Experiment No: 1a

Client-Server Network Topology using Cisco packet tracer

Name : Ujjawal Sharma
Reg. No : 19BLC1016
Faculty Name : Dr. Kalaivanan N

Aim:

a. To set up Client-Server Network Topology using Cisco packet tracer
b. To Analyze the Network behavior in both Simulation Mode and Real Time Mode
c. To set up HTTP, DNS services and analyze the network behavior

Tool Required:

Cisco Packet Tracer

Theory:

CISCO PACKET TRACER:

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

Features:

- **Packet Tracer Workspaces:** Cisco Packet Tracer has two workspaces—logical and physical. The logical workspace allows users to build logical network topologies by placing, connecting, and clustering virtual network devices. The physical workspace provides a graphical physical dimension of the logical network, giving a sense of scale and placement in how network devices such as routers, switches, and hosts would look in a real environment. The physical view also provides geographic representations of networks, including multiple cities, buildings, and wiring closets.

- **Packet Tracer Modes:** Cisco Packet Tracer provides two operating modes to visualize the behavior of a network—real-time mode and simulation mode. In real-time mode the network behaves as real devices do, with immediate real-time response for all network activities. The real-time mode gives students a viable alternative to real equipment and allows them to gain configuration practice before working with real equipment. In simulation mode the user can see and control time intervals, the inner workings of data transfer, and the propagation of data across a network. This helps students understand the fundamental

concepts behind network operations. A solid understanding of network fundamentals can help accelerate learning about related concepts.

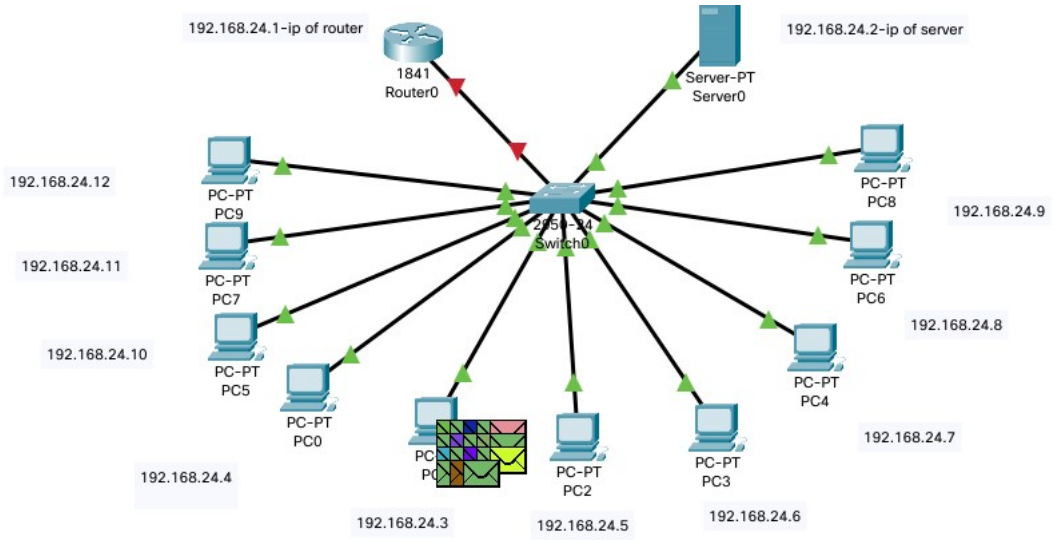
- **Activity Wizard:** The Activity Wizard allows users to author their own learning activities by setting up scenarios using instructional text, and creating initial and final network topologies and predefined packets. The Activity Wizard also includes grading and feedback capabilities.

PROCEDURE:

1. In the Devices section go to End Devices and select PC's
2. In the Devices section go to Networks and select Server, Router and Switch.
3. Connect all the devices using Fast Ethernet Cable
4. Assign Ipv4 address to all the PC's and provide their gateway as the ipv4 address of Router and DNS as the ipv4 of the server.
5. After the connections have been made click on any of the PC and in the desktop bar go to the command prompt section and ping all other devices.
6. In the Simulation mode assign packets to any one PC and deliver it to some other PC. Click on Simulation to get the trace. Check the Simulation panel for successful simulations
7. Select any PC and go to the Programming section. In it select HTTP JAVASCRIPT as file type and in the URL mention "http://www.vit.ac.in" and write an index.html file accordingly. Now in any of the PC'S run www.vit.ac.in. The output screen would have details as programmed by you in the index.html file.

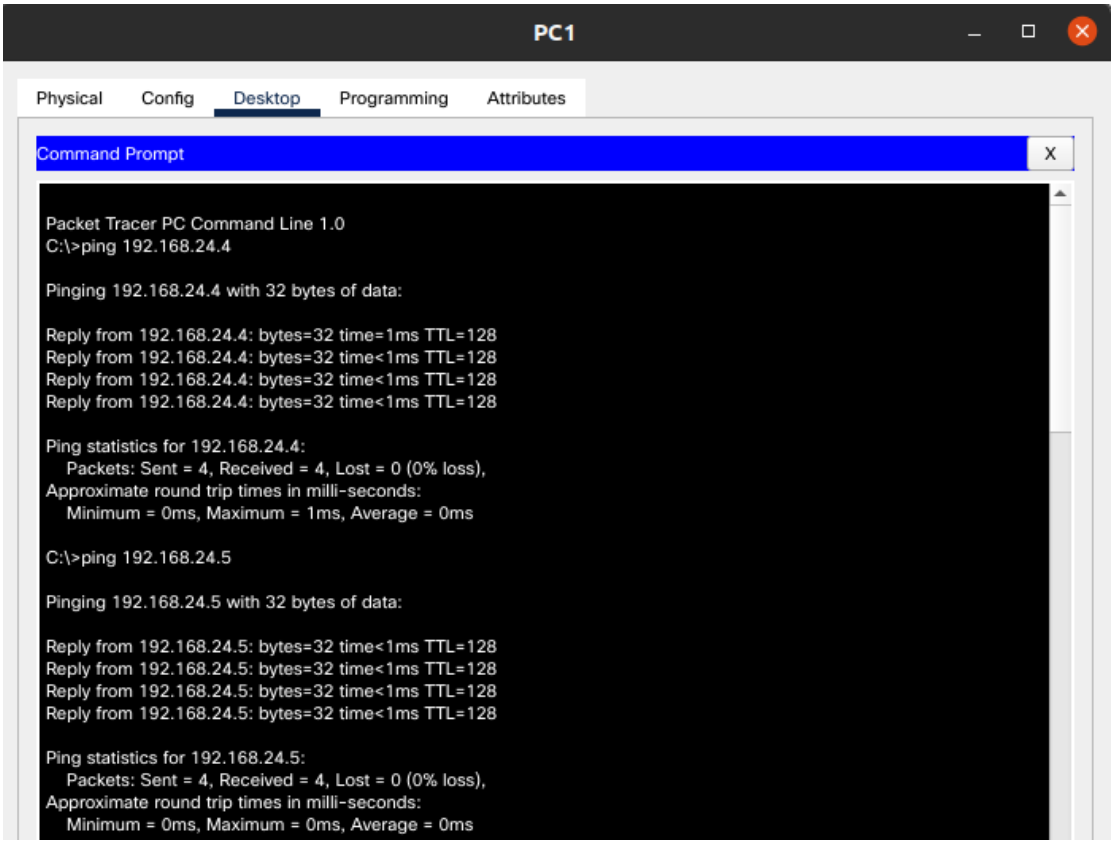
EXERCISE:

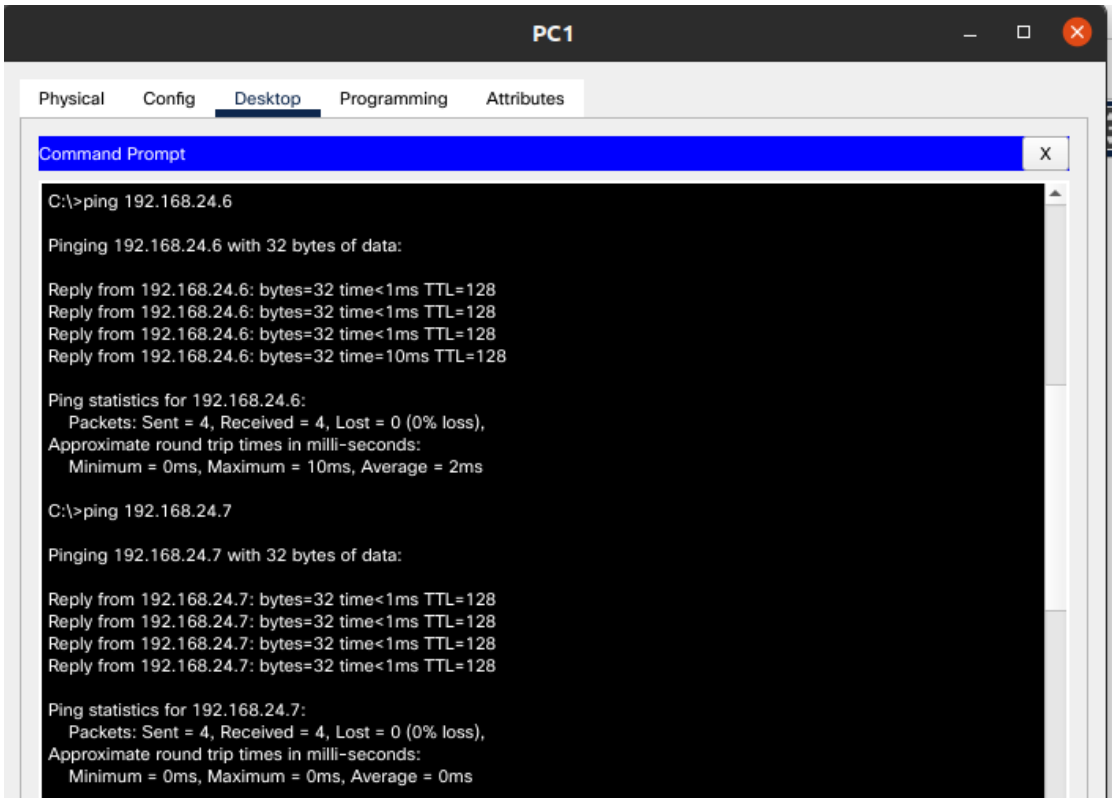
a) **Build a Local Area Network with at least 10 clients, 1 switch and a server using star topology**

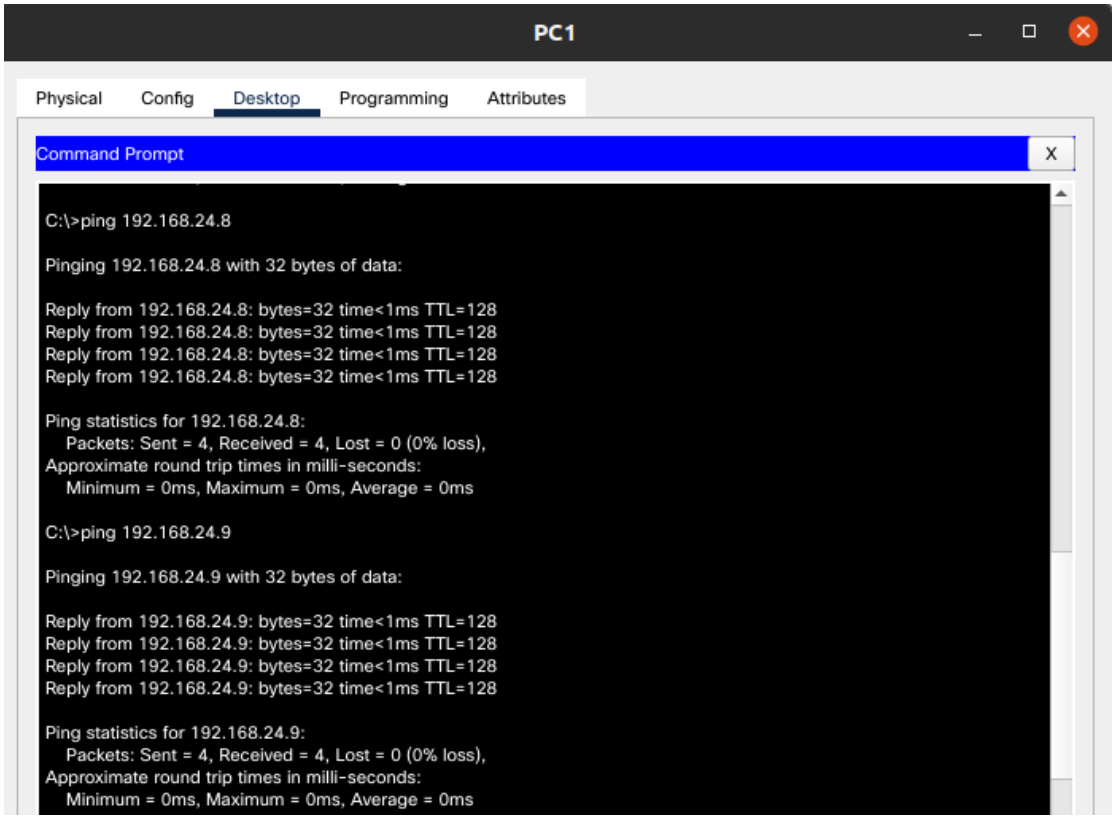


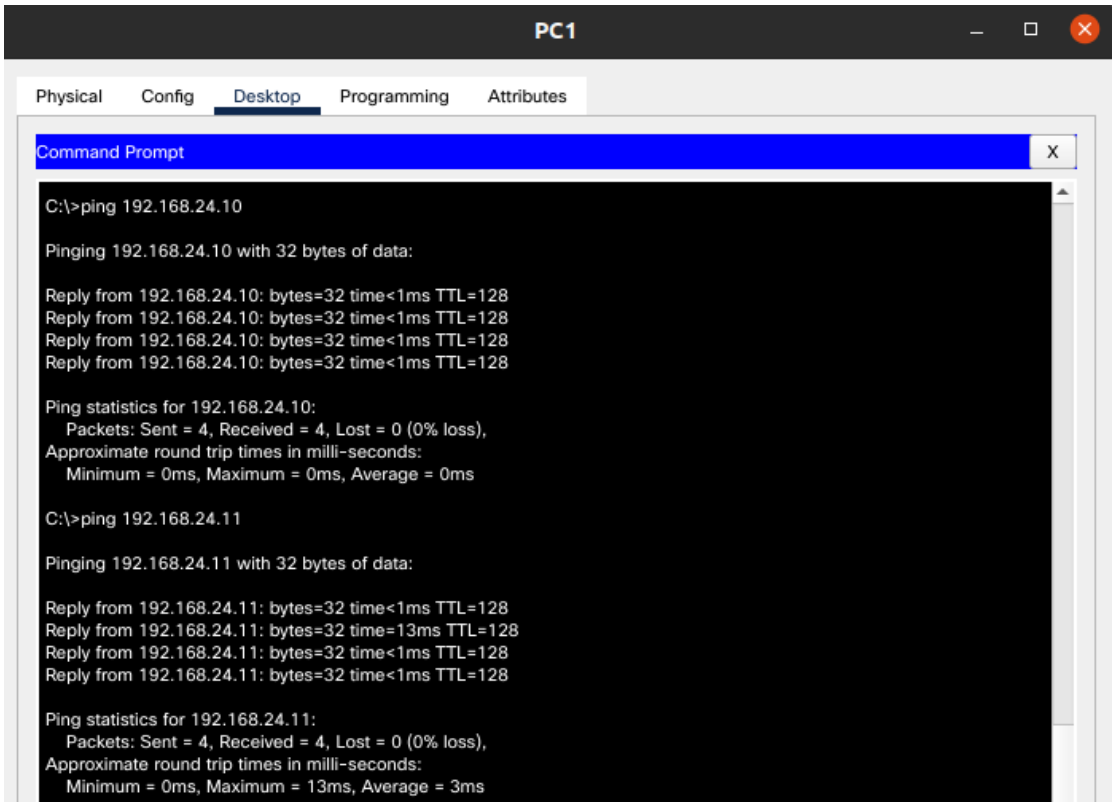
b) Configure the entire network and verify the connection between all clients and server

Pinging all devices from PC1:




PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.24.6
Pinging 192.168.24.6 with 32 bytes of data:
Reply from 192.168.24.6: bytes=32 time<1ms TTL=128
Reply from 192.168.24.6: bytes=32 time<1ms TTL=128
Reply from 192.168.24.6: bytes=32 time<1ms TTL=128
Reply from 192.168.24.6: bytes=32 time=10ms TTL=128
Ping statistics for 192.168.24.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>ping 192.168.24.7
Pinging 192.168.24.7 with 32 bytes of data:
Reply from 192.168.24.7: bytes=32 time<1ms TTL=128
Reply from 192.168.24.7: bytes=32 time<1ms TTL=128
Reply from 192.168.24.7: bytes=32 time<1ms TTL=128
Reply from 192.168.24.7: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.24.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

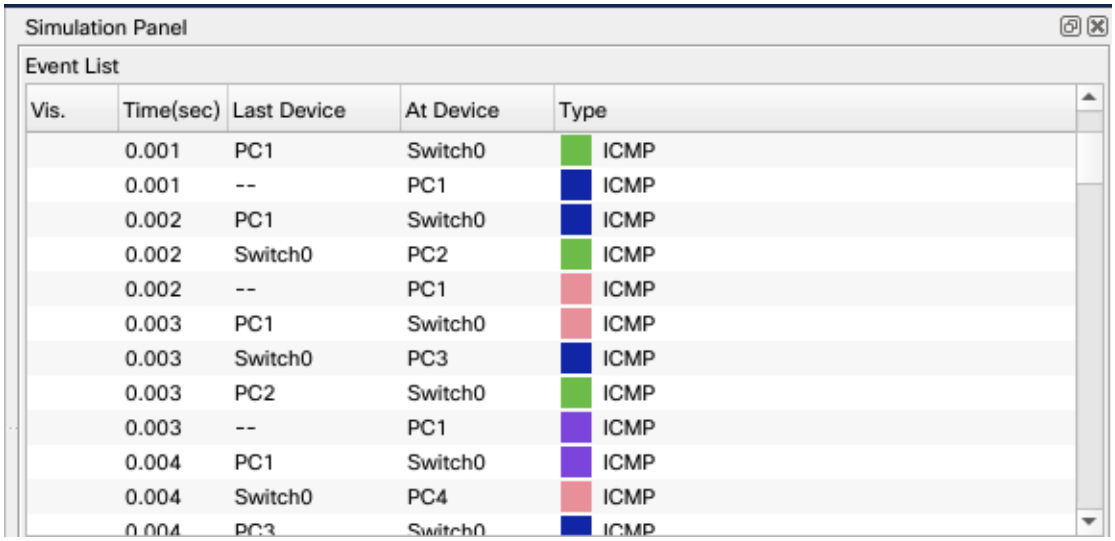

PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.24.8
Pinging 192.168.24.8 with 32 bytes of data:
Reply from 192.168.24.8: bytes=32 time<1ms TTL=128
Reply from 192.168.24.8: bytes=32 time<1ms TTL=128
Reply from 192.168.24.8: bytes=32 time<1ms TTL=128
Reply from 192.168.24.8: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.24.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.24.9
Pinging 192.168.24.9 with 32 bytes of data:
Reply from 192.168.24.9: bytes=32 time<1ms TTL=128
Reply from 192.168.24.9: bytes=32 time<1ms TTL=128
Reply from 192.168.24.9: bytes=32 time<1ms TTL=128
Reply from 192.168.24.9: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.24.9:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms



c) Analyze the network behaviour in simulation mode

Sending packets to all the devices from PC1

EVENT LIST:



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.004	PC3	Switch0	ICMP
	0.004	Switch0	PC1	ICMP
	0.004	--	PC1	ICMP
	0.005	PC1	Switch0	ICMP
	0.005	Switch0	PC6	ICMP
	0.005	PC4	Switch0	ICMP
	0.005	Switch0	PC1	ICMP
	0.005	--	PC1	ICMP
	0.006	PC1	Switch0	ICMP
	0.006	Switch0	PC8	ICMP
	0.006	PC6	Switch0	ICMP
	0.006	Switch0	PC1	ICMP

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.006	Switch0	PC8	ICMP
	0.006	PC6	Switch0	ICMP
	0.006	Switch0	PC1	ICMP
	0.006	--	PC1	ICMP
	0.007	PC1	Switch0	ICMP
	0.007	Switch0	PC0	ICMP
	0.007	PC8	Switch0	ICMP
	0.007	Switch0	PC1	ICMP
	0.007	--	PC1	ICMP
	0.008	PC1	Switch0	ICMP
	0.008	Switch0	PC5	ICMP
	0.008	PC0	Switch0	ICMP

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.008	PC0	Switch0	ICMP
	0.008	Switch0	PC1	ICMP
	0.008	--	PC1	ICMP
	0.009	PC1	Switch0	ICMP
	0.009	Switch0	PC7	ICMP
	0.009	PC5	Switch0	ICMP
	0.009	Switch0	PC1	ICMP
	0.010	Switch0	PC9	ICMP
	0.010	PC7	Switch0	ICMP
	0.010	Switch0	PC1	ICMP
	0.011	PC9	Switch0	ICMP
	0.011	Switch0	PC1	ICMP

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.009	Switch0	PC1	ICMP
	0.010	Switch0	PC9	ICMP
	0.010	PC7	Switch0	ICMP
	0.010	Switch0	PC1	ICMP
	0.011	PC9	Switch0	ICMP
	0.011	Switch0	PC1	ICMP

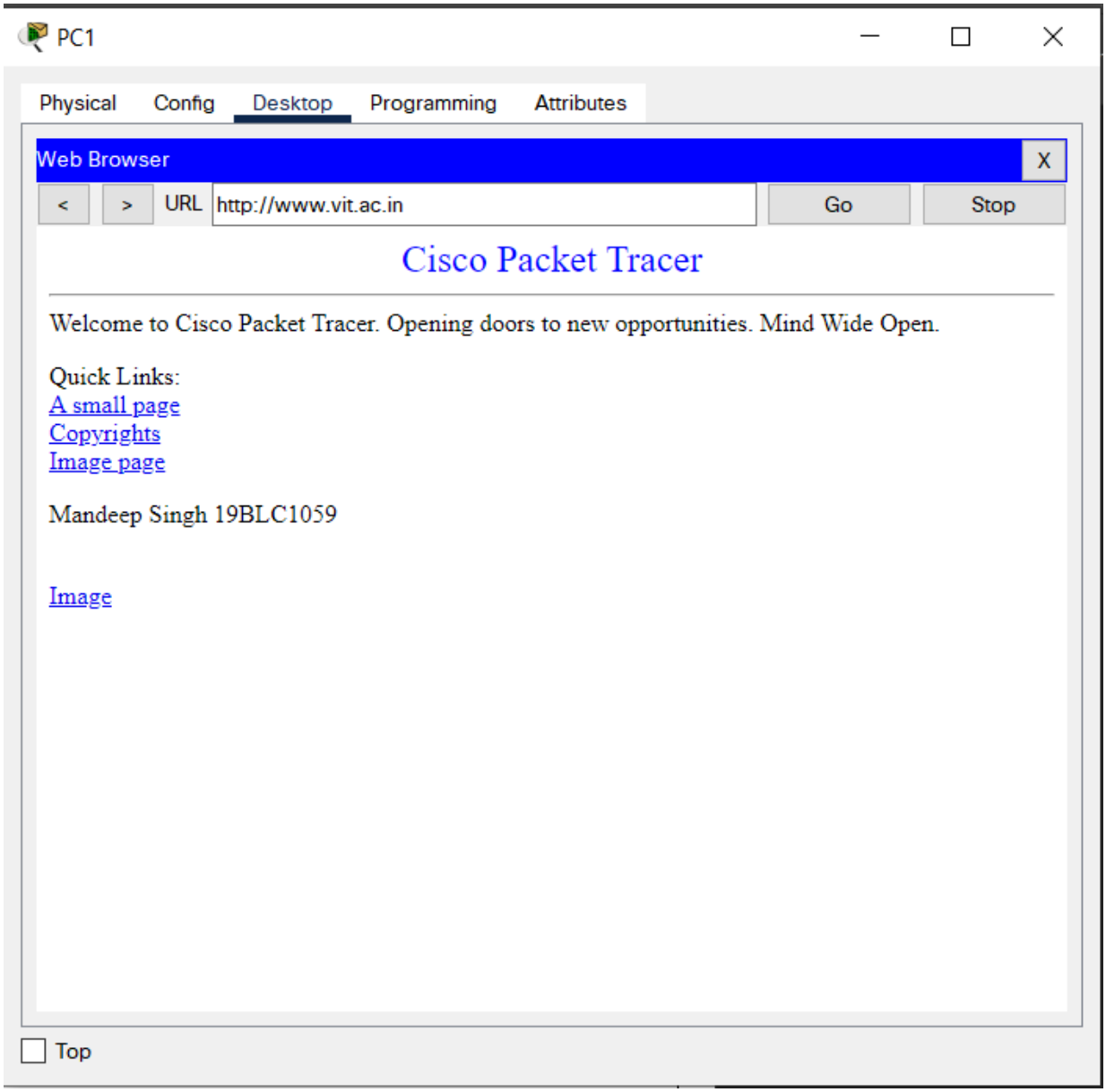
STATUS:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC1	PC2	IC...		0.000	N
	Successful	PC1	PC3	IC...		0.000	N
	Successful	PC1	PC4	IC...		0.000	N

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC1	PC6	IC...		0.000	N
	Successful	PC1	PC8	IC...		0.000	N
	Successful	PC1	PC0	IC...		0.000	N

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC1	PC5	IC...		0.000	N
	Successful	PC1	PC7	IC...		0.000	N
	Successful	PC1	PC9	IC...		0.000	N

d) Configure the HTTP and DNS services in the server and analyse the network behaviour in real time mode



INFERENCES & RESULT

Setting up a LAN Network and transferring data packets through a server. The results were matching with the experiment requirements.

Experiment No: 1b

Study of Basic Networking Commands

Aim:

To study and understand the basic networking commands.

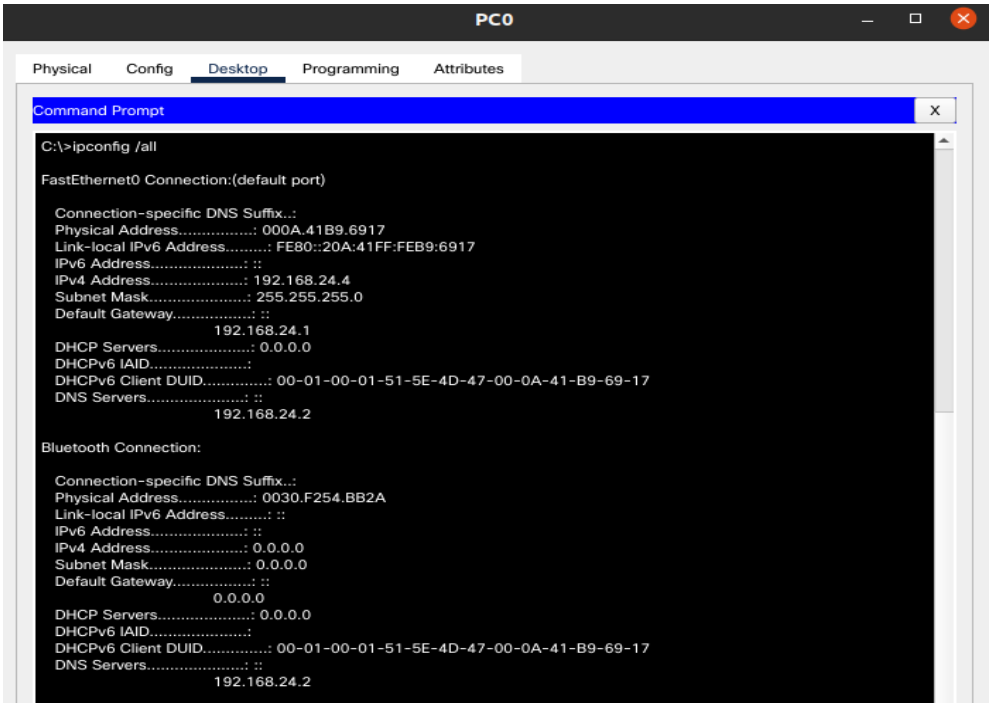
Theory:

A computer network consists of several computers connected together. The network can be as simple as a few computers connected in your home or office, or as complicated as a large university network or even the entire Internet. When your computer is part of a network, you have access to those systems either directly or through services like mail and the web.

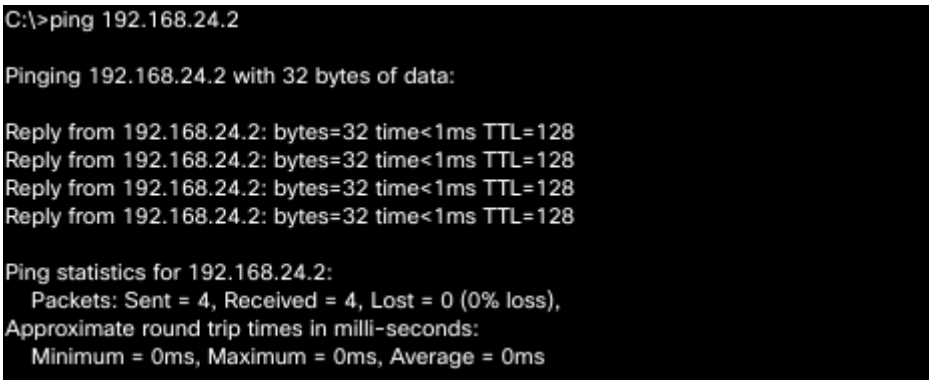
There are a variety of networking programs that you can use. Some are handy for performing diagnostics to see if everything is working properly. Others (like mail readers and web browsers) are useful for getting your work done and staying in contact with other people.

COMMANDS

- **ipconfig:**
  Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

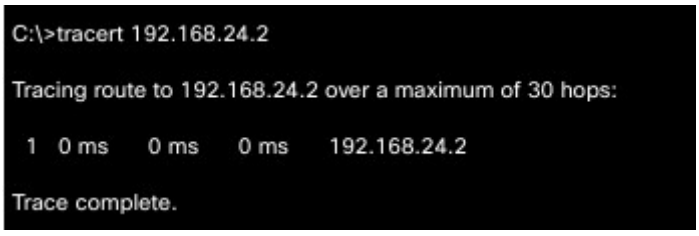


- **ping:**
  Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.



- **tracert:**

  This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.return an ICMP time Exceeded message to the source computer.

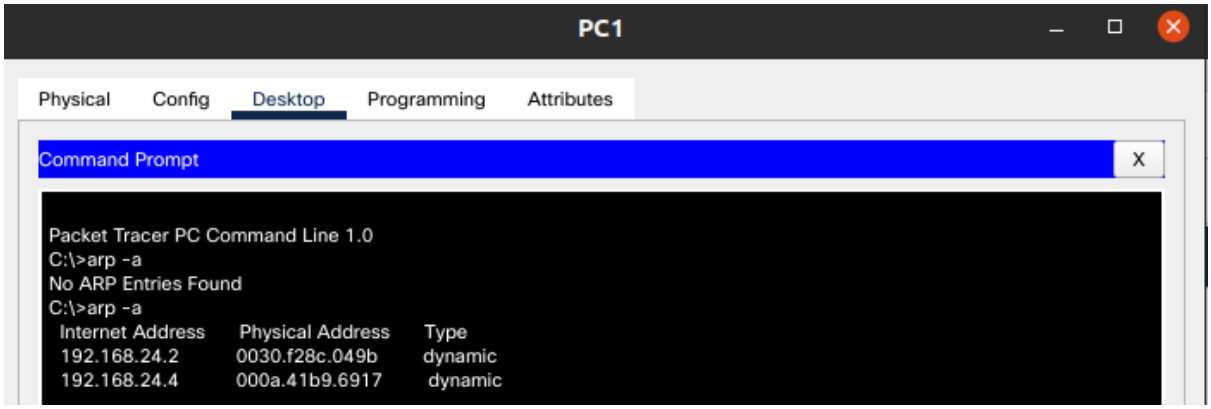


- **nslookup**

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.

- **Arp:**

  Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).



Result:

Thus a few basic networking commands are studied and practiced successfully.