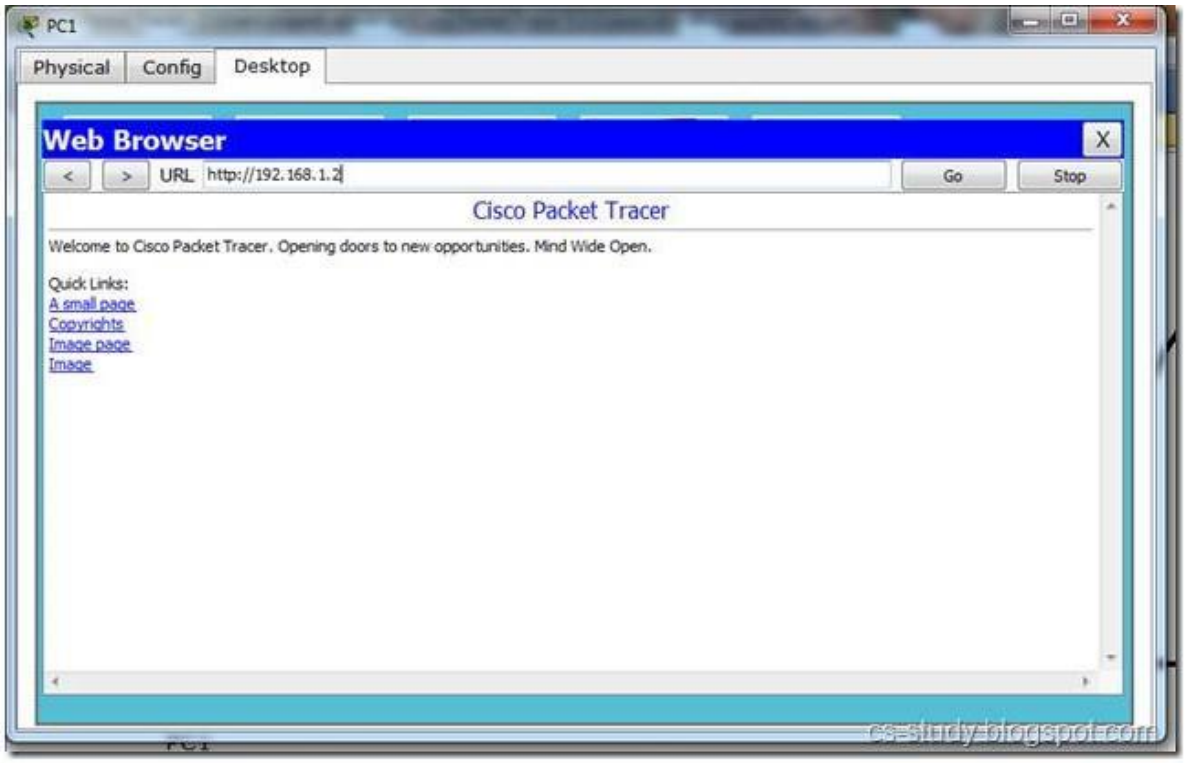


Configure IP on server 1.

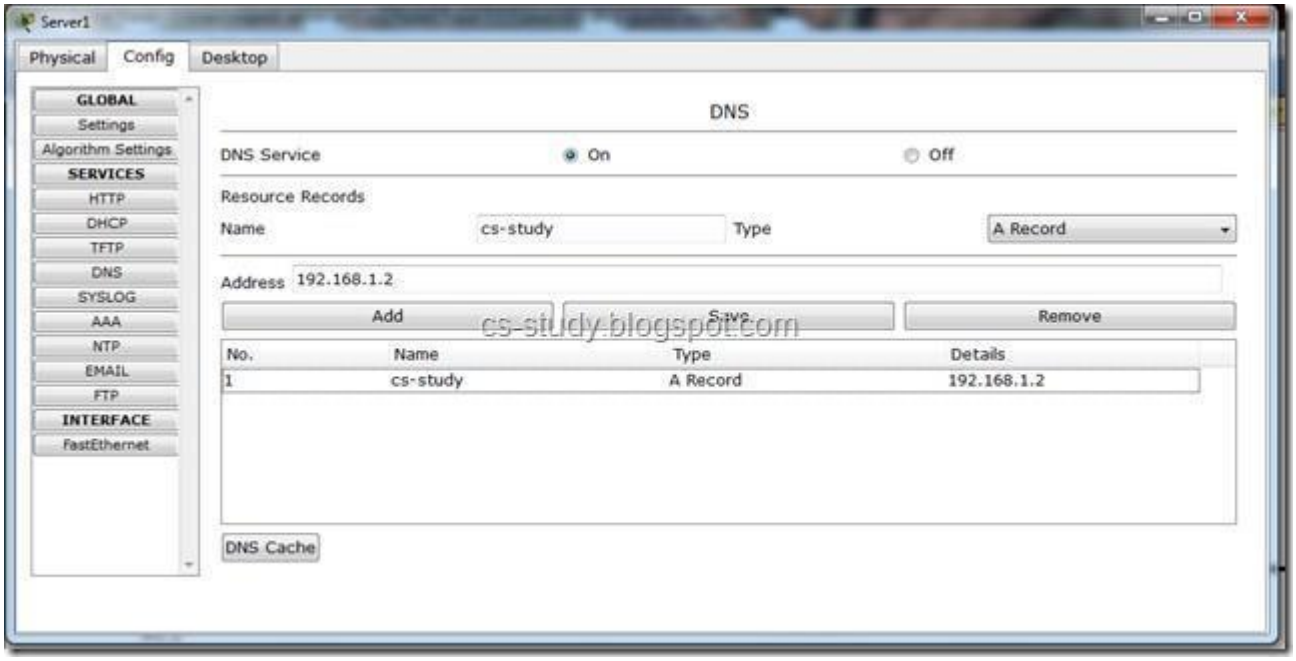


Change the mode of PC and select DHCP.

Go to Web Browser and enter the ip of Server 0.By entering this you will be able to access the website of server.



Now, configure the DNS on server 1.



Now again go to web browser and PC and enter the name that you set it for DNS.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-7

AIM: To make the straight and cross cable of Cat5/Cat6 and share the data between devices.

Equipment Used: Crimping Tool, RJ-45 Connectors, Network Cable (CAT5 or CAT6), two computers.

Learning Objective: To learn the working of network devices and how to make the network cable.

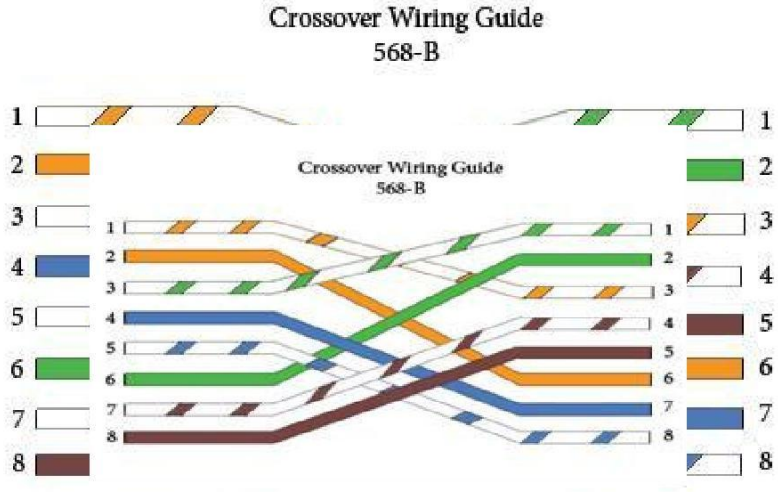
Procedure: To make the cable following steps should be followed.

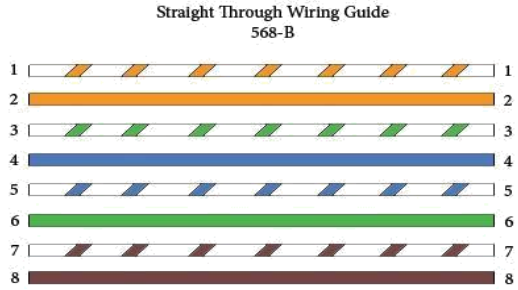
1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Carefully cut the wires because if the internal wires cut off the wire will be damaged.

2. Untwist all the wires and straighten that so that it can be crimped easily and put off in RJ-45 connector.

3. Now you have to ends and arrange their ends according to their color coding given below:

Diagram shows you how to prepare Cross wired and straight through connection





B) To make a point to point connection between two computers. Following steps to follow.

Using crossover Ethernet cable connects both PCs via the (RJ45) port.

PC - 1:

Give the IP address to the PC-1. Any class you can use.

Switch of the firewall by moving to the control panel.

Share any file or folder by right click on that.

PC - 2:

Give the IP address to the PC-1. Use the same network and class as it is used in PC-1.

If the ping shows reply from both the computers, then you can share files and folders between the computers.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-8

AIM: To analyze various methods of network configuration and network troubleshooting.

Software used: Packet tracer and command prompt

Equipment Used: Two Computers, Network Cable OR (we can also perform on a packet tracer)

Learning Objective: To learn the various network configuration commands and how to connect two computers on a network.

Procedure:

Following is a list of the basic **network troubleshooting commands** that are built-in the Windows based operating systems and UNIX etc. The right use of these troubleshooting commands can help a lot in diagnosing and resolving the uncommon network problems. If you would like terms directly related to routers please see router networking terms.

PING

Ping is the most important troubleshooting command and it checks the connectivity with the other computers. For example, your system's IP address is 10.10.10.10 and your network servers' IP address is 10.10.10.1 and you can check the connectivity with the server by using the Ping command in following format.

At DOS prompt type Ping 10.10.10.1 and press enter.

If you get the reply from the server then the connectivity is ok and if you get the error message like this "Request time out" this means the there is some problem in the connectivity with the server.

PING Options:

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-4] [-6 target_name

Options:

-t	Pings the specified host until stopped. To see statistics and continue - Type Control-Break; To stop - press Ctrl+C.
-a	Resolve addresses to hostnames.
-n	count Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i	TTL Time To Live.
-v	TOS Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).

-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only). Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

IPCONFIG

IPconfig is another important command in Windows. It shows the IP address of the computer and also it shows the DNS, DHCP, Gateway addresses of the network and subnet mask. At DOS prompt type ipconfig and press enter to see the IP address of your computer.

At DOS prompt type inconfig/all and press enter to see the detailed information. USAGE:

ipconfig [/allcompartments] [/? | /all | /renew [adapter] | /release [adapter] | /renew6 [adapter] | /release6 [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid] | /showclassid6 adapter | /setclassid6 adapter [classid]]

Options:

/all	Display full configuration information.
/release	Release the IPv4 address for the specified adapter.
/release6	Release the IPv6 address for the specified adapter.
/renew	Renew the IPv4 address for the specified adapter.
/renew6	Renew the IPv6 address for the specified adapter.
/flushdns	Purges the DNS Resolver cache.
/registerdns	Refreshes all DHCP leases and re-registers DNS names
/displaydns	Display the contents of the DNS Resolver Cache.
/showclassid	Displays all the dhcp class IDs allowed for adapter.
/setclassid	Modifies the dhcp class id.
/showclassid6	Displays all the IPv6 DHCP class IDs allowed for adapter.
/setclassid6	Modifies the IPv6 DHCP class id.

NSLOOKUP

NSLOOKUP is a TCP/IP based command and it checks domain name aliases, DNS records, operating system information by sending query to the Internet Domain Name Servers. You can resolve the errors with the DNS of your network server

HOSTNAME

Hostname command shows you the computer name.

At DOS prompt type Hostname and press enter

NETSTAT

NETSTAT utility shows the protocols statistics and the current established TCP/IP connections in the computer.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases, well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-f	Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays NetworkDirect connections, listeners, and shared endpoints.
-y	Displays the TCP connection template for all connections. Cannot be combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

NBTSTAT

NBTSTAT helps to troubleshoot the NETBIOS name resolutions problems.

NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

-a	(adapter status) Lists the remote machine's name table given its name
-A	(Adapter status) Lists the remote machine's name table given its IP address.
-c	(cache) Lists NBT's cache of remote [machine] names and their IP addresses
-n	(names) Lists local NetBIOS names.
-r	(resolved) Lists names resolved by broadcast and via WINS
-R	(Reload) Purges and reloads the remote cache name table
-S	(Sessions) Lists sessions table with the destination IP addresses

-s	(sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names.
-RR	(ReleaseRefresh) Sends Name Release packets to WINs and then, starts Refresh
RemoteName	Remote host machine name.
IP address	Dotted decimal representation of the IP address.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

ARP

ARP displays and modifies IP to Physical address translation table that is used by the ARP protocols.

ARP -s inet_addr eth_adr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g	Same as –a
inet_addr	Specifies an Internet address.
-N if addr	Displays the ARP entries for the network interface specified by if_addr.
-d	Deletes the host specified by inet_addr.
-s	Adds the host and associates the Internet address inet_addr with the physical address eth_addr. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr	Specifies a physical address
if_addr	If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

FINGER

Finger command is used to retrieve the information about a user on a network.

TRACERT

Tracert command is used to determine the path of the remote system. This tool also provides the number of hops and the IP address of each hop. For example if you want to see that how many hops (routers) are involved to reach www.yahoo.com and what's the IP address of each hop then use the following command.

At command prompt type tracert www.yahoo.com you will see a list of all the hops and their IP addresses.

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

-d	Do not resolve addresses to hostnames.

-h maximum_hops	Maximum number of hops to search for target.
-j host-list	Loose source route along host-list (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.
-6	Force using IPv6.

ROUTE

Route command allows you to make manual entries in the routing table.

Hopefully the above mentioned commands will help you to diagnose the troubleshooting the computer networking problems.

ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

-	Clears the routing tables of all gateway entries. If this is used in conjunction with one of the f commands, the tables are cleared prior to running the command.
-	When used with the ADD command, makes a route persistent across boots of the system. By p default, routes are not preserved when the system is restarted. When used with the PRINT command, displays the list of registered persistent routes. Ignored for all other commands, which always affect the appropriate persistent routes. This option is not supported Windows'95. Command
-4	Force using IPv4.
- Force using IPv6. 6	

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-9

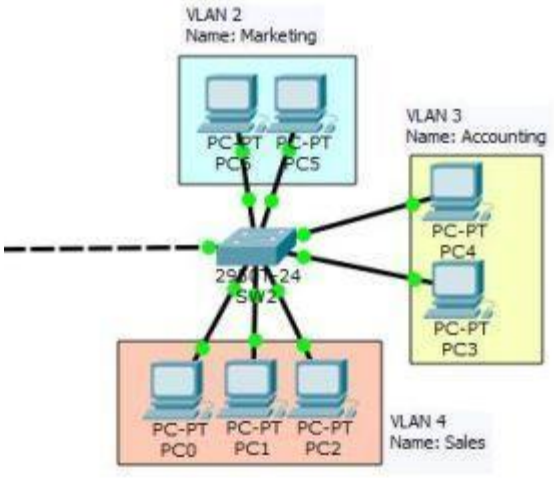
AIM: To learn and implement the basic configuration of switches.

Hardware used: Switches (L2/L3), Serial cable, Console cable and patch cords.

Learning Objective: To learn the basic configuration of switches.

Procedure:

Let's start to configure VLAN on Cisco switch using Cisco Packet Tracer.



Configure VLAN on Cisco Switch

1. Open the VLAN lab and create these three VLAN and named Marketing, Accounting, and Sales. So let's create them with the following commands.
2. First, change the switch name with "**hostname**" command.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. Switch(config)#hostname SW2
SW2(config)#
```

3. Now create the VLANs using "**VLAN"** command.

```
SW2(config)#vlan 2
SW2(config-vlan)#name Marketing
SW2(config-vlan)#vlan 3
SW2(config-vlan)#name Accounting
SW2(config-vlan)#vlan 4
SW2(config-vlan)#name Sales
```

SW2(config-vlan)#

4. Just type the "**do sh vlan**" command from config mod to see whether VLANs are created or not.

```
SW2(config-vlan)#do sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, 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
                                                 Gig0/1, Gig0/2
2    Marketing                         active
3    Accounting                        active
4    Sales                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
```

Show VLAN Command

You see the VLANs are created successfully.

5. Now try to add interfaces to each of these VLANs. All the Interfaces ports are within the default VLAN and not yet grouped to Marketing, Accounting, and Sales. So try to add an interface to a VLAN with the "**Switchport**" command.

```
SW2(config)#interface fastEthernet
0/5 SW2(config-if)#switchport mode
access SW2(config-if)#switchport
access vlan 2 SW2(config-if)#exit
SW2(config)#interface fastEthernet
0/6 SW2(config-if)#switchport mode
access SW2(config-if)#switchport
access vlan 2 SW2(config-if)#
```

I have added the [**fastEthernet 0/5**] and [**fastEthernet 0/6**] to VLAN 2 which is our Marketing VLAN. In this method, we add each interface one by one, but you can use "**Interface range"** command to add a group of ports to a VLAN.

```
SW2(config)#interface range fastEthernet 0/2-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 4
```

6. Finally type "**do sh vlan**" and see the result again.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	

EXPERIMENT-10

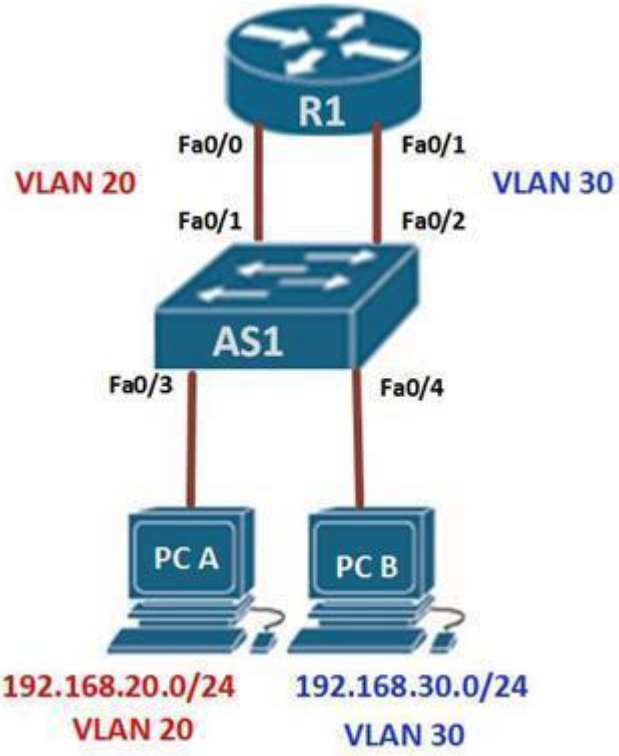
AIM: To learn the implementation of Inter VLAN routing.

Hardware used: Switches (L2/L3), Serial cable, Console cable and patch cords.

Learning Objective: To learn the basic configuration of switches.

Procedure:

In this section, we will configure Inter-VLAN routing on the router and the switch using the scenario we have just seen above. All the VLANs are active and the PCs have been assigned ports, our configuration will only be limited to the router's inter-VLAN configuration and the switch ports connecting to R1.



The ip addressing in use is shown below.

Device	Interface	Ip address	Subnet mask	Default gateway
PC A	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC B	NIC	192.168.30.3	255.255.255.0	192.168.30.1
R1	Fa0/0	192.168.20.1	255.255.255.0	
	Fa0/1	192.168.30.1	255.255.255.0	

Testing connectivity using the ping command should reveal that PC A cannot ping PC B.

The first step is to configure the switchports to access the specified VLAN, fa0/1 to VLAN 20 and fa0/2 to VLAN 30. This is accomplished using the commands shown below.

```
AS1(config)#interface fastEthernet 0/1
AS1(config-if)#switchport mode access
AS1(config-if)#switchport access vlan 20
AS1(config-if)#exit
AS1(config)#interface fastEthernet 0/2
AS1(config-if)#switchport mode access
AS1(config-if)#switchport access vlan 30
AS1(config-if)#exit
```

This is the only configuration on the switch, once this is done save the configuration and move on to the router.

On R1, we need to configure its interfaces with the default gateways corresponding to the VLANs. That is; on fa0/0 -192.168.20.1/24 and on fa0/1 – 192.168.30.1/24. We accomplish this using the commands shown below.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastethernet 0/1
R1(config-if)#ip address 192.168.30.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

With this configuration we should save and test for connectivity on PC A and PC B, by using the ping command, and the results should be successful. Examining the routing table of R1 should show us the two routes as shown in the output below. This confirms that the router knows of the two VLANs and therefore traffic can flow between them.

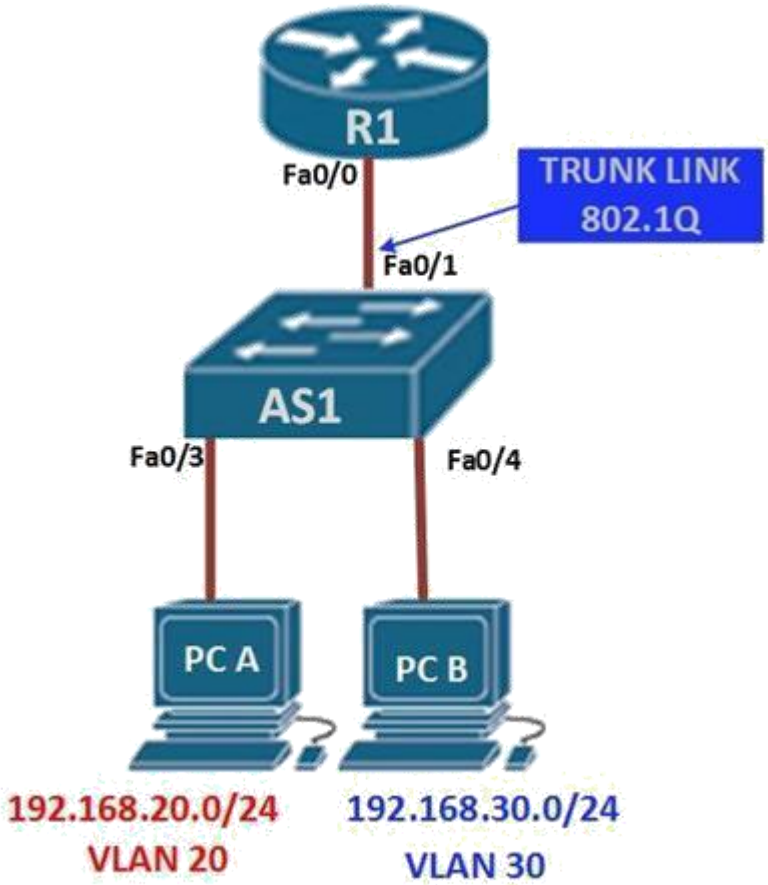
1. Inter-VLAN routing using router-on-a-stick

With the example shown above, there are several concerns, suppose we had 10 or even 20 VLANs configured on the switch, even if the switch has enough ports to support the connection to the router, it is highly unlikely that the router would have so many Ethernet interfaces. Therefore, we need a way to use the limited router interfaces to support routing between many VLANs that may be on a switch.

2. Introduction to Router-on-a-stick

In the second type of inter-VLAN routing which is Router-on-a-stick, the router is connected to the switch using a single interface. The switchport connecting to the router is configured as a trunk link. The single interface on the router is then configured with multiple IP addresses that correspond to the VLANs on the switch. This interface accepts traffic from all the VLANs and determines the destination network based on the source and destination IP in the packets. It then forwards the data to the switch with the correct VLAN information.

As you can see in the diagram below, the router is connected to the switch AS1 using a single, physical network connection.

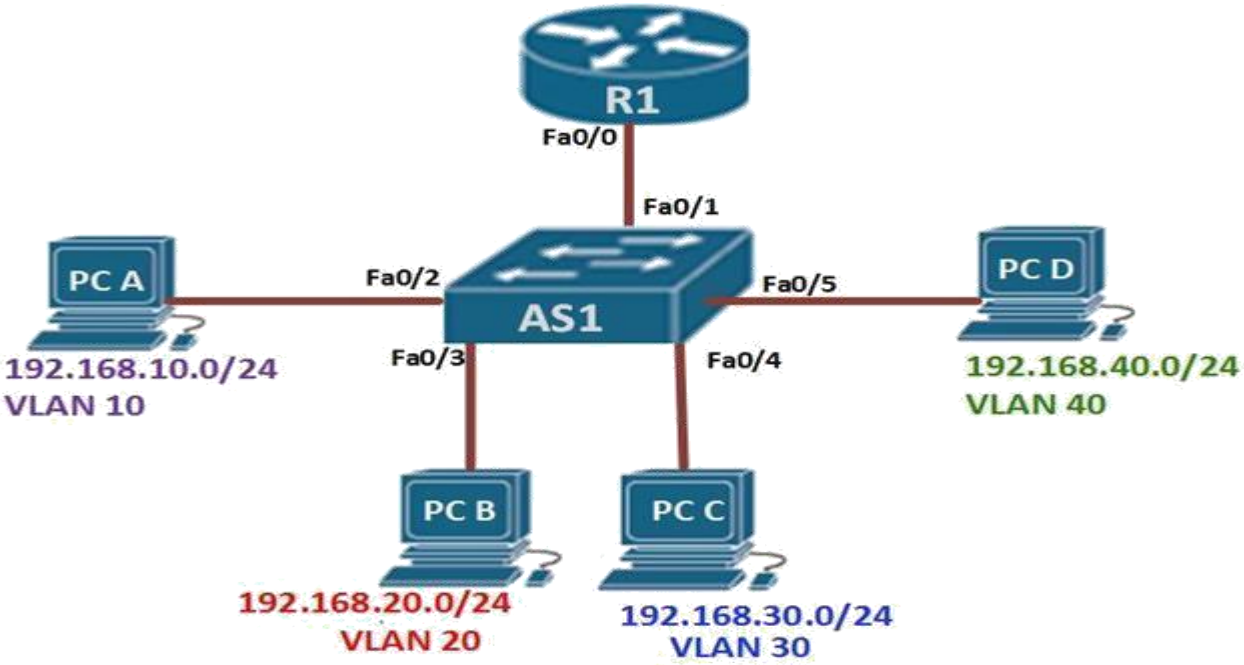


In this type of inter-VLAN routing, the interface connecting the router to the switch is usually a trunk link. The router accepts traffic that is tagged from the VLANs on the switch through the trunk link. On the router, the physical interface is divided into smaller interfaces called subinterfaces. When the router receives the tagged traffic, it forwards the traffic out to the subinterface that has the destination IP address.

subinterfaces aren't real interfaces but they use the LAN physical interfaces on the router to forward data to various VLANs. Each subinterface is configured with an IP address and assigned a VLAN based on the design.

1. Configuring inter-VLAN routing using router-on-a-stick

In this section, we will configure inter-VLAN routing using router-on-a-stick and using the topology shown below. It has been modified by adding additional VLANs so as to show the effectiveness of using router-on-a-stick as opposed to traditional inter-VLAN routing.



In our scenario, we have four hosts located on 4 VLANs, the native VLAN is VLAN 99. Our task is to configure inter-VLAN routing on the router and the switch and ensure that all devices can communicate at the end of the lab. The Ip addressing scheme for the topology is shown below.

Device	Interface	Ip address	Subnet mask	Default gateway
PC A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC B	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC C	NIC	192.168.30.2	255.255.255.0	192.168.30.1
PC D	NIC	192.168.40.2	255.255.255.0	192.168.40.1

NOTE: Unlike traditional inter-VLAN routing, when using subinterfaces, we do not assign an ip address to the interface on the router that is connected to the switch.

In this lab, the configuration on the PC's and the switch ports connecting to them is done correctly, our task is to configure the interface fa0/1 on AS1 and configuration on R1.

Step 1.

On switch AS1 we need to define the interface connected to the router as a **trunk link.** This will allow traffic from all VLANs to get to the router using that interface. The command to accomplish this is on AS1 is:

```
AS1(config)#interface fastEthernet 0/1
AS1(config-if)#switchport mode trunk
```

NOTE: many errors may rise if the switchport connected to the switch is not configured as a trunk.

Step 2.

At this step inter-VLAN routing can be configured on the router. As we mentioned earlier, when configuring router-on-a-stick, we use subinterfaces.

Each subinterface is created using the interface ***interface_id.Subinterface_id*** in the global configuration mode. As shown below.

```
Router(config)#interface <interface_ID.Subinterface_ID>
```

NOTE: the "." Between the interface ID and the subinterface ID is a must. The subinterface ID is a logical number but ideally it should describe the VLAN ID.

To create a subinterface which will be used to route for VLAN 10, we will use the command shown below.

```
R1(config)#interface fastethernet 0/0.10
```

This will take us into the subinterface configuration mode which is denoted by the prompt shown below.

```
R1(config-subif)#
```

In the subinterface mode, we can link the VLAN ID to this interface as well as assign it an ip address and a subnet mask.

Step 3.

To link the subinterface with the specific VLAN, we use the command "**encapsulation dot1q <VLAN_ID>**" this will specify that this interface will get traffic from the specified VLAN. In our example, the command needed to link VLAN 10 to this subinterface is shown below:

```
R1(config-subif)#encapsulation dot1q 10
```

Step 4.

In this mode, we can also assign the subinterface with the ip address and subnet mask which will be used for VLAN 10. The default gateway on the PC's will be used as the interface address as shown below.

```
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
```

Step 5.

When all the subinterfaces have been assigned to their respective VLANs, we need to activate the LAN interfaces that they are connected to by issuing the no shutdown command.

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

This will activate the interface and allow for inter-VLAN routing.

NOTE: the native VLAN is used to carry untagged traffic, the configuration for the native VLAN subinterface on the router is done using the command shown below.

```
router(config-subif)#encapsulation dot1Q <NATIVE_VLAN_ID> native
```

The native keyword is used to identify the specified VLAN as the native VLAN.

In our scenario, the commands needed to configure inter-VLAN routing using router-on-a-stick are shown below.

DEVICE	COMMAND
AS1	AS1(config)#interface fastethernet 0/1 AS1(config-if)#switchport mode trunk AS1(config-if)#exit
R1	R1(config)#interface fastethernet0/0.10 R1(config-subif)#encapsulation dot1Q 10 R1(config-subif)#ip address 192.168.10.1 255.255.255.0 R1(config-subif)#exit R1(config)#interface fastethernet0/0.20 R1(config-subif)#encapsulation dot1Q 20 R1(config-subif)#ip address 192.168.20.1 255.255.255.0 R1(config-subif)#exit R1(config)#interface fastethernet0/0.30 R1(config-subif)#encapsulation dot1Q 30 R1(config-subif)#ip address 192.168.30.1 255.255.255.0 R1(config-subif)#exit R1(config)#interface fastethernet0/0.40 R1(config-subif)#encapsulation dot1Q 40 R1(config-subif)#ip address 192.168.40.1 255.255.255.0 R1(config-subif)#exit R1(config)#interface fastethernet 0/0 R1(config-if)# no shutdown R1(config-if)#exit

With this configuration, we should be able to communicate between the different VLANs.

Date of Performance **Worksheet of the student** **Registration Number**

Aim:

Observation:

Result and Discussion:

Learning Outcomes (what I have learnt):

Sr. No.	Parameter	Marks obtained	Max. Marks
1.	Understanding of the student about the procedure/apparatus.		20
2.	Observations and analysis including learning outcomes		20
3.	Completion of experiment, Discipline and Cleanliness		10
	Signature of Faculty	Total marks obtained	