EXPERIMENT - 7

AIM : Configuration of VLAN in Cisco switch

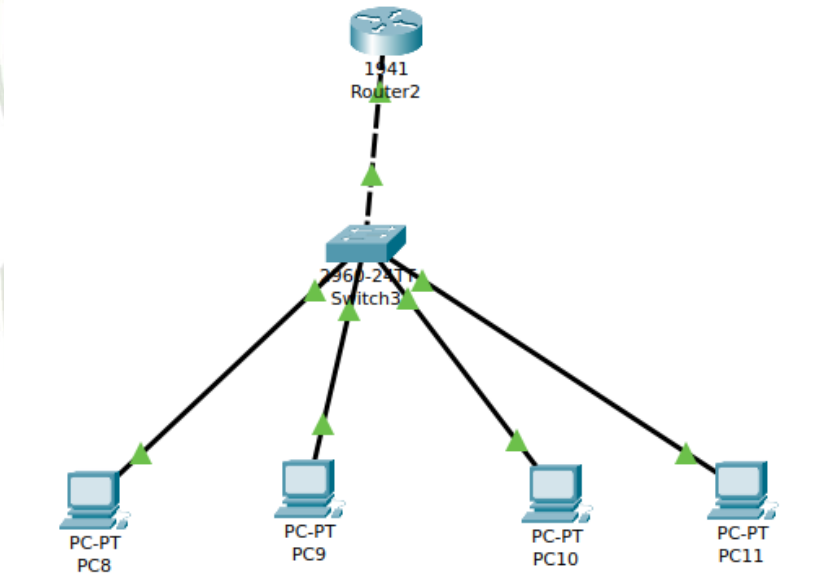
DESCRIPTION:

VLAN (Virtual Local Area Network) is a way to logically divide a physical network into separate, isolated segments. This segmentation helps improve network efficiency, security, and management by grouping devices based on criteria like function or department, even if they share the same physical infrastructure. VLANs allow for better control of broadcast traffic, enhanced security, and increased flexibility in network design.

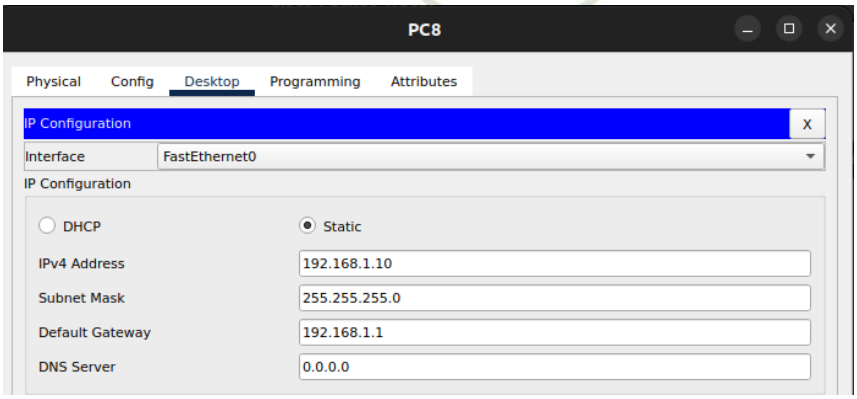
VLAN in Cisco switch :

- Open packet tracker.
- At the bottom we can find many options such as network devices, end device, components, connections etc.
- Select end devices and then choose 4 PCs, a switch-PT and a router- 1941.
- Connect all the devices as shown in the below figure, using connecting wires.
- Change the configuration of the devices accordingly.

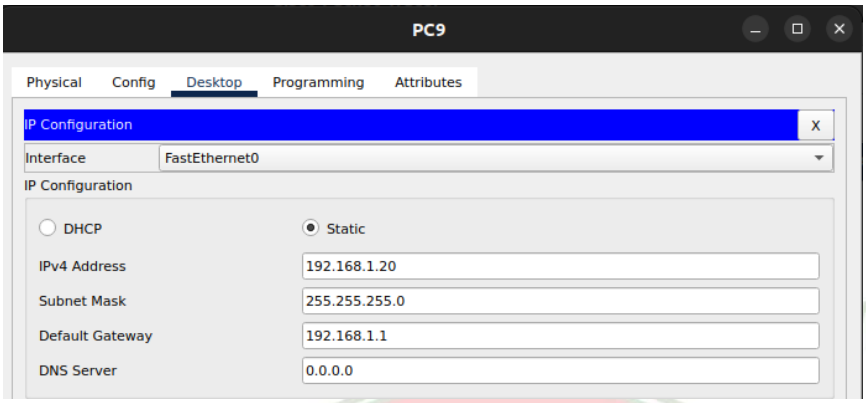
Configuration of VLAN :



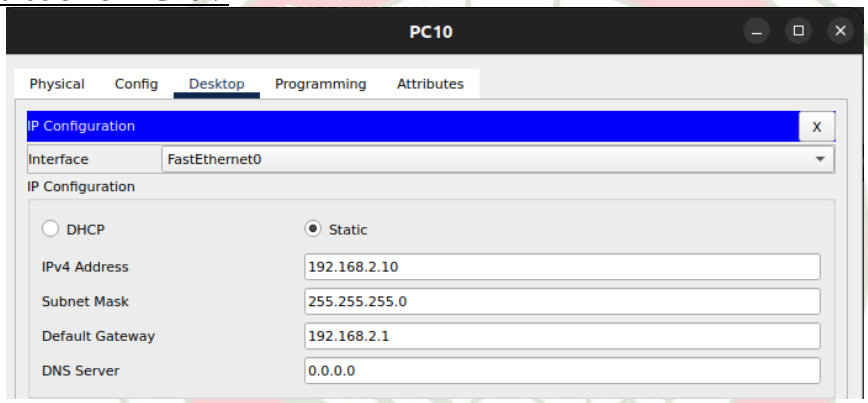
Configuration of PC8 :



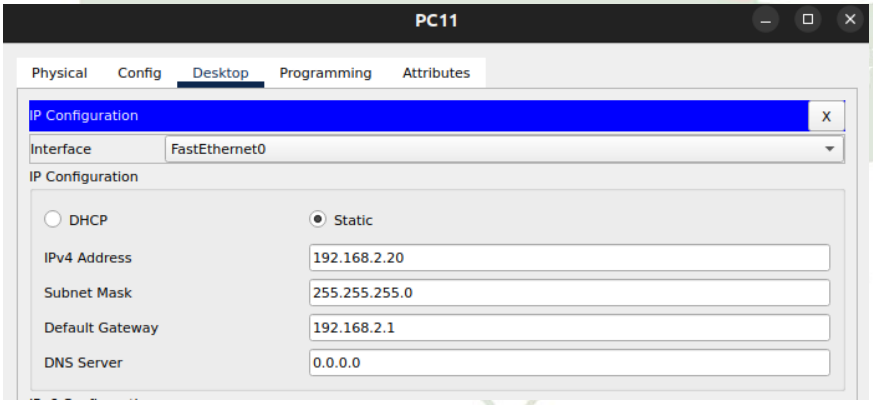
Configuration of PC9 :



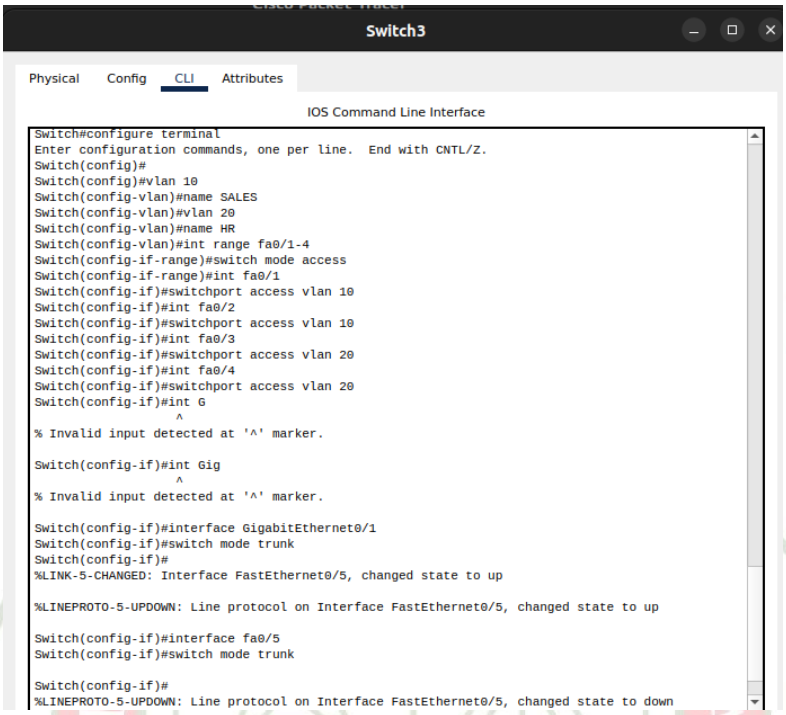
Configuration of PC10 :



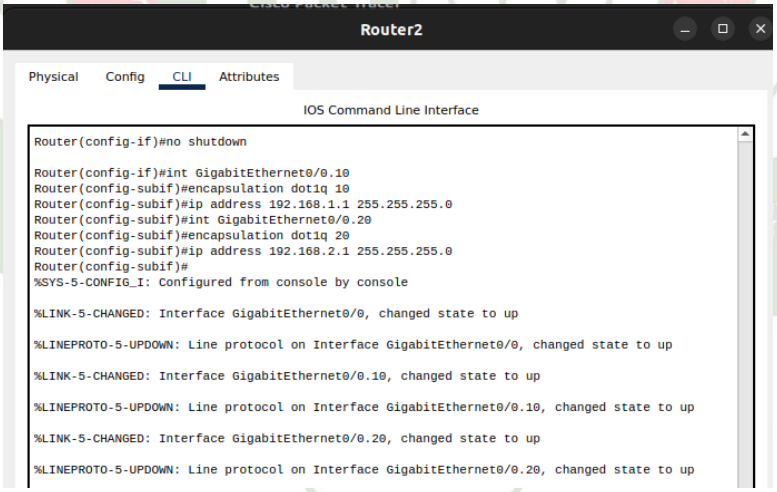
Configuration of PC11 :



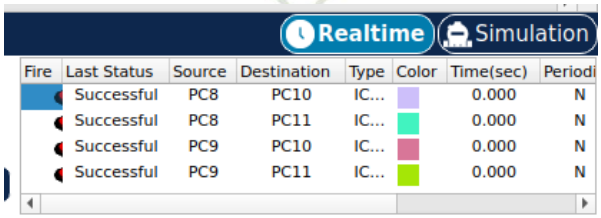
Configuration of switch:



Configuration of Router:



RESULT:



CONCLUSION:

We can see that the packet is successfully transmitted from PC8 to PC9. Thus the configurations and connections are correct.

EXPERIMENT -8

AIM: Develop different local area networks using GNS3. Connect two or more Local area networks. Explore various sub-netting options.

DESCRIPTION:

GNS3 stands for Graphical Network Simulator-3 which is an open source network software emulator that allows the combination of virtual and real networks, used to simulate complex network designs. It uses Dynamips emulation software to simulate Cisco IOS.

The resources utilized are 3 PCs, 1 switch.

Steps to create GNS3 topology with 3 PC's and 1 Switch:

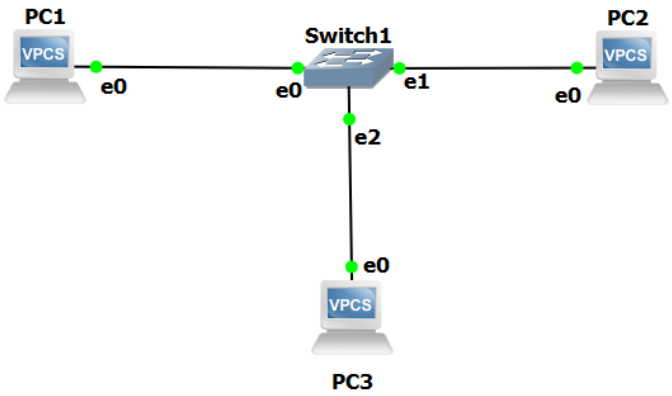
1) Click on **End devices** in the Devices Toolbar, drag and drop 3 instances of **VPCS** to the GNS3 Workspace

2) Click on **Switches** in the Devices Toolbar. Drag and drop the built-in ethernet switch

3) Click the **Add a Link** button, and add links from each PC to switch.

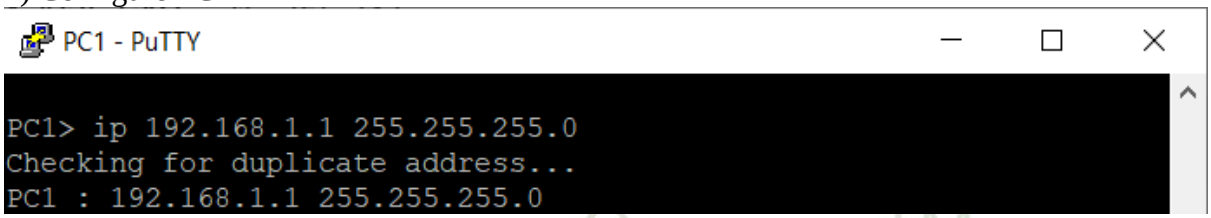
4) Click on the **Interface labels** button on the GNS3 Toolbar, which shows interfaces connected between devices.

5) Click the Green "Play" button on the GNS3 Toolbar to power on all devices in the topology.

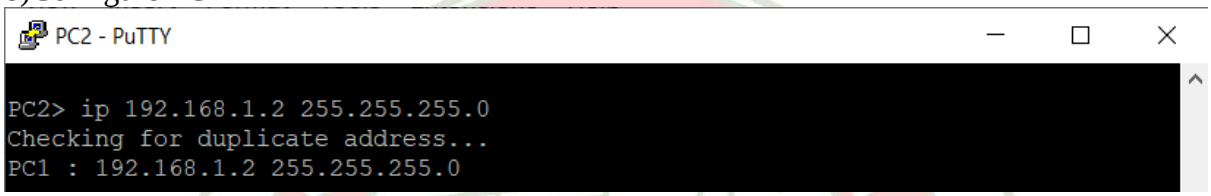


6) Click the **Console connect to all devices** button on the GNS3 Toolbar to open a connection to every device in the topology.

7) Configure PC1

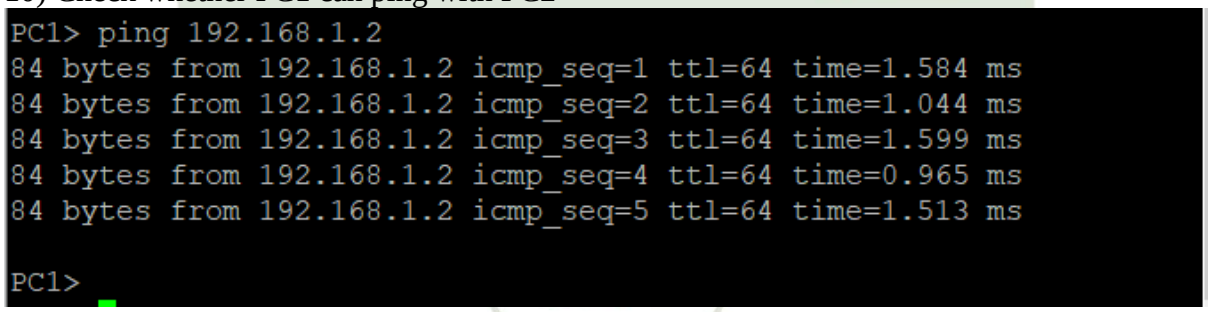


8)Configure PC-2



9)Configure PC3

10) Check whether PC1 can ping with PC2



11) Similarly, check with other PC's

RESULT: After the configuration and connection of all devices, the ping is successful between all the PC's

EXPERIMENT-9

AIM: Configure Static routing using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

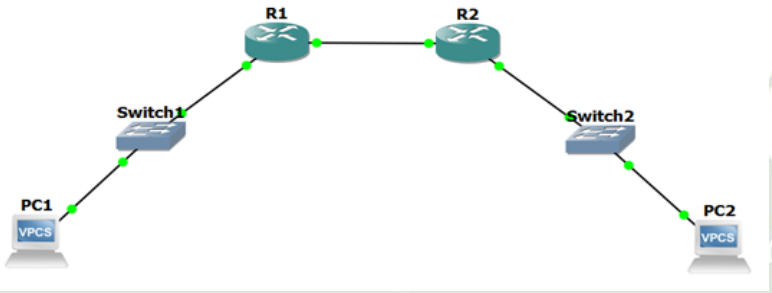
3.Display device information

4.End

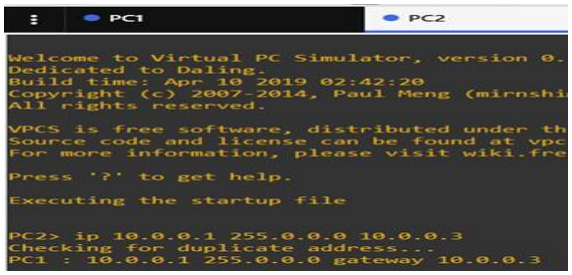
DESCRIPTION AND EXECUTION:

The resources utilized are 2 PCs, 2 switches and 2 routers.

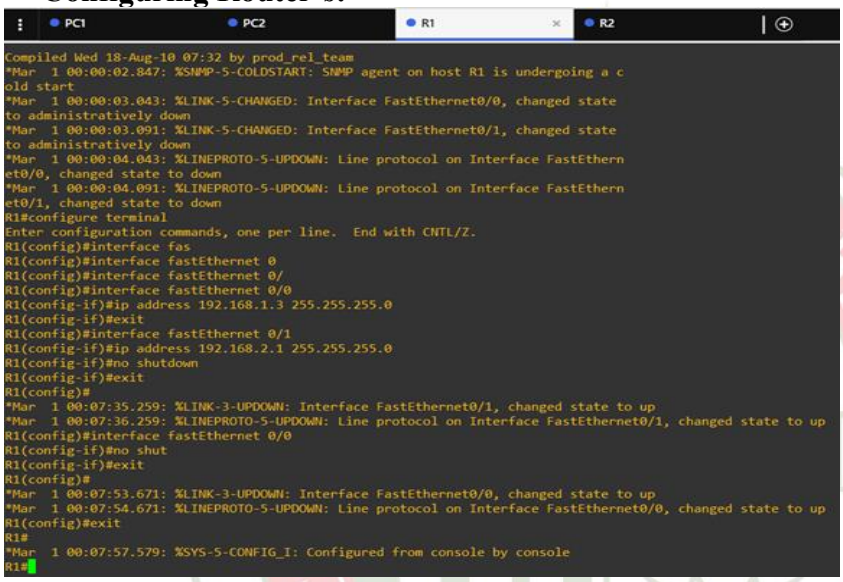
Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the routers.



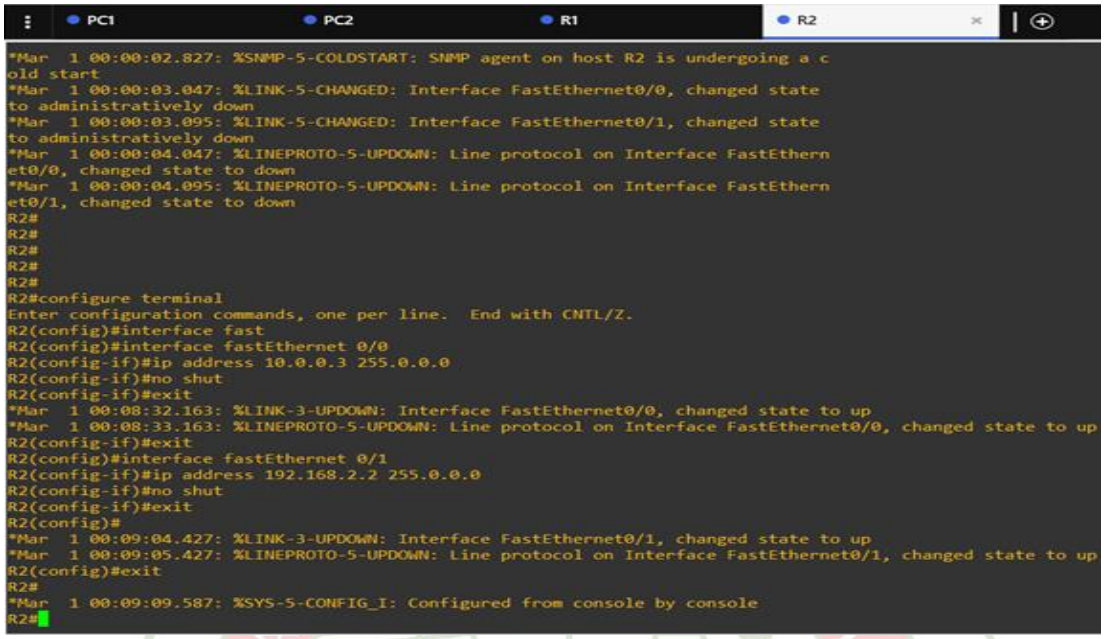
Configuring PC's:

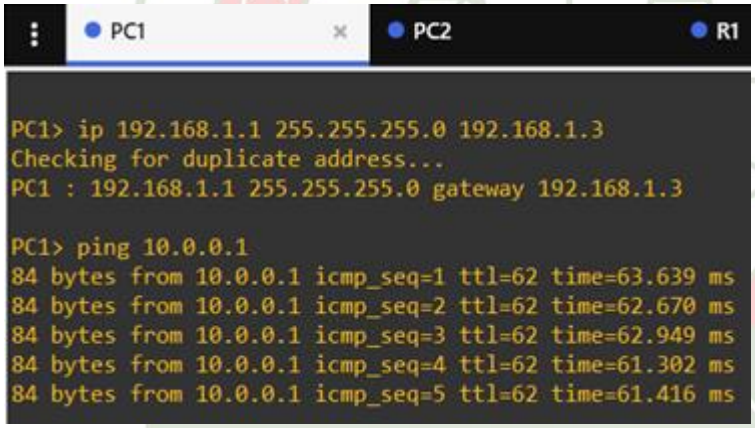


Configuring Router's:



Checking connection:





RESULT: After the configuration and connection of all devices, the ping is successful from PC1 to PC2

EXPERIMENT-10

AIM: Basic OSPF configuration using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

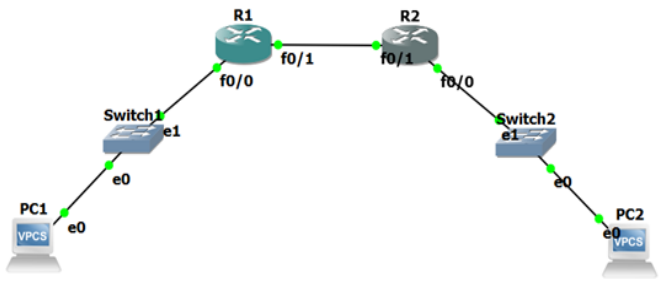
3.Display device information

4.End

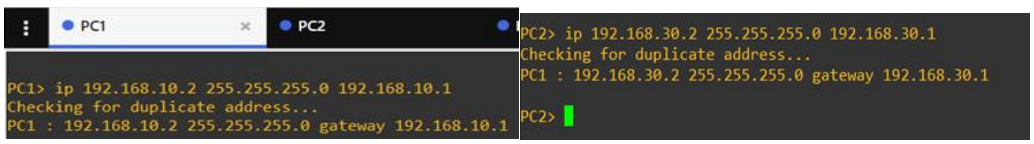
DESCRIPTION AND EXECUTION:

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

The resources utilized are 4 PCs, 1 switch and 1 router. Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the switch and router.



Configuring PC's:



Configuring Router's

PC1 PC2 R1 R2

```
o up
*Mar  1 00:00:03.591: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:03.951: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3600 Software (C3660-A3JK9S-M), Version 12.4(25d), RELEASE S
OFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 07:32 by prod_rel_team
*Mar  1 00:00:03.963: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a c
old start
*Mar  1 00:00:04.455: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Mar  1 00:00:04.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar  1 00:00:05.595: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar  1 00:00:05.599: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:07:06.711: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:07.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#interface f0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:07:26.499: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:27.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config)#
```

PC1 PC2 R1

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.20.0 0.0.0.255 area 0
R1(config-router)#exit
```

PC1 PC2 R1 R2

```
*Mar  1 00:00:03.419: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:00:03.555: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:03.915: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3600 Software (C3660-A3JK9S-M), Version 12.4(25d), RELEASE S
OFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 07:32 by prod_rel_team
*Mar  1 00:00:03.923: %SNMP-5-COLDSTART: SNMP agent on host R2 is undergoing a c
old start
*Mar  1 00:00:04.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Mar  1 00:00:04.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar  1 00:00:05.559: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar  1 00:00:05.563: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.30.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:30.127: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.20.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:53.079: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:54.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
```

```
PC1  PC2  R1  R2
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:30.127: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.20.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:53.079: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:54.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config)#router ospf 1
R2(config-router)#network 192.168.20.0 0.0.0.255 area 0
R2(config-router)#network 192.168
*Mar  1 00:30:12.335: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on FastEthernet0/1 from LOADING to FULL, Loading Done
R2(config-router)#network 192.168.30.0 0.0.0.255 area 0
R2(config-router)#end
R2#
*Mar  1 00:30:48.555: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Checking connection:

```
PC1  PC2  R1
Press '?' to get help.

Executing the startup file


PC2> ip 192.168.30.2 255.255.255.0 192.168.30.1
Checking for duplicate address...
PC1 : 192.168.30.2 255.255.255.0 gateway 192.168.30.1

PC2> pimg 192.168.10.2
Bad command: "pimg 192.168.10.2". Use ? for help.

PC2> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=62 time=36.087 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=62 time=44.473 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=62 time=38.276 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=62 time=36.353 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=62 time=36.766 ms
```

RESULT: After the configuration and connection of all devices, the ping is successful from PC1 to PC2

EXPERIMENT-11

AIM: Basic EIGRP Configuration using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

3.Display device information

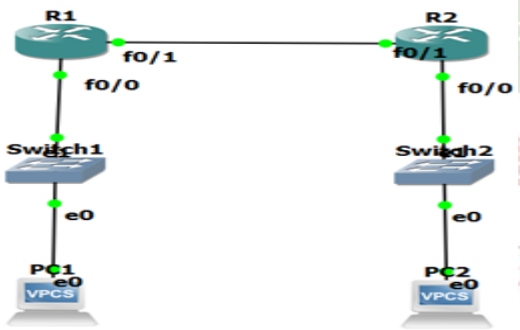
4.End

DESCRIPTION AND EXECUTION:

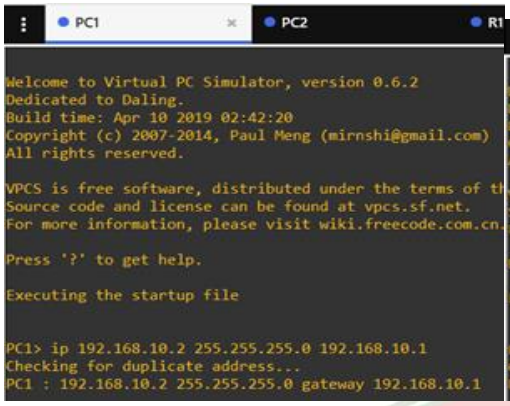
Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP.

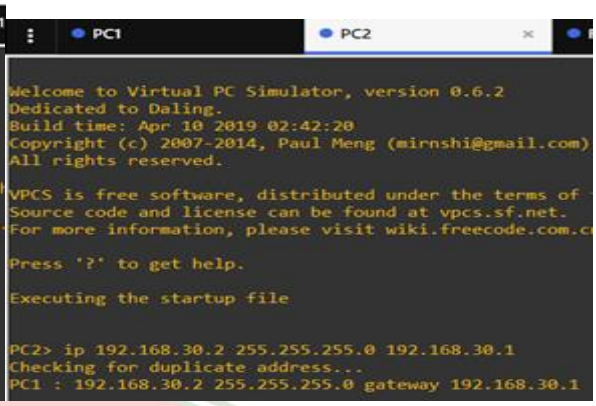
The resources utilized are 2 PCs, 2 switches and 2 routers.

Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the switch and router.

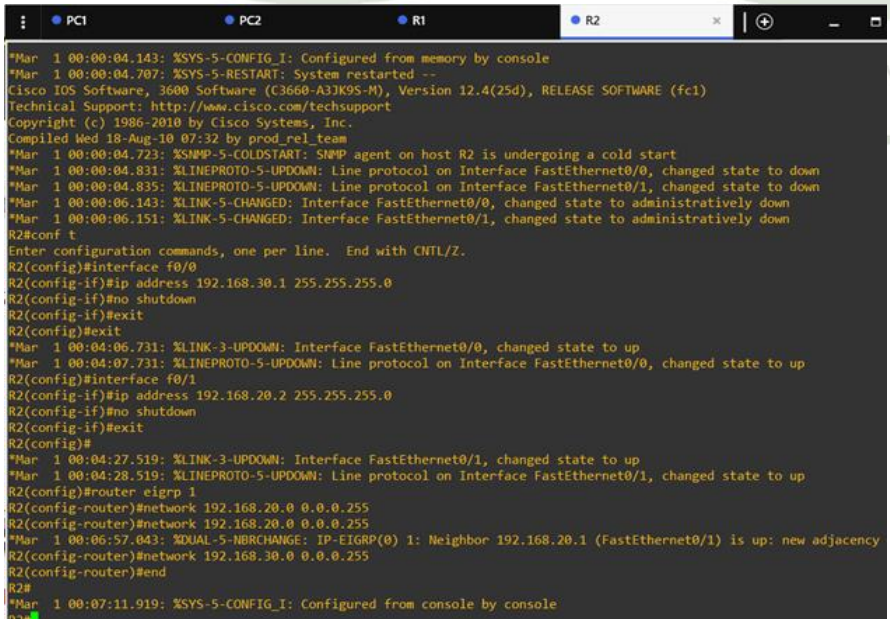


Configuring PC's:

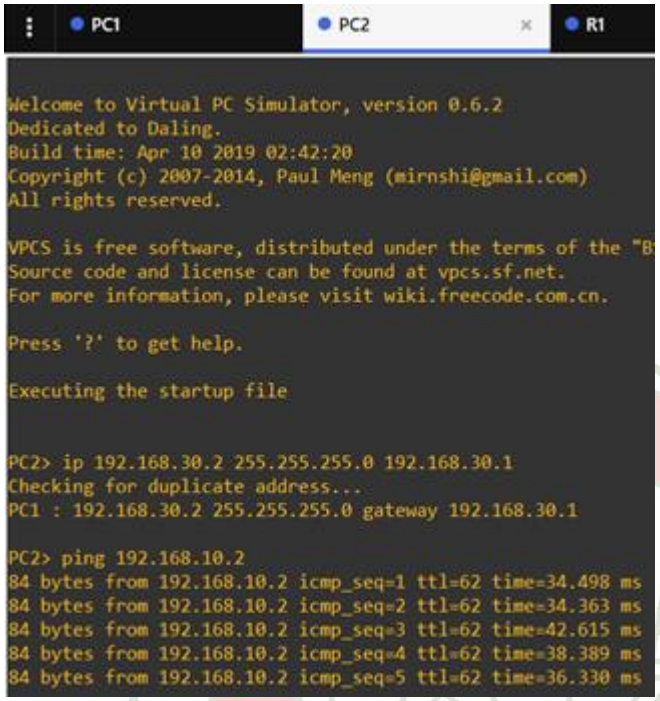


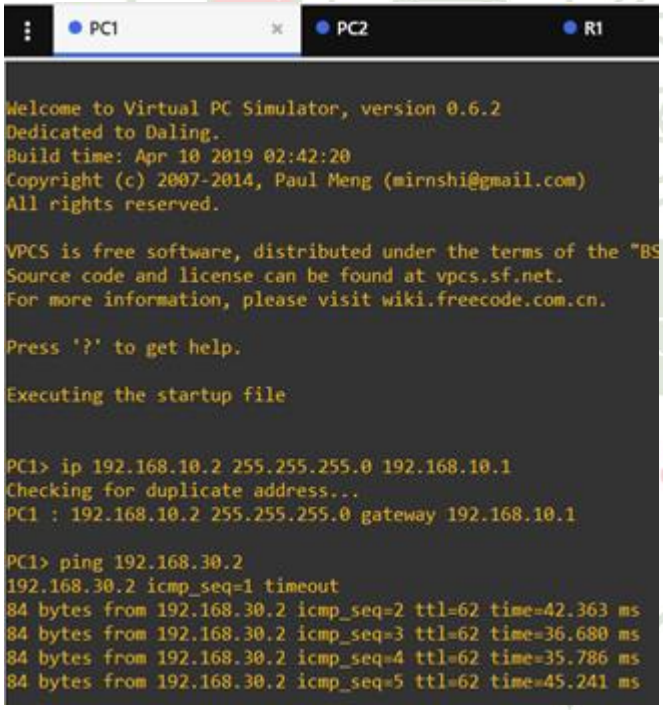


Configuring Routers:



Checking connection:





RESULT: After the configuration and connection of all devices, the ping is successful between PCs

EXPERIMENT-12

AIM: Illustrate TCPDUMP command

DESCRIPTION:

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

COMMANDS:

Installing tcpdump tool in Linux

For RedHat based linux OS

yum install tcpdump

For Ubuntu/Debian OS

apt install tcpdump

Working with tcpdump command:

1. To capture the packets of current network interface
   sudo tcpdump
   This will capture the packets from the current interface of the network through which the system is connected to the internet.

OUTPUT:

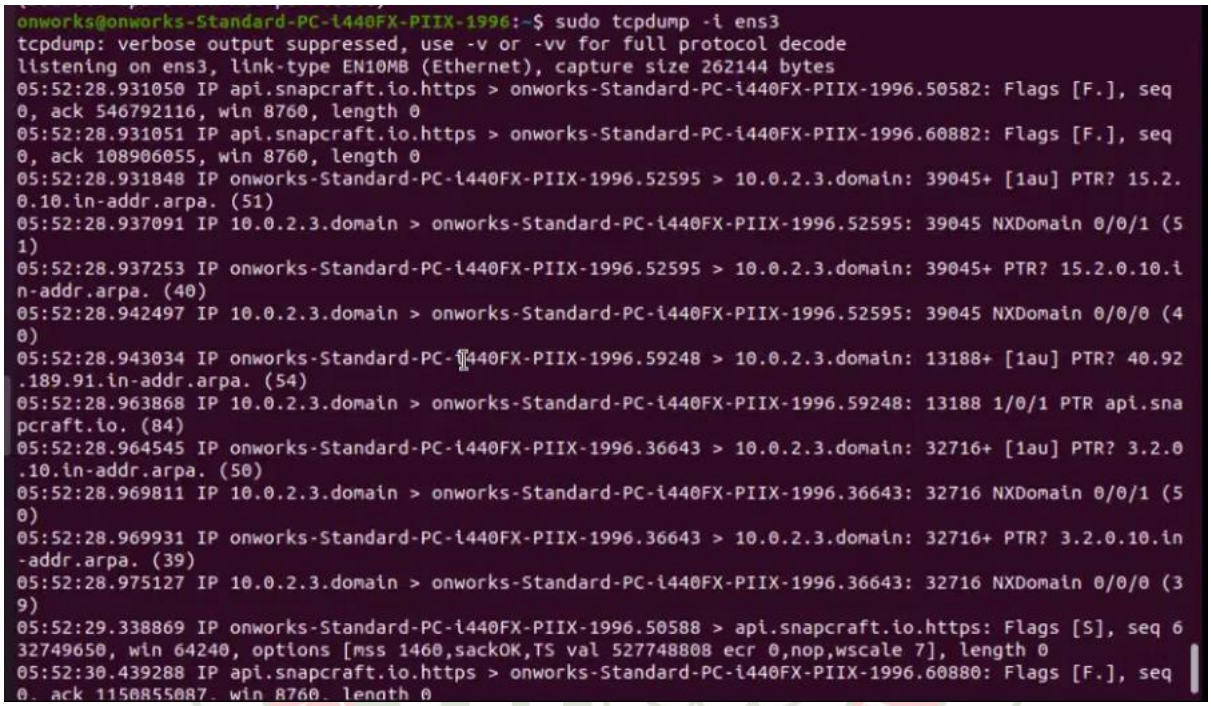
```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump
[sudo] password for onworks:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
05:48:14.000181 IP6 onworks-Standard-PC-i440FX-PIIX-1996.39452 > 2001:67c:1560:8003::c7.ntp: NTPv4, Clie
nt, length 48
05:48:14.003418 IP onworks-Standard-PC-i440FX-PIIX-1996.40401 > 10.0.2.3.domain: 17769+ [1au] PTR? 7.c.0
.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (101)
05:48:14.024113 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.40401: 17769 NXDomain 0/1/1 (1
65)
05:48:14.024254 IP onworks-Standard-PC-i440FX-PIIX-1996.40401 > 10.0.2.3.domain: 17769+ PTR? 7.c.0.0.0.0
.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (90)
05:48:14.043893 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.40401: 17769 NXDomain 0/1/0 (1
54)
05:48:14.044492 IP onworks-Standard-PC-i440FX-PIIX-1996.38770 > 10.0.2.3.domain: 48851+ [1au] PTR? f.9.f
.e.7.b.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa. (101)
05:48:14.050374 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.38770: 48851 NXDomain 0/1/1 (1
65)
05:48:14.050442 IP onworks-Standard-PC-i440FX-PIIX-1996.38770 > 10.0.2.3.domain: 48851+ PTR? f.9.f.e.7.b
.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa. (90)
05:48:14.056105 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.38770: 48851 NXDomain 0/1/0 (1
54)
05:48:14.057724 IP onworks-Standard-PC-i440FX-PIIX-1996.51120 > 10.0.2.3.domain: 44979+ [1au] PTR? 3.2.0
.10.in-addr.arpa. (50)
05:48:14.062638 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.51120: 44979 NXDomain 0/0/1 (5
0)
05:48:14.062690 IP onworks-Standard-PC-i440FX-PIIX-1996.51120 > 10.0.2.3.domain: 44979+ PTR? 3.2.0.10.in
-addr.arpa. (39)
05:48:14.067810 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.51120: 44979 NXDomain 0/0/0 (3
9)
05:48:14.068863 IP onworks-Standard-PC-i440FX-PIIX-1996.44277 > 10.0.2.3.domain: 27335+ [1au] PTR? 15.2.
0.10.in-addr.arpa. (51)
05:48:14.074037 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.44277: 27335 NXDomain 0/0/1 (5
1)
05:48:14.074090 IP onworks-Standard-PC-i440FX-PIIX-1996.44277 > 10.0.2.3.domain: 27335+ PTR? 15.2.0.10.i
n-addr.arpa. (40)
05:48:14.079237 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.44277: 27335 NXDomain 0/0/0 (4
0)
05:48:19.255857 ARP, Request who-has 10.0.2.3 tell onworks-Standard-PC-i440FX-PIIX-1996, length 28
```

2. To capture packets from a specific network interface

sudo tcpdump -i wlo1

This command will now capture the packets from wlo1 network interface.

Output:

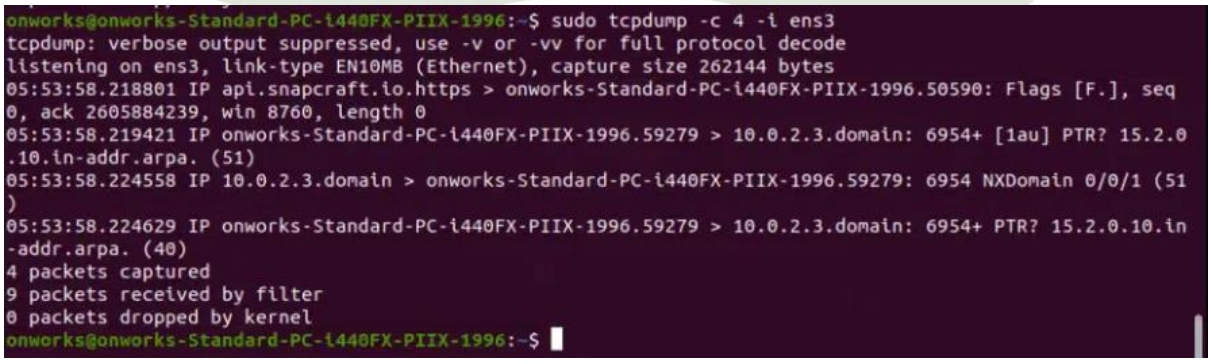


3. To capture specific number of packets

sudo tcpdump -c 4 -i wlo1

This command will capture only 4 packets from the wlo1 interface.

OUTPUT



4. To print captured packets in ASCII format

sudo tcpdump -A -i wlo1

This command will now print the captured packets from wlo1 to ASCII value.

OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -A -i ens3
[sudo] password for onworks:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:04:43.000266 IP6 onworks-Standard-PC-i440FX-PIIX-1996.34021 > 2001:67c:1560:8003::c7.ntp: NTPv4, Clie
nt, length 48
`....8.@.....8... ..|.`.....{.8j.#......"k....
06:04:43.004188 IP onworks-Standard-PC-i440FX-PIIX-1996.37210 > 10.0.2.3.domain: 60980+ [1au] PTR? 7.c.0
.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (101)
E...J.@.@..;
...
....Z.5.m...4..........7.c.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa.......)
........
06:04:43.329876 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.37210: 60980 NXDomain 0/1/1 (1
65)
E.......@.\~
...
....5.Z..fa.4..........7.c.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa......4.
......+.4.ns1   canonical.com.
hostmaster.jx.....*0.....       :.......).........
06:04:43.330060 IP onworks-Standard-PC-i440FX-PIIX-1996.37210 > 10.0.2.3.domain: 60980+ PTR? 7.c.0.0.0.0
.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (90)
E..vJZ@.@...
...
....Z.5.b...4..........7.c.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa.....
06:04:43.335832 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.37210: 60980 NXDomain 0/1/0 (1
54)
E.......@.\.
...
....5.Z...z.4..........7.c.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa......4.
......+.4.ns1   canonical.com.
hostmaster.jx.....*0.....       :.....
06:04:43.338905 IP onworks-Standard-PC-i440FX-PIIX-1996.54857 > 10.0.2.3.domain: 2900+ [1au] PTR? f.9.f.
e.7.b.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa. (101)
E...J\@.@...
...
....I.5.m...T..........f.9.f.e.7.b.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa.......)
........
06:04:43.344822 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.54857: 2900 NXDomain 0/1/1 (16
```

5. To display all available interfaces

sudo tcpdump -D

This command will display all the interfaces that are available in the system.

OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -D
1.ens3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

6. To display packets in HEX and ASCII values
sudo tcpdump -XX -i wlo1
This command will now print the packets captured from the wlo1 interface in the HEX and ASCII values.
OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -XX -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:06:08.998046 IP onworks-Standard-PC-i440FX-PIIX-1996.60890 > api.snapcraft.io.https: Flags [S], seq 5
18894480, win 64240, options [mss 1460,sackOK,TS val 924234676 ecr 0,nop,wscale 7], length 0
        0x0000:  5255 0a00 0202 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  003c dba1 4000 4006 9b3b 0a00 020f 5bbd  .<..@.@..;....[.
        0x0020:  5c13 edda 01bb 1eed b390 0000 0000 a002  \...............
        0x0030:  faf0 c40d 0000 0204 05b4 0402 080a 3716  ..............7.
        0x0040:  b3b4 0000 0000 0103 0307                 ..........
06:06:08.998122 IP onworks-Standard-PC-i440FX-PIIX-1996.60888 > api.snapcraft.io.https: Flags [S], seq 2
244248178, win 64240, options [mss 1460,sackOK,TS val 924234676 ecr 0,nop,wscale 7], length 0
        0x0000:  5255 0a00 0202 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  003c 8f47 4000 4006 e795 0a00 020f 5bbd  .<.G@.@.......[.
        0x0020:  5c13 edd8 01bb 85c4 8272 0000 0000 a002  \........r......
        0x0030:  faf0 c40d 0000 0204 05b4 0402 080a 3716  ..............7.
        0x0040:  b3b4 0000 0000 0103 0307                 ..........
06:06:08.998784 IP onworks-Standard-PC-i440FX-PIIX-1996.56572 > 10.0.2.3.domain: 17108+ [1au] PTR? 19.92
.189.91.in-addr.arpa. (54)
        0x0000:  5255 0a00 0203 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  0052 827d 4000 4011 a00c 0a00 020f 0a00  .R.}@.@.........
        0x0020:  0203 dcfc 0035 003e 1861 42d4 0100 0001  .....5.>.aB.....
        0x0030:  0000 0000 0001 0231 3902 3932 0331 3839  .......19.92.189
        0x0040:  0239 3107 696e 2d61 6464 7204 6172 7061  .91.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......)........
06:06:09.329377 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.56572: 17108 1/0/1 PTR api.sna
pcraft.io. (84)
        0x0000:  5254 0012 3456 5255 0a00 0202 0800 4500  RT..4VRU......E.
        0x0010:  0070 57e2 0000 4011 0a8a 0a00 0203 0a00  .pW...@.........
        0x0020:  020f 0035 dcfc 005c 96e1 42d4 8180 0001  ...5...\..B.....
        0x0030:  0001 0000 0001 0231 3902 3932 0331 3839  .......19.92.189
        0x0040:  0239 3107 696e 2d61 6464 7204 6172 7061  .91.in-addr.arpa
        0x0050:  0000 0c00 01c0 0c00 0c00 0100 000e 1000  ................
```

7. To save captured packets into a file
sudo tcpdump -w captured_packets.pcap -i wlo1

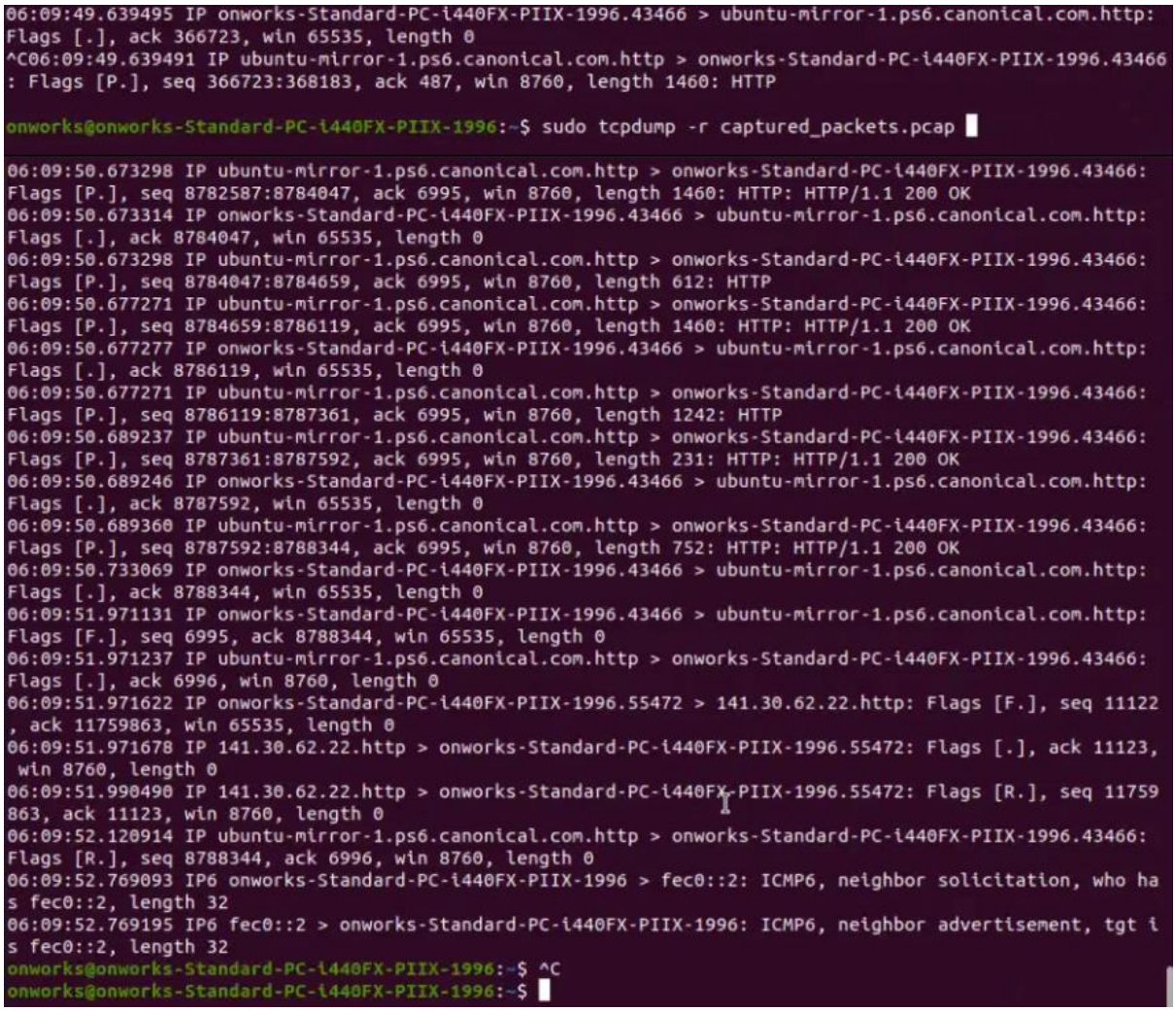
This command will now output all the captures packets in a file named as captured_packets.pcap.
OUTPUT

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -w captured_packets.pcap -i ens3
[sudo] password for onworks:
tcpdump: listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6945 packets captured
6945 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

8. To read captured packets from a file
sudo tcpdump -r captured_packets.pcap

This command will now read the captured packets from the captured_packets.pcap file.

OUTPUT



9. To capture packets with ip address
sudo tcpdump -n -i wlo1

This command will now capture the packets with IP addresses.
OUTPUT

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -n -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:13:49.830711 IP 10.0.2.15.50648 > 91.189.92.40.443: Flags [S], seq 2473722447, win 64240, options [ms
s 1460,sackOK,TS val 527781608 ecr 0,nop,wscale 7], length 0
06:13:49.830770 IP 10.0.2.15.50646 > 91.189.92.40.443: Flags [S], seq 4139998373, win 64240, options [ms
s 1460,sackOK,TS val 527781608 ecr 0,nop,wscale 7], length 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50646: Flags [F.], seq 0, ack 4139998374, win 8192, leng
th 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50638: Flags [F.], seq 0, ack 478652487, win 8760, lengt
h 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50630: Flags [F.], seq 0, ack 3530249906, win 8760, leng
th 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50628: Flags [F.], seq 0, ack 3627054957, win 8760, leng
th 0
06:13:51.944216 IP 91.189.92.40.443 > 10.0.2.15.50626: Flags [F.], seq 0, ack 816105158, win 8760, lengt
h 0
06:13:51.944216 IP 91.189.92.40.443 > 10.0.2.15.50624: Flags [F.], seq 0, ack 3202938958, win 8760, leng
th 0
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

10. To capture only TCP packets
sudo tcpdump -i wlo1 tcp

This command will now capture only TCP packets from wlo1.
OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -i ens3 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:14:24.384720 IP onworks-Standard-PC-i440FX-PIIX-1996.50650 > api.snapcraft.io.https: Flags [S], seq 1
615645445, win 64240, options [mss 1460,sackOK,TS val 527816168 ecr 0,nop,wscale 7], length 0
06:14:24.500819 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50636: Flags [F.], seq
0, ack 2567671397, win 8760, length 0
06:14:24.500820 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50634: Flags [F.], seq
0, ack 3404788314, win 8760, length 0
06:14:24.871697 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50640: Flags [F.], seq
0, ack 3663748440, win 8760, length 0
06:14:25.880965 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50650: Flags [F.], seq
0, ack 1615645446, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50638: Flags [F.], seq
0, ack 478652487, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50630: Flags [F.], seq
0, ack 3530249906, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50628: Flags [F.], seq
0, ack 3627054957, win 8760, length 0
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

CONCLUSION: The tcpdump command is studied and analysed