Practical file submitted in partial fulfillment for the evaluation of

Computer Networks and Internet Protocol lab (AIDS256)

VIPS
योगः कर्मसु कौशलम्
IN PURSUIT OF PERFECTION

VIVEKANANDA SCHOOL OF ENGINEERING AND TECHNOLOGY

Submitted By:

Student Name: Harsh Sharma

Enrolment no: 03217711921

Branch & Section: AI & DS – A

Submitted to:

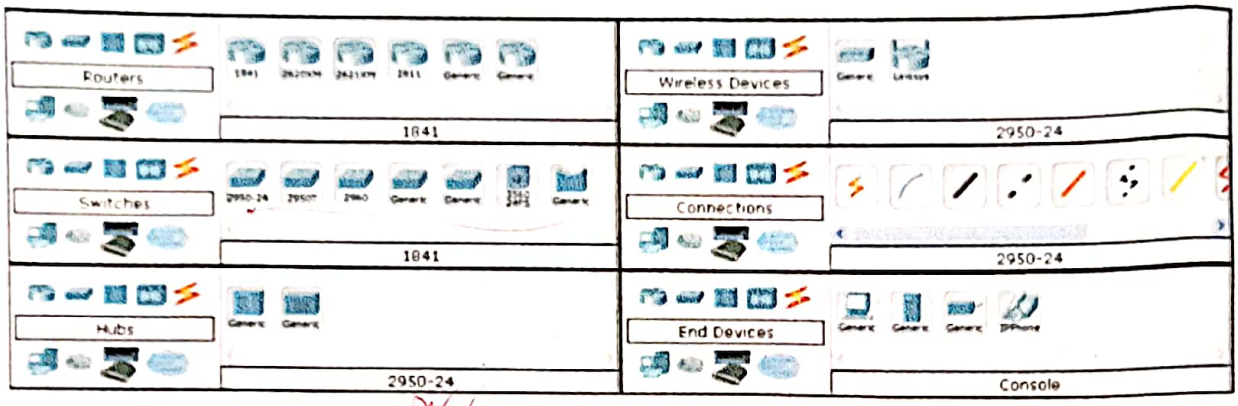
Dr. Praveen Chaurasia

Scanned with OKEN Scanner

Index

S.No	Experiment Title	Page No.	Date	Grade/ Evaluation	Sign
1	Introduction to Network Simulator packet tracer & establish a peer to peer network		9-3-23	A	
2	Running & using services commands related to networking		16-3-23	B+	
3(a)	To install & configure network devices (Hub, Switch) to create a LAN Network		23-3-23	B	
3(b)	To create a LAN network using a switch		23-3-23	B	
3(c)	To create a LAN network using a Hub.		23-3-23	B+	
4	Create Ring, Bus, Star & Mesh topology using Cisco Packet Tracer		6-4-23	B	
5	Explain various parameters of HTTP protocols.		13-4-23	A	
6	Analyzing various parameters for TCP protocol in action		20-4-23	B+	
7	Introduction to basic networking tools: Wireless & Network Miner		25-5-23	A	
8	Introduction to Datadog tool for data monitoring in network		1-6-23	B	

Scanned with OKEN Scanner



Peer to Peer Network

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : 1

Experiment No. 1

Aim :- Introduction to Network simulator - Packet Tracer & establish peer to peer Netwo

Objectives

- Introduction to packet Tracer interface
- To learn how to use different components & build a simple network.

Theory

Cisco Packet Tracer is a protocol simulator developed by Dennis Frezzo & his team at Cisco System. Cisco Packet Tracer is a powerful & dynamic tool that display the various protocols used in networking, in either real time or simulation mode.

Steps to install cisco packet tracer

To obtain & install cisco packet tracer, follow these steps.

1) Download the version of Packet Tracer you require
Packet Tracer 8.2.1 MacOS 64 bit.
Packet Tracer 8.2.1 Windows 64 bit.
2) Launch the Packet Tracer Install Program.
3) Lauch Cisco Packet Tracer by selecting the appropriate icon.
4) When prompted, click on Skills for all green button to authenticate.
5) Cisco Packet Tracer will launch & you are ready to explore its features.

Packet Tracer interface & how to create a topology

1) Start Packet Tracer & Enter into simulation mode.
2) Choose Devices & connections.
3) Building the topology - Adding the hosts in the following ways:
- Single Click on End devices.
- Single Click on generic host
- Move the cursor in the topology area. You will notice in turn into a '+' sig
4) Building Connections amongst devices - Connecting the hosts PCs to other

CLASSTIME

Scanned with OKEN Scanner

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::206:2AFF:FE12:C931
   IPv6 Address.....: ::
   IPv4 Address.....: 192.68.1.10
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.68.1.11

Pinging 192.68.1.11 with 32 bytes of data:

Reply from 192.68.1.11: bytes=32 time<1ms TTL=128
Reply from 192.68.1.11: bytes=32 time<1ms TTL=128
Reply from 192.68.1.11: bytes=32 time<1ms TTL=128
Reply from 192.68.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.68.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:21FF:FEB7:B191
   IPv6 Address.....: ::
   IPv4 Address.....: 192.68.1.11
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.68.1.10

Pinging 192.68.1.10 with 32 bytes of data:

Reply from 192.68.1.10: bytes=32 time<1ms TTL=128
Reply from 192.68.1.10: bytes=32 time<1ms TTL=128
Reply from 192.68.1.10: bytes=32 time<1ms TTL=128
Reply from 192.68.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.68.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

devices.

- Click once on copper Straight-through cable when connecting different devices types.
- Click once on copper Cross-over cable when connecting with devices with similar types.

5) Configuring IP Address & Subnet Masks on hosts

- Click once on PC0
- Choose the config tab.
- Click on fast Ethernet.
- Enter IP address & Subnet Masks.

Exercises.

1) Design a peer to peer network by establishing a connection b/w two PCs

2) Assign IP address to them as mentioned.

Host	IP Address	Subnet Masks
PC0	192.68.1.10	255.255.255.0
PC1	192.68.1.11	255.255.255.0

3) Observe the flow of data from host to host by creating network traffic.

4) Use commands such as ipconfig, ncconfig, ping to check their function & output on CPT - command prompt.

CLASSTIME

Scanned with OKEN Scanner

```
nging google.com [2404:6800:4002:82d::200e] with 32 bytes of data:
ply from 2404:6800:4002:82d::200e: time=7ms
ply from 2404:6800:4002:82d::200e: time=10ms
ply from 2404:6800:4002:82d::200e: time=9ms
ply from 2404:6800:4002:82d::200e: time=10ms

ng statistics for 2404:6800:4002:82d::200e:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
  Minimum = 7ms, Maximum = 10ms, Average = 9ms
```

```
Tracing route to google.com [2404:6800:4002:82d::200e]
over a maximum of 30 hops:

  1    3 ms     3 ms     2 ms  2405:201:4008:7181:8ea3:99ff:fe3f:e6a9
  2     *        *        *    Request timed out.
  3    7 ms     7 ms     8 ms  2405:200:801:300::71
  4     *        *        *    Request timed out.
  5    7 ms     8 ms     8 ms  2001:4860:1:1::1ea2
  6  757 ms   710 ms   614 ms  2404:6800:8011::1
  7    8 ms     7 ms     8 ms  2001:4860:0:1::5e46
  8     *        *        *    Request timed out.
  9    9 ms     7 ms     7 ms  2001:4860:0:1a::1
 10    8 ms     6 ms     7 ms  2001:4860:0:1::5e63
 11    9 ms     7 ms     7 ms  del11s22-in-x0e.1e100.net [2404:6800:4002:82d::200e]

Trace complete.
```

```
racing route to google.com [2404:6800:4002:82d::200e]
ver a maximum of 30 hops:
 0  DESKTOP-DUDQHO9 [2405:201:4008:7181:dc87:11be:46c:d9f5]
 1  2405:201:4008:7181:8ea3:99ff:fe3f:e6a9
 2     *        *        *
mputing statistics for 25 seconds...
            Source to Here   This Node/Link
op  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
 0                                          DESKTOP-DUDQHO9 [2405:201:4008:7181:dc87:11be:46c:d9f5]
                                 0/ 100 =  0%   |
 1    3ms     0/ 100 =  0%     0/ 100 =  0%  2405:201:4008:7181:8ea3:99ff:fe3f:e6a9

race complete.
```

```
Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:201:4008:7181:f130:2ac8:f85e:d4bf
   Temporary IPv6 Address. . . . . . : 2405:201:4008:7181:dc87:11be:46c:d9f5
   Link-local IPv6 Address . . . . . : fe80::a9a4:8b2c:671a:e18b%2
   IPv4 Address. . . . . . . . . . . : 192.168.29.49
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8ea3:99ff:fe3f:e6a9%2
                                       192.168.29.1
```

```
Physical Address    Transport Name
=================== ============================================================
C-C1-0C-B3-91-0B    \Device\Tcpip_{02074E48-AB60-4773-BD57-299B8E83C310}
```

```
Server:  reliance.reliance
Address:  192.168.29.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:82d::200e
          142.250.206.174
```

```
xamples:

  > route PRINT
  > route PRINT -4
  > route PRINT -6
  > route PRINT 157*                .... Only prints those matching 157*

  > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
        destination^      ^mask      ^gateway     metric^    ^
                                                    Interface^
    If IF is not given, it tries to find the best interface for a given
    gateway.
  > route ADD 3ffe::/32 3ffe::1

  > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

    CHANGE is used to modify gateway and/or metric only.

  > route DELETE 157.0.0.0
  > route DELETE 3ffe::/32
```

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No : .....

Experiment NO. 2

Running and using Services / Commands related to networking.

Commands :

1) Ping : It is a command prompt command used to test the ability of the source computer to reach a specific destination computer.

2) Traceroute : It is command which shows the path a packet of information taken from one computer to another. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. It will tell how long each 'hop' from router to router takes.

3) Path Ping : It is a route tracing tool that combines features of Ping & Tracert with additional information that neither of those tools provides. It sends packet to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop.

4) Ipconfig : Displays all current TCP/IP network configuration values & refreshes Dynamic host configuration Protocol & Domain Name System settings. Used without parameters, Ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

5) Getmac : Used to get the mac addresses.

6) ARP : It stands for Address Resolution Protocol. Network nodes use this protocol to match IP address to MAC Addresses. ARP is used to view & modify the ARP tables entries on the local computer.

7) Nslookup : Query a DNS domain nameservers to lookup & find IP address information of computers in the internet. Convert a host or domain name into an IP address.

CLASSTIME

Scanned with OKEN Scanner

```
isplays and modifies the IP-to-Physical address translation tables used by
ddress resolution protocol (ARP).

RP -s inet_addr eth_addr [if_addr]
RP -d inet_addr [if_addr]
RP -a [inet_addr] [-N if_addr] [-v]

 -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.
 -v            Displays current ARP entries in verbose mode.  All invalid
               entries and entries on the loop-back interface will be shown.
 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. inet_addr may be
               wildcarded with * to delete all hosts.
 -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.
xample:
 > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
 > arp -a                                    .... Displays the arp table.
```

```
anipulates network routing tables.

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

 -f               Clears the routing tables of all gateway entries.  If this is
                  used in conjunction with one of the commands, the tables are
                  cleared prior to running the command.

 -p               When used with the ADD command, makes a route persistent across
                  boots of the system. By default, routes are not preserved
                  when the system is restarted. Ignored for all other commands,
                  which always affect the appropriate persistent routes.

 -4               Force using IPv4.

 -6               Force using IPv6.

 command          One of these:
                    PRINT     Prints a route
                    ADD       Adds a route
                    DELETE    Deletes a route
                    CHANGE    Modifies an existing route
 destination      Specifies the host.
 MASK             Specifies that the next parameter is the 'netmask' value.
 netmask          Specifies a subnet mask value for this route entry.
                  If not specified, it defaults to 255.255.255.255.
 gateway          Specifies gateway.
 interface        the interface number for the specified route.
 METRIC           specifies the metric, ie. cost for the destination.

ll symbolic names used for destination are looked up in the network database
ile NETWORKS. The symbolic names for gateway are looked up in the host name
atabase file HOSTS.

f the command is PRINT or DELETE. Destination or gateway can be a wildcard,
wildcard is specified as a star '*'), or the gateway argument may be omitted.

f Dest contains a * or ?, it is treated as a shell pattern, and only
atching destination routes are printed. The '*' matches any string,
nd '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

attern match is only allowed in PRINT command.
iagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

xamples:
```

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49963        DESKTOP-DUDQHO9:49964  ESTABLISHED
  TCP    127.0.0.1:49964        DESKTOP-DUDQHO9:49963  ESTABLISHED
  TCP    127.0.0.1:55082        DESKTOP-DUDQHO9:55083  ESTABLISHED
  TCP    127.0.0.1:55083        DESKTOP-DUDQHO9:55082  ESTABLISHED
  TCP    127.0.0.1:55085        DESKTOP-DUDQHO9:55086  ESTABLISHED
  TCP    127.0.0.1:55086        DESKTOP-DUDQHO9:55085  ESTABLISHED
  TCP    192.168.29.49:49501    20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.49:62484    ec2-65-2-109-57:https  ESTABLISHED
  TCP    192.168.29.49:62487    ec2-65-2-109-57:https  ESTABLISHED
  TCP    192.168.29.49:62766    52.111.232.10:https    ESTABLISHED
  TCP    192.168.29.49:62828    20.49.99.116:8883      ESTABLISHED
  TCP    192.168.29.49:62829    20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.49:62830    20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.49:62920    170:https              CLOSE_WAIT
  TCP    192.168.29.49:62921    170:https              CLOSE_WAIT
  TCP    192.168.29.49:62938    ec2-15-207-187-50:https  ESTABLISHED
  TCP    [::1]:1521             DESKTOP-DUDQHO9:57864  ESTABLISHED
  TCP    [::1]:57864            DESKTOP-DUDQHO9:1521   ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62638  del11s11-in-x0a:https  CLOSE_WAIT
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62746  [2603:1040:f00::23a]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62783  sc-in-xbc:5228         ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62786  [2620:1ec:21::14]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62796  [2603:1040:f00::23a]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62852  [2603:1046:c04:839::2]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62924  [2607:f740:e619::1]:https  CLOSE_WAIT
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62926  [2607:f740:e619::1]:https  CLOSE_WAIT
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62937  [2603:1063:14::7]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62939  [2603:1063:14::7]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62941  [2620:1ec:42::132]:https  ESTABLISHED
  TCP    [2405:201:4008:7181:dc87:11be:46c:d9f5]:62941
```

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

8) Route : To view the routing table.

9) Netstat : The Netstat command is used to show detailed network status.

CLASSTIME

Scanned with OKEN Scanner

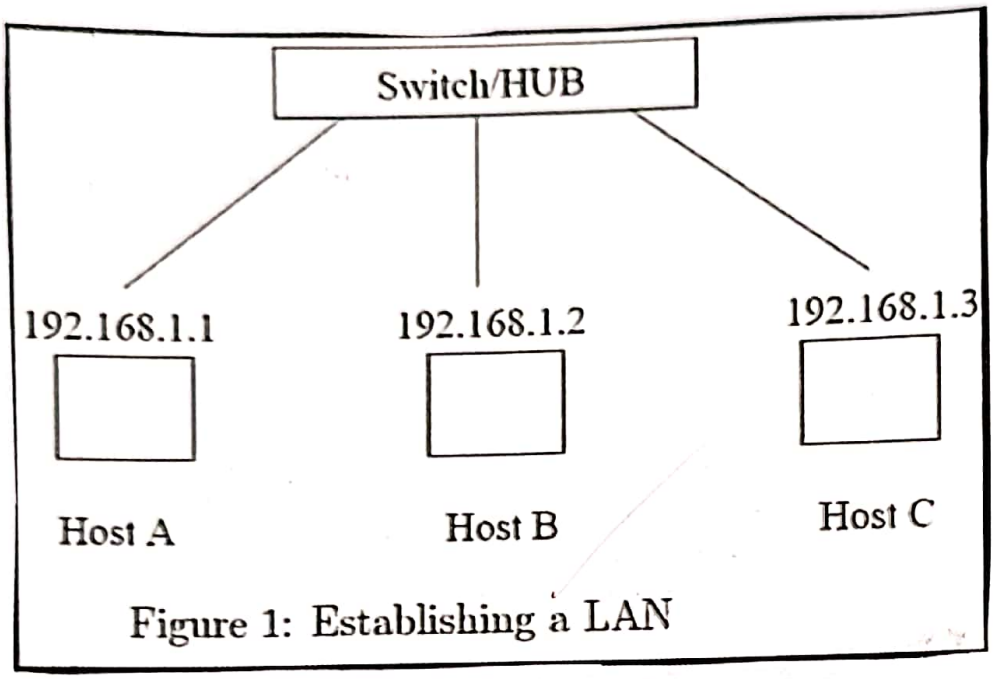
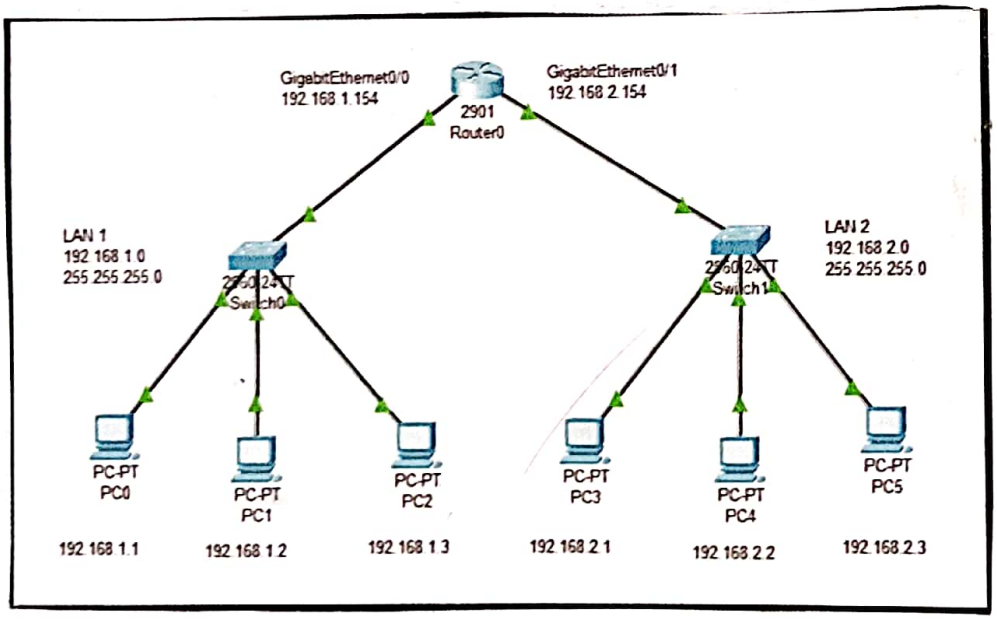


Figure 1: Establishing a LAN



Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

Experiment NO. 3

Create LAN network using Hub, Switch. Establish Inter LAN communication using Router.

Objective

To install & configure network devices HUB, Switch & Router PCs are interfaced using connectivity devices.

Theory

1) Repeaters: functioning at physical layer. A repeater is an electronic device that receives a signal & retransmit at a higher level &/or higher power, so onto the otherside of an obstruction, so that the signal can cover longer distances. Repeater has two ports, so cannot be used to connect for more than two devices.

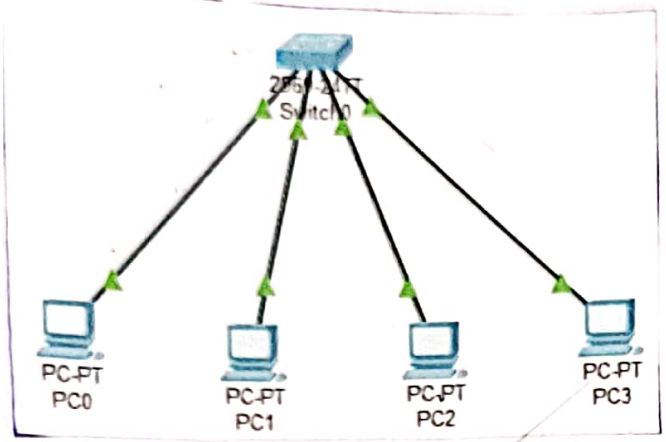
2) Hub: An Ethernet hub, active hub, network hub, repeater hub, It is a device for connecting multiple twisted pair or fiber optic Ethernet devices together & making them act as a single network segment. Hub works at the physical layer of the OSI model. This device is a form of multiport repeater.

3) Switch: It is a computer networking device that connects network segments. The term commonly referred to a network bridge that processes & route data at data link layer of the OSI model. Switches that additionally process data at the network layer are often referred to as a layer 3 switches or multilayer switches.

4) Bridge: A network bridge connects multiple segments at the data link layer of the OSI model. In the Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1 D standards. A bridge and switch are very much alike a switch being a bridge with numerous ports. Switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determined if the bridge is able to send the given pack to the another segment of the network.

CLASSTIME

Scanned with OKEN Scanner



PC0

Physical Config Desktop Programming Attributes

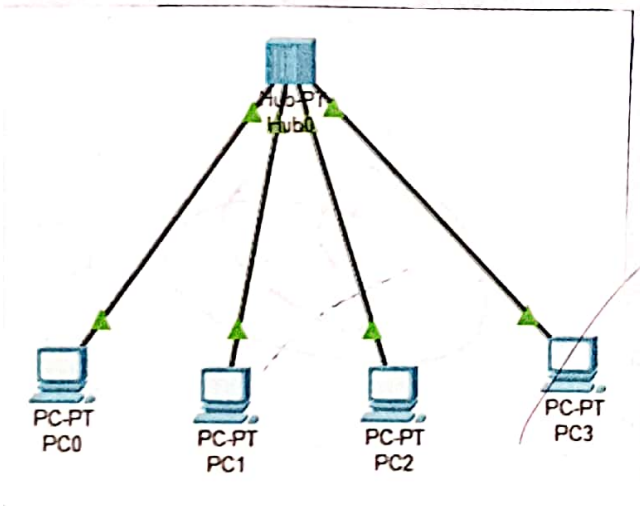
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:

Reply from 10.10.10.4: bytes=32 time<1ms TTL=128
Reply from 10.10.10.4: bytes=32 time=1ms TTL=128
Reply from 10.10.10.4: bytes=32 time=1ms TTL=128
Reply from 10.10.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

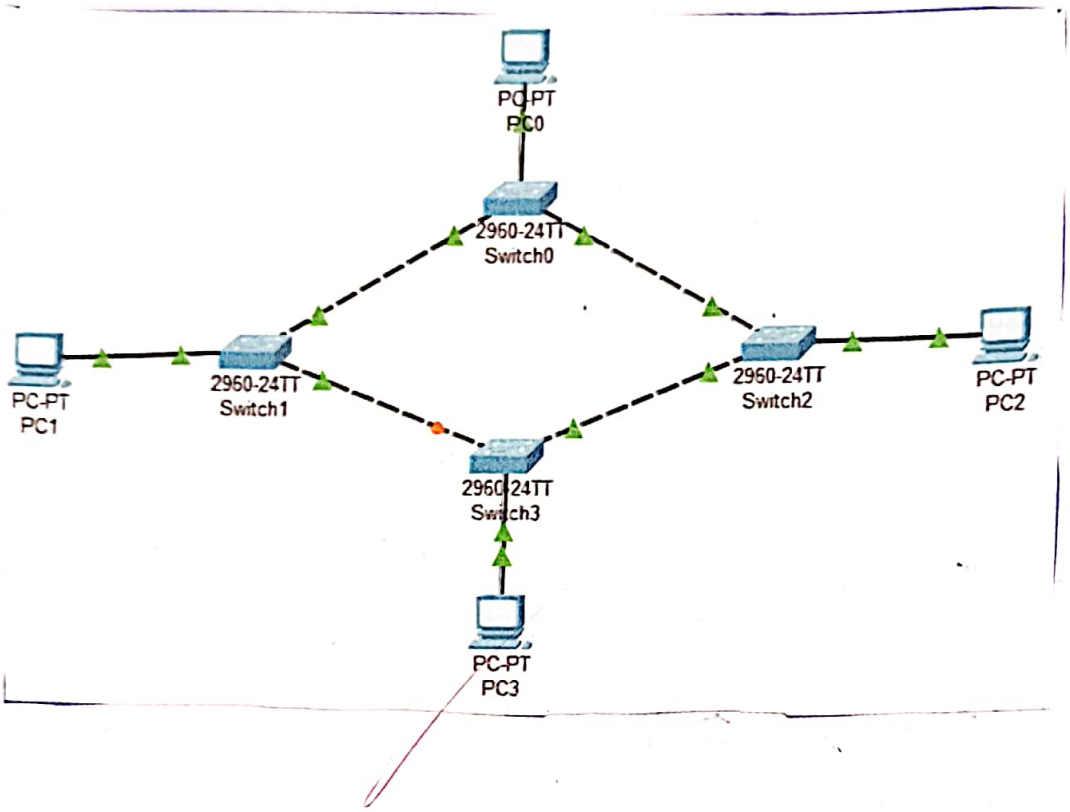
5) Router :- It is an electronic device that interconnects two or more computer network, & electively interchanges packet of data between them. Each data packet contains address information that a router can use to determine if the source & destination are on the same network, or if the data packet must be transferred from one network to another.

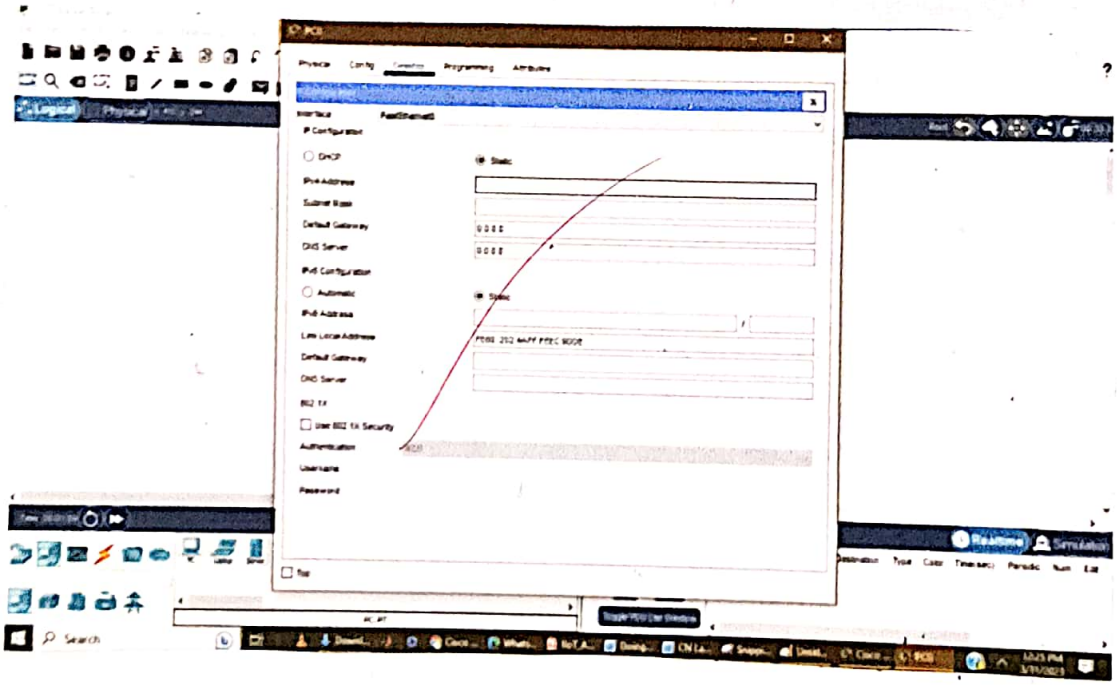
6) Gate Way :- In a communication network, a network node equipped for interfacing with another network that uses different protocols. It may contains devices such as protocol translator, impedance matching devices, rate converters, fault isolators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedure b/w both networks. A protocol translation gateway interconnects networks with different network protocol technology by performing the required protocol conversions.

Result

Thus install & configure Network devices PCs are interfaced using connectivity devices - Hub, router and Switch have been done successfully.

Scanned with OKEN Scanner





Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

Experiment NO. 4

Create Ring, Bus, Star and Mesh topology using Cisco Packet Tracer.

Objectives

1) To learn to implement different network topologies in CPT.
2) To analyse their working and application.

* Implementation of Ring Topology.

Ring topology is a kind of arrangement of the networks in which every device is linked with two other devices. This makes a circular ring of interconnected devices which gives it its name. Data is usually transmitted in one direction along the ring, known as a unidirectional ring. The data is delivered from one device to the next until it reaches the decided destination.

Steps to configure & setup Ring Topology in Cisco Packet Tracer:

1) First, open the cisco packet tracer desktop & select the devices given:

S.NO.	Device	Model Name
1	PC	PC
2	Switch	PT-Switch

IP Addressing Table

S.NO.	Device	IPv4 Address	Subnet Mask
1	PC0	192.168.0.1	255.255.255.0
2	PC1	192.168.0.2	255.255.255.0
3	PC2	192.168.03	255.255.255.0
4	PC3	192.168.04	255.255.255.0

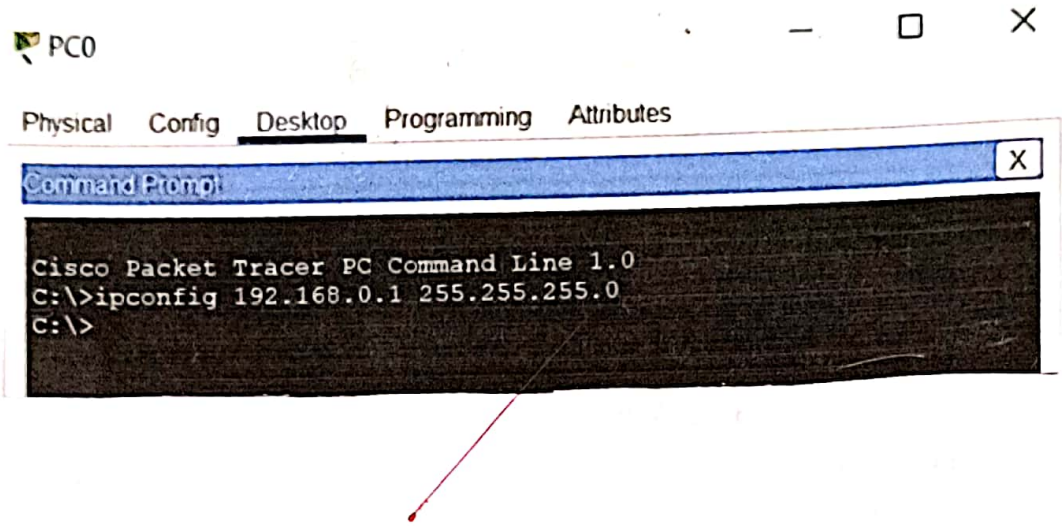
- Then, create a network topology
- Use an automatic connecting cable to connect the devices with others.

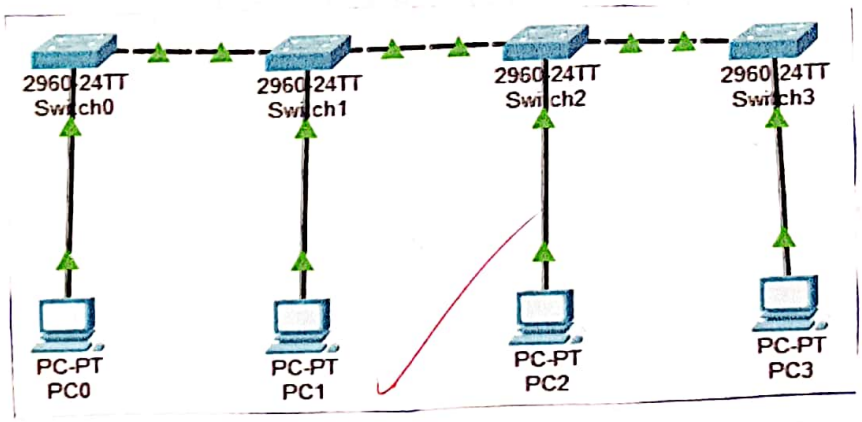
2) Configure the PCs with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then go to desktop & then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and Subnet mask.

CLASSTIME

Scanned with OKEN Scanner





Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

• Repeat the same procedure with other PCs to configure them thoroughly.

3) Verify the connection by pinging the IP address of any host in PC0

• Use the Ping command to verify the connection.

• As we can see we are getting replies from a targeted node on both PCs

• Hence, the connection is verified.

Simulation Result:

Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another targeted from PC1 to PC3

* Implementation of Bus Topology

It is a network in which nodes are directly linked with a common half-duplex link. A host on a bus topology is called station. In a bus network, every station will accept all network packets, and these packets generated by each station have equal information. priority. It includes a single network segment & collision domain.

Steps to configure & setup Bus Topology in Cisco Packet Tracer:

1) First, open the CPT desktop & select the devices given below:

S.NO.	Device	Model Name
1	PC	PC
2	Switch	PT-Switch

IP addressing table

S.NO.	Device	IPv4 Address	Subnet Mask
1	PC0	192.168.0.1	255.255.255.0
2	PC1	192.168.0.2	255.255.255.0
3	PC2	192.168.0.3	255.255.255.0
4	PC3	192.168.0.4	255.255.255.0

• Then, create a network topology.

• Use an automatic connecting cables.

2) Configure the PCs with IPv4 address and Subnet Mask according to the IP addressing table given above.

• To assign an IP address in PC0, click on PC0.

CLASSTIME

Scanned with OKEN Scanner

PC0

Physical Config Desktop Programming Attributes

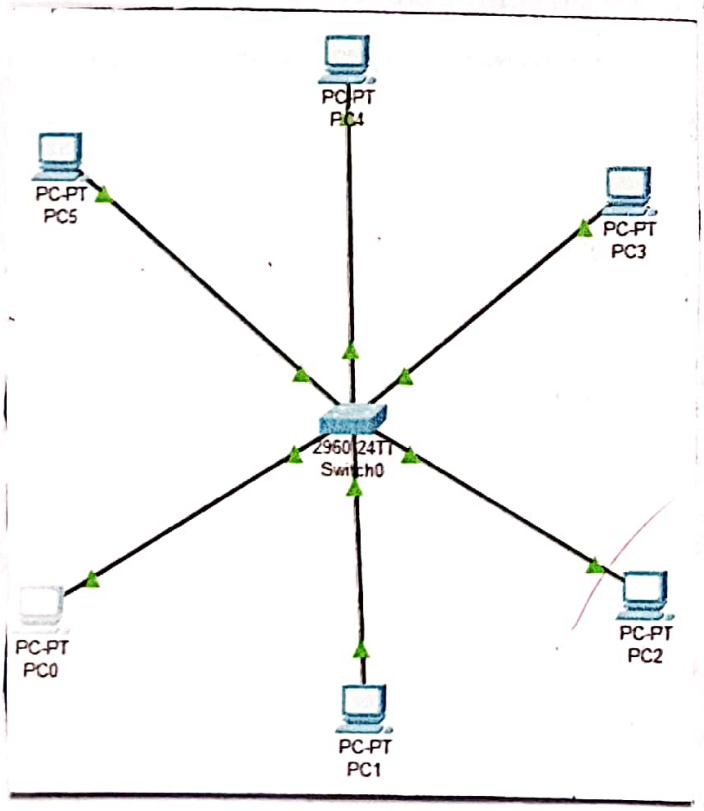
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.0.1 255.255.255.0
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

- Fill IPv4 address and Subnet mask.
- Assigning an IP address using ipconfig command, as we can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address> <Subnet mask> <defaultgateway>
- Repeat the same procedure with other PCs to config them thoroughly.

3) Verify the connections by pinging the IP address of any host in PC0.

- Use the ping command to verify the connection.
- As we can see we are getting replies from a targeted node on both PCs.
- Hence the connection is verified.

Simulation Result :

Check a simulation of the experiment by sending two PDU packets one targ from PC0 to PC2 & another targeted from PC1 to PC3.

* Implementing Star Topology

It is for a LAN is one in which each node is connected to a central connectic point, such as a hub or switch. Whenever a node tries to connect with another node then the transmission of the message must be happening with the help of the central node.

Steps Implementing Star Topology using Cisco Packet Tracer:

1) We have taken a switch & linked it to six end devices.
2) Provide the IP address to each device.
3) Link every device with the switch.
4) Transfer message from one device to another & check the table for validation. Now to check whether the connection are correct or not try to ping any device.

IP Addressing Table.

S.NO.	Device	IPv4 Address	Subnet Mask
1	PC0	192.168.0.1	255.255.255.0
2	PC2	192.168.02	255.255.255.0

CLASSTIME

Scanned with OKEN Scanner

PC2

Physical Config Desktop Programming Attributes

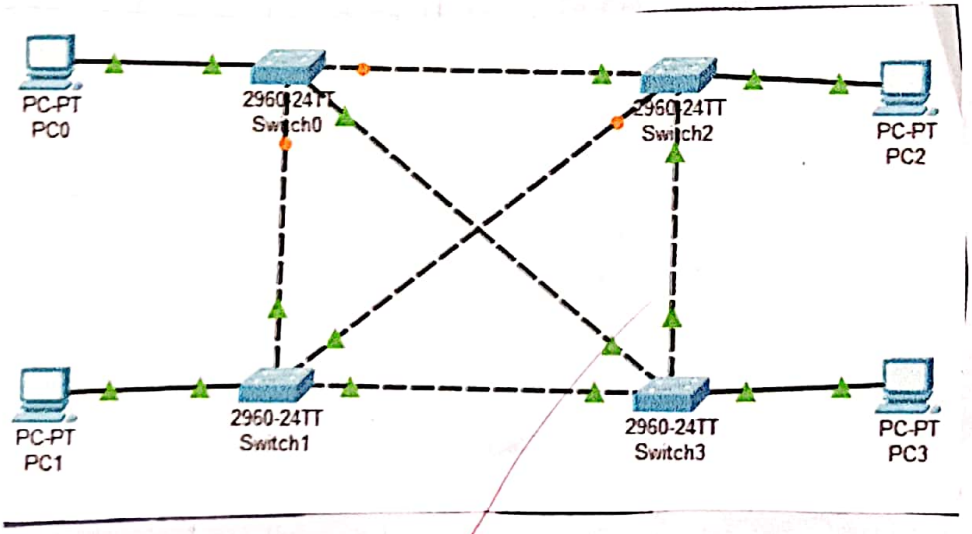
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=4ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=3ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```



Scanned with OKEN Scanner

Topic : ..... Date : ..... Page No. : .....

3	PC2	192.168.0.3	255.255.255.0
4	PC3	192.168.0.4	255.255.255.0
5	PC4	192.168.0.5	255.255.255.0
6	PC5	192.168.0.6	255.255.255.0

To do ping one terminal of one device and run the following command:

Command:

"ping ip_address_of_any_device"

Example:

ping 192.168.1.4

Simulation Result

Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another from PC1 to PC3.

* Implementation Of Mesh Topology

In this each and every device sends its own signal to the other devices that are present in the arrangement of the network.

Steps to configure & setup Ring Topology in Cisco Packet Tracer:

1) First, open CPT desktop & select the devices given below.

S.NO.	Device	Model Name
1	PC	PC
2	Switch	PT-Switch

IP Addressing Table

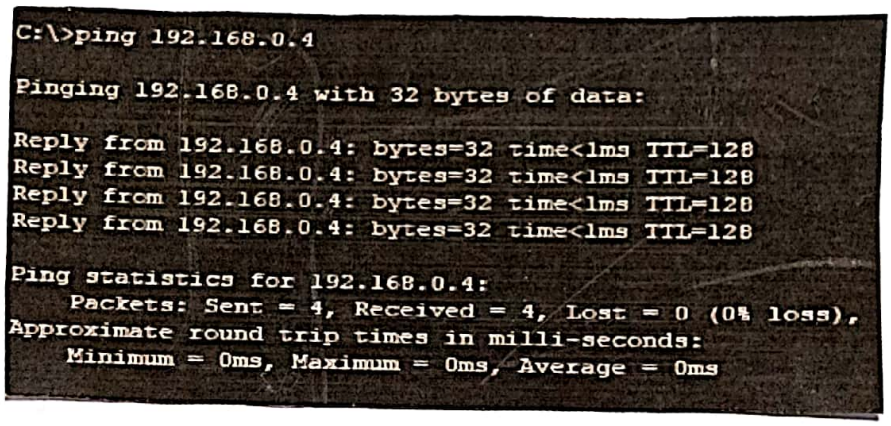
S.NO.	Device	IPv4 Address	Subnet Mask
1	PC0	192.168.0.1	255.255.255.0
2	PC1	192.168.0.2	255.255.255.0
3	PC2	192.168.0.3	255.255.255.0
4	PC3	192.168.0.4	255.255.255.0

- Then create a network topology
- Use an automatic connecting cable.

2) Configure the PCs with IPv4 address & Subnet Mask acc. to IP addressing

CLASSTIME

Scanned with OKEN Scanner



Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

- To assign an IP address in PC0, click on PC0
- Then go to desktop & then IP configuration
- fill IPv4 address & subnet mask.
- Assign IP address using IPconfig command.
- Go to the command terminal of PC.
- Then type ipconfig <IPv4address> <subnet mask> <default gateway>
- Repeat the same procedure with other PCs.

3) Verify the connection by pinging the IP address of any host in PC0.

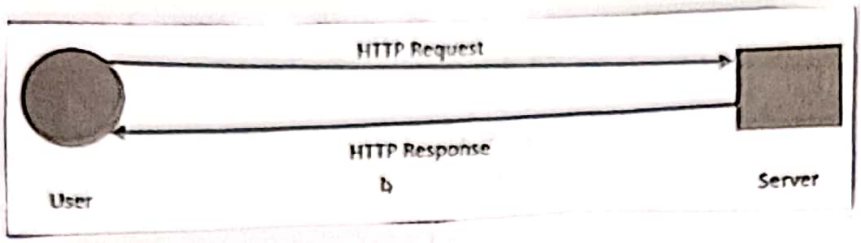
- Use the ping command to verify connection
- We will check if we are getting replies or not.
- Here we get replies from a targeted node on both PCs.
- Hence the connection is verified.

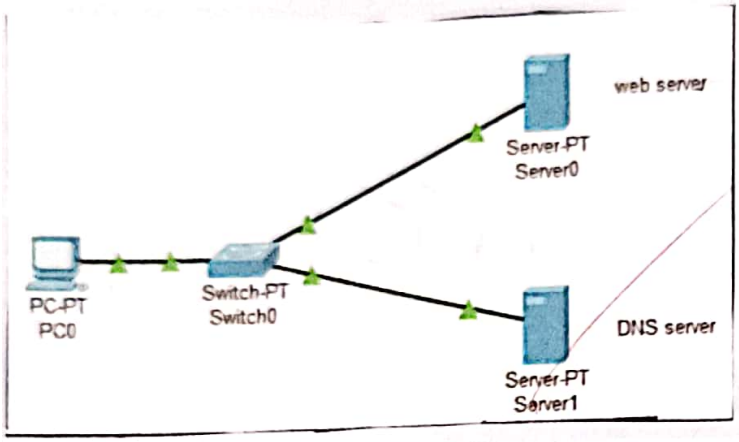
Simulation Result

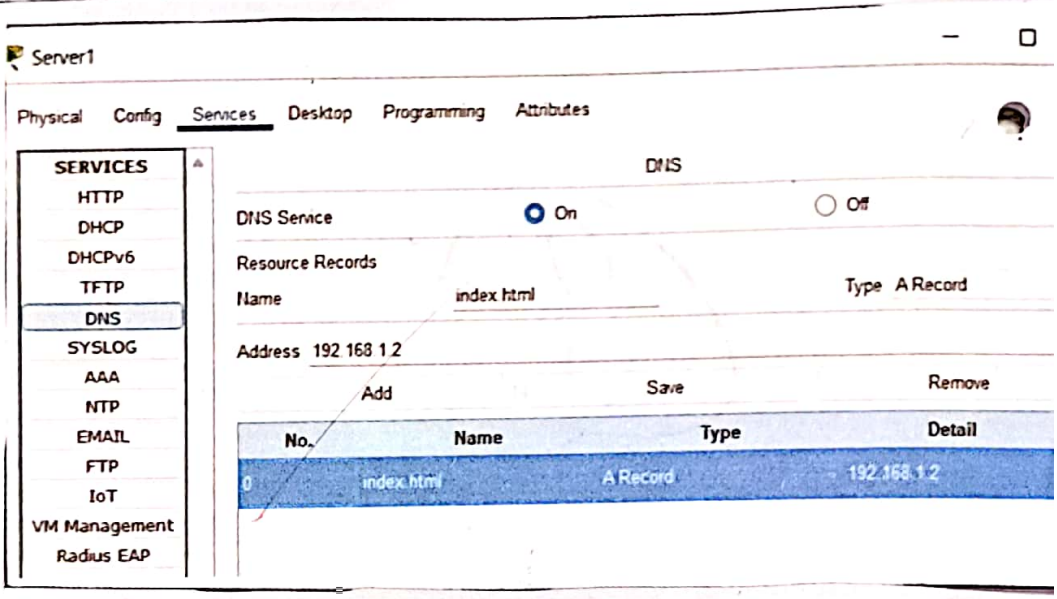
Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 & another from PC1 to PC3.

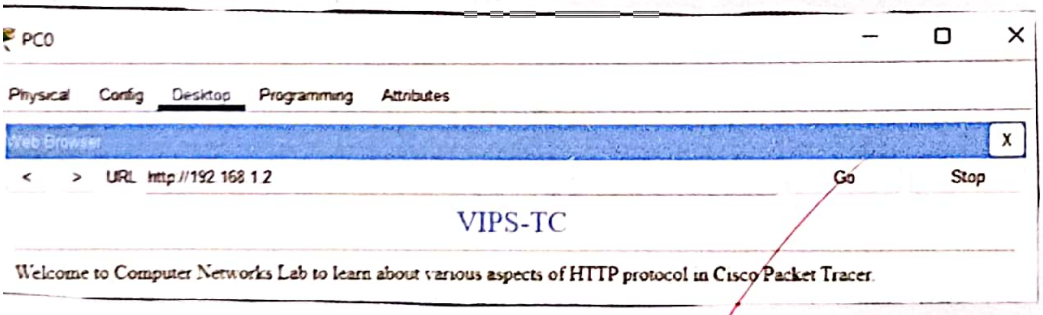
CLASSTIME

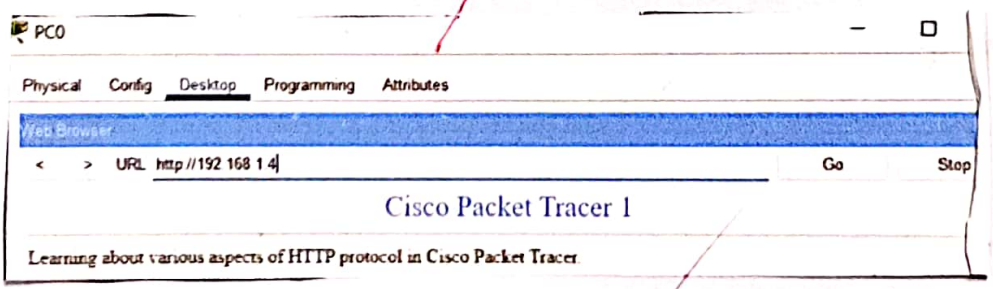
Scanned with OKEN Scanner











Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

Experiment NO. 5

Explore various aspects of HTTP Protocols.

Objective

1) Introduction to HTTP Protocol
2) To learn how to use different components & built a simple network.

Theory

Hypertext is text that links to other information by clicking on a link in a hypertext document, a user can quickly jump to different content through hypertext. It is associated with web pages & this techno. has been around since 1960s. Today, the web is where hypertext reigns, where nearly every pages includes links to other pages & both text & images can be used as link to more content.

Steps to configure Web server/ HTTP in CPT.

1) Open cisco Packet Tracer.
2) Make a topology by selecting 1 PC, 1 PT switch & 2 Server.
3) Connects all the devices using copper straight through cable connecting all using fast ethernet port.
4) Assigning IP address to all devices

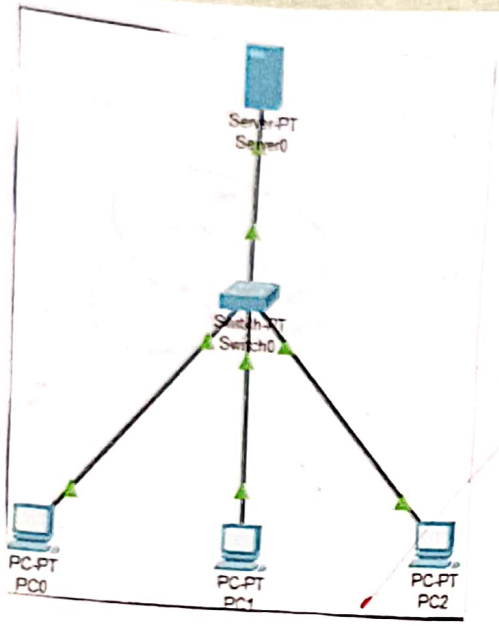
Host	IP Address	Subnet Mask	DNS Server
PC0	192.168.1.1	255.255.255.0	192.168.1.3
Web Server	192.168.1.2	255.255.255.0	192.168.1.3
DNS Server	192.168.1.3	255.255.255.0	192.168.1.3

5) Double click on web Server & select services tab. Go to HTTP option. Open index.html
6) In Index.html file, edit the pre written code.

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to Computer Networks lab to learn about various aspects of
HTTP protocol
```

CLASSTIME

Scanned with OKEN Scanner



PC0

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.1.4/helloworld.html Go Stop

Hello, world!

Back

PC0

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.1.4/image.html Go Stop

Image of Cisco Logo

This is an image of Cisco Logo

Back

PC0

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.1.4/copyrights.html Go Stop

DOWNLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE CISCO END USER LICENSE AGREEMENT("EULA" https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html) AND THE SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER ("SEULA" https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-packet-tracer-software.pdf). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, THEN CISCO SYSTEMS, INC. ("CISCO") IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE.

Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

<h2> by Dr. Vishal </h2>
</html>.

1) Click on Save & in dialog box press yes.

8) Double click on DNS server. Under services tab, select DNS option. Turn on th radio button next to DNS option. Click on Save.

9) Double click on PC. Go to service tab & select web browser option. In the url field write the name of website created as IP address of web server. Clic OK.

Exercise

Task 1) Open Cisco Packet Tracer, Make a topology by selecting 3 PC, 1 PT switch & 1 server. Assign IP address as given.

Host	IP Address	Subnet Mask	DNS Server
PC0	192.168.1.1	255.255.255.0	192.168.1.5
PC1	192.168.1.2	255.255.255.0	192.168.1.5
PC2	192.168.1.3	255.255.255.0	192.168.1.5
Web Server	192.168.1.4	255.255.255.0	192.168.1.5

In index.html file, edit the pre written code

<html>
Cisco Packet Tracer Task 1
<hr> learning about various aspects of HTTP protocol in CPT.
<h2> by (your name) </h2>
</html>.

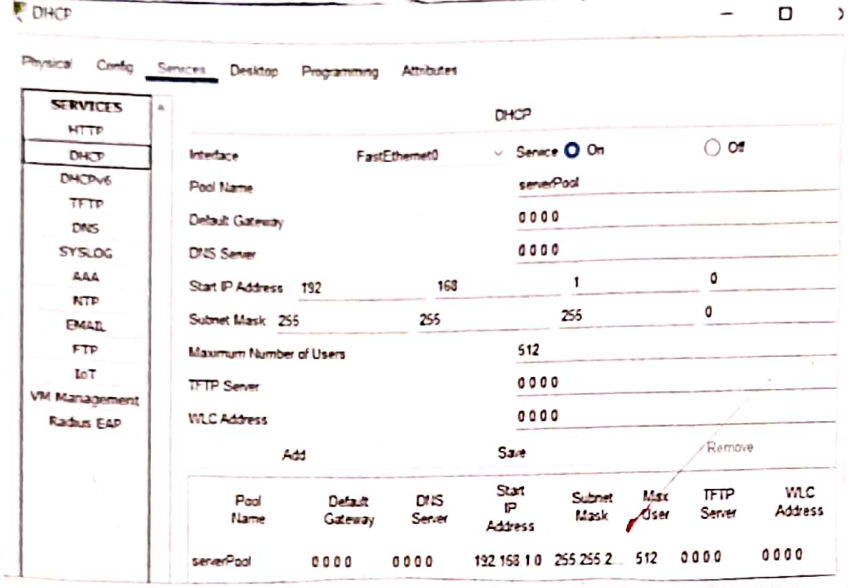
Task 2) Open Cisco Packet Tracer. Make a topology by selecting 3 PC, 1 2960 switch & 4 servers.

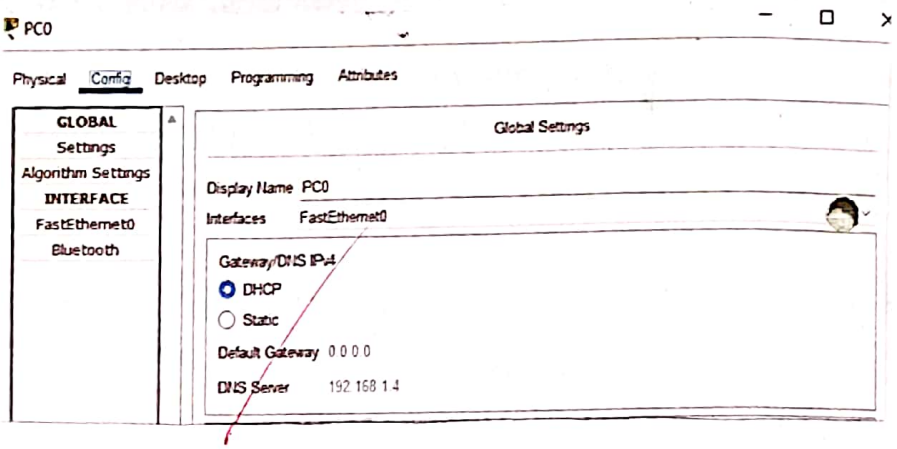
• Assigning IP address as given.

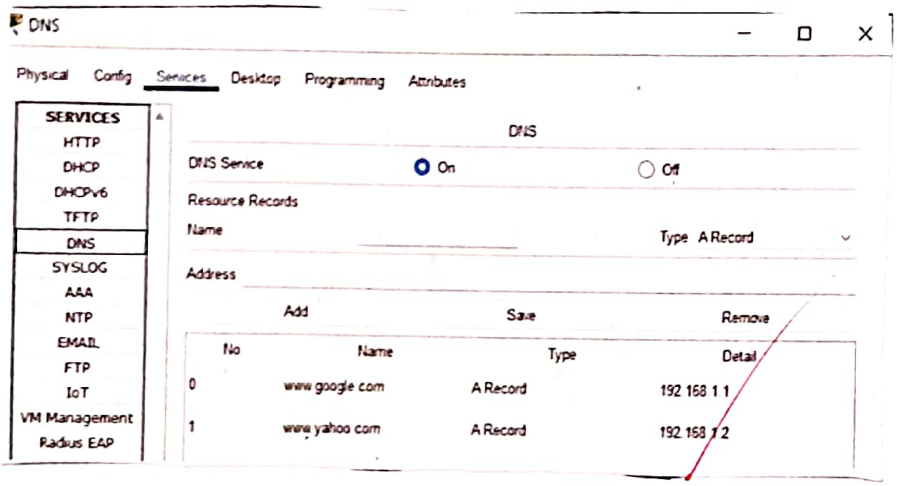
Host	IP Address	Subnet Mask	DNS server
Google	192.168.1.1	255.255.255.0	192.168.1.4
Yahoo	192.168.1.2	255.255.255.0	192.168.1.4
DHCP	192.168.1.3	255.255.255.0	192.168.1.4
DNS	192.168.1.4	255.255.255.0	192.168.1.4

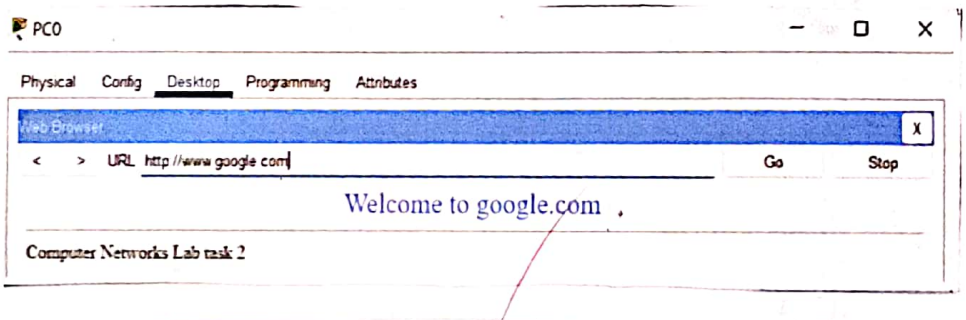
CLASSTIME

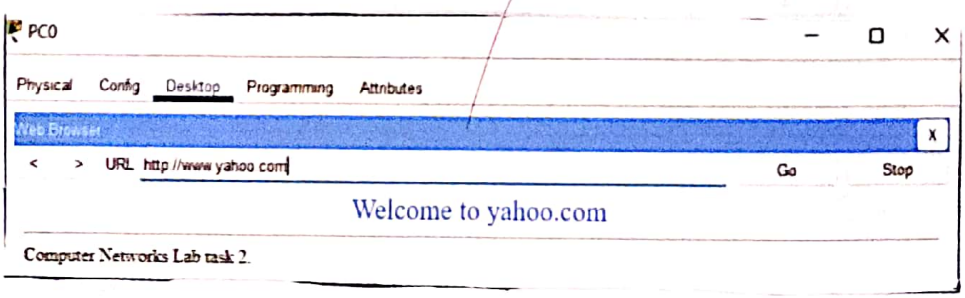
Scanned with OKEN Scanner











Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

• Set DNS for DHCP: for it, go to services tab & configure DHCP by enabling DNS IP address & disabling all other services. In DHCP service option, turn on DHCP & set DNS server IP server address to be 192.168.1.4 & start IP add: to be 192.168.1.10

• Set IP address of PCs by turning on DHCP option instead of static.

• Configure DNS server, go to service tab & disable all services options except DNS in order to avoid error due to Multiple servers. In the DNS option, turn on DNS service.

• Double click on Google server. Go to services tab & select HTML option. In the HTML option, edit 'index.html file to be:

```
<html>
<center><font size='+2' color='blue'>Welcome to google.com</font></center>
<hr> computer Networks Lab task 2.
</html>
```

Click on save.

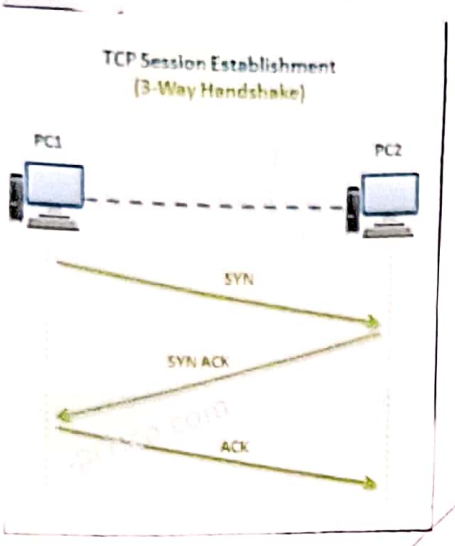
• Double click on yahoo server. Goto service tab & select HTML option. In the HTML option, edit index.html file to be:

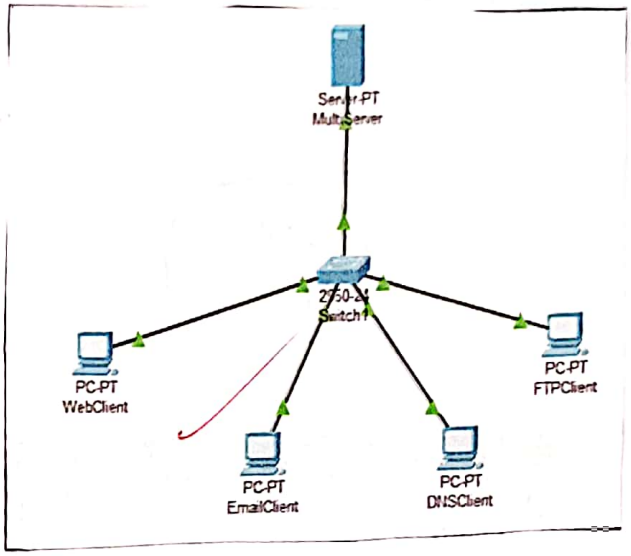
```
<html>
<center><font size='+2' color='blue'>Welcome to yahoo.com</font></center>
<hr> Computer Networks Lab task 2.
</html>
```

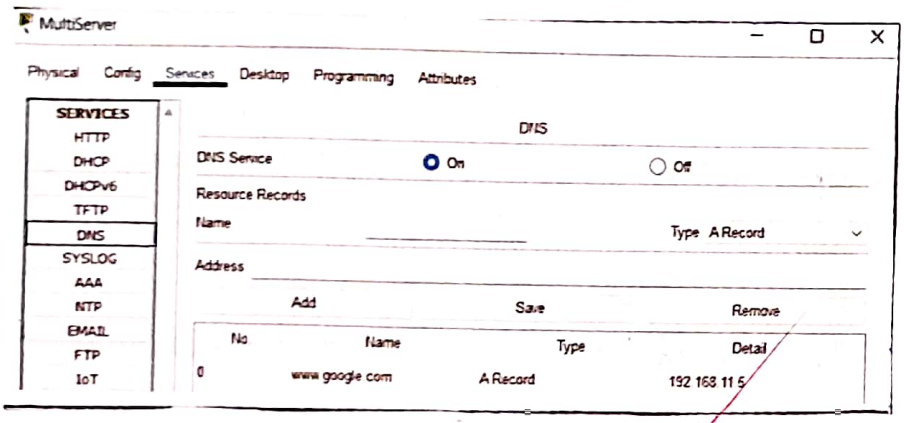
• Now call www.google.com, www.yahoo.com from each PC using web browser service option.

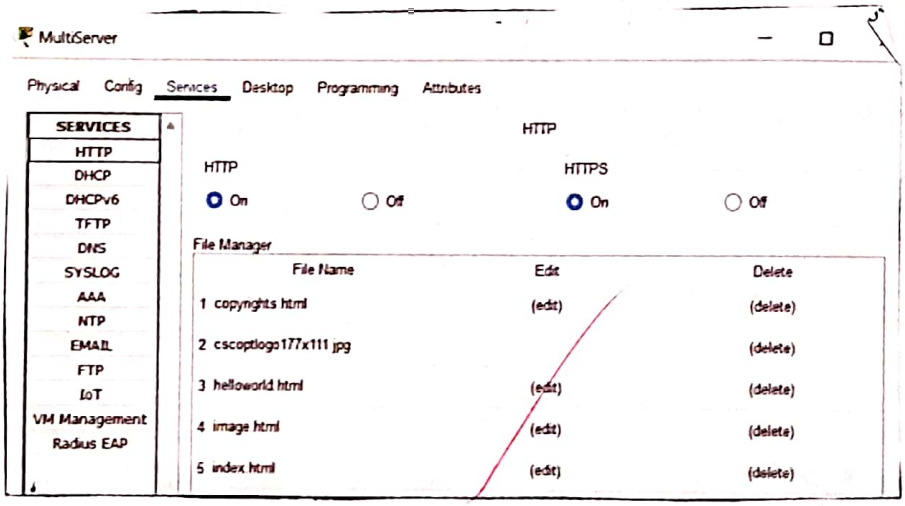
CLASSTIME

Scanned with OKEN Scanner









Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

Experiment No. 6

Analyzing various parameters for TCP Protocol in action.

Objectives

- To generate Network Traffic in Simulation Mode.
- This simulation activity is intended to provide a foundation for understanding the TCP & UDP in detail.
- Examine the functionality of the TCP & UDP Protocols in a network setup & its demonstration through Cisco Packet Tracer Tool.

Theory

Simulation mode provides the ability to view the functionality of the different protocols. As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name & associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocol & the associated PDU. This activity provides an opportunity to explore functionality of the TCP & UDP Protocols, multiplexing & the function of port numbers in determining which local application requested the data or is sending the data.

TCP is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arises from packet-based messaging, such as lost packet, corrupted packets. It is a connection oriented transport protocol. The TCP session must be establishe to use TCP.

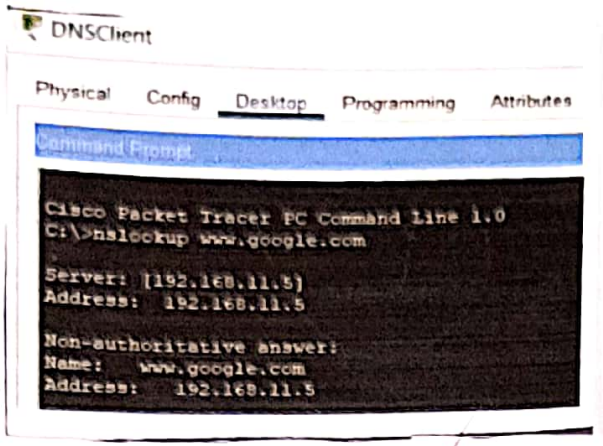
Three-way Handshake mechanism consists of three messages as its name implies. These messages are: SYN, SYN-ACK, ACK. In these segments, related TCP Header flags are set to 1 i.e., if it is a SYN Message, SYN bit is set to 1 and similary for others.

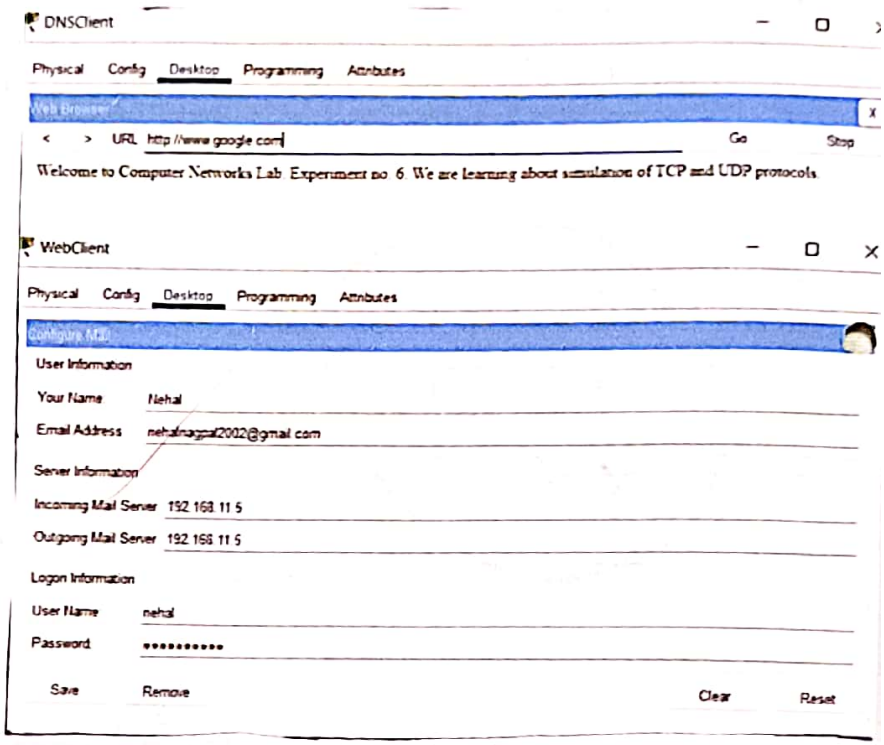
Steps to configure TCP & UDP Protocols simulation in Cisco Packe Tracer

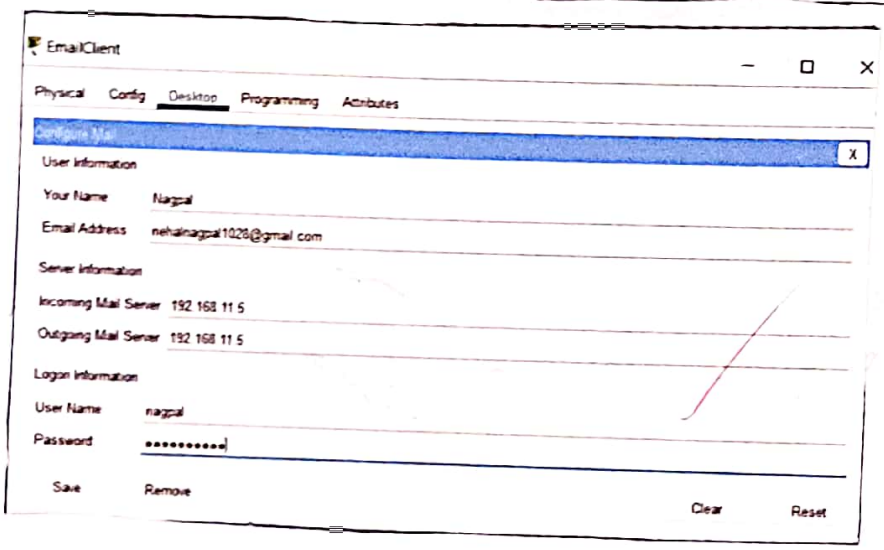
1) Open Cisco Packet Tracer.

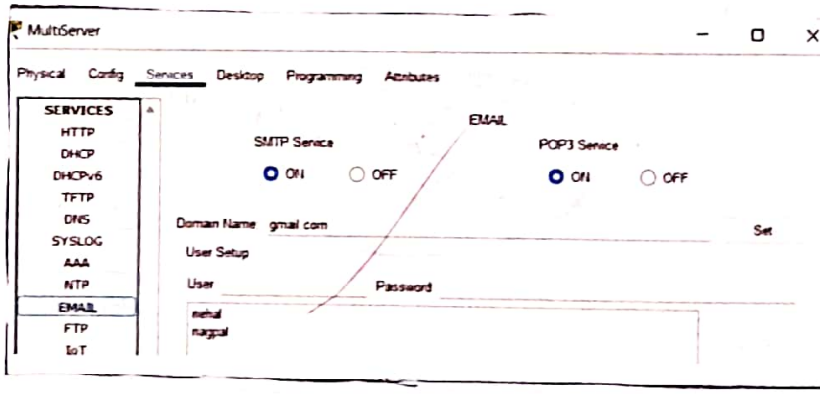
CLASSTIME

Scanned with OKEN Scanner









Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No : .....

2) Make a topology as shown in figure.

3) Connect all the devices using copper straight through cable, connecting all using Fast Ethernet Port.

4) Assign IP Address to all devices

Host	Label	IP Address	Subnet Mask	DNS Server
PC0	Web Client	192.168.11.1	255.255.255.0	192.168.11.5
PC1	Email Client	192.168.11.2	"	"
PC2	DNS Client	192.168.11.3	"	"
PC3	FTP Client	192.168.11.4	"	"
Server	MultiServer	192.168.11.5	"	"

5) Double Click on Multi Server, from the pop-up window, select service tab

- Under Services selected DNS service.
- Turn on DNS service
- Within DNS, name record to be www.google.com address - 192.168.11.5.
- Click on Add record.

6) Double click on Multi Serve, from the pop-up window, select services tab.

- Under Services select HTTP services.
- Turn on HTTP & HTTPS options ON
- Select index.html & click on edit option.
- Type the following text

<html>
Welcome to Compute Network lab.
</html>.

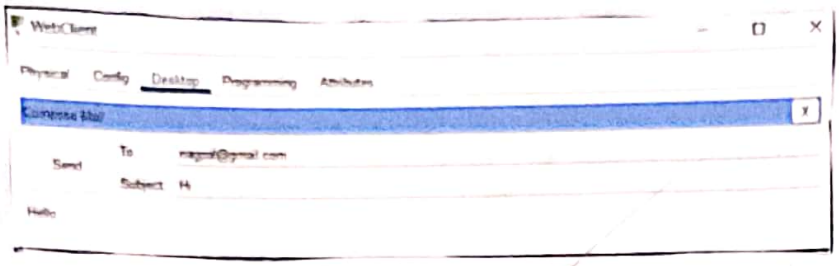
- Click on save, click on yes.

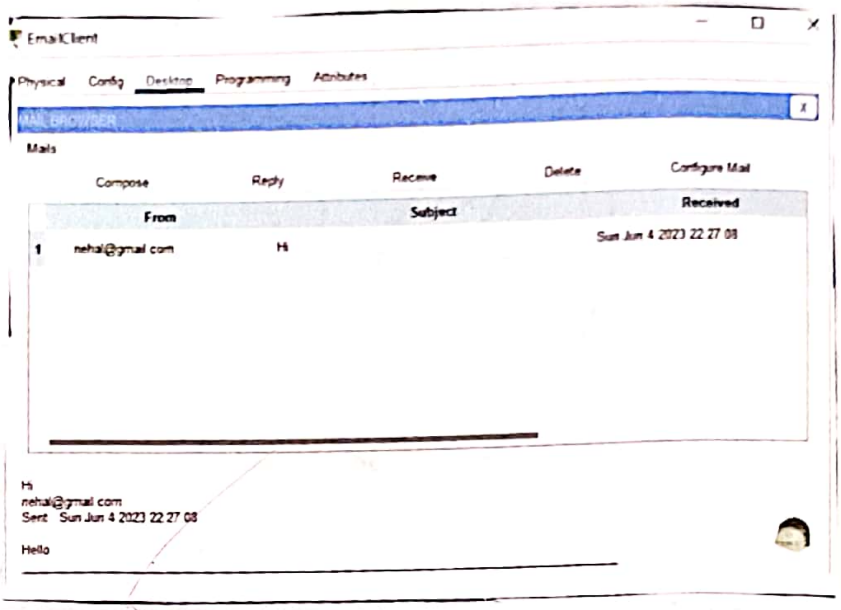
7) Double Click on DNS client.

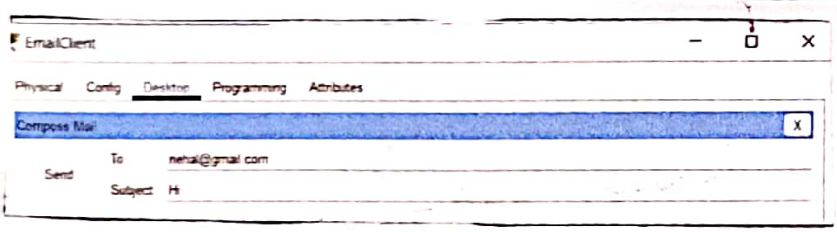
- Within the desktop tab select command prompt option.
- Type nslookup www.google.com.
- This statement lets you know whether DNS Client can connect to server or not & resolve the IP address issues.
- Within the Desktop Tab select Web browser Option
- In the URL type www.google.com

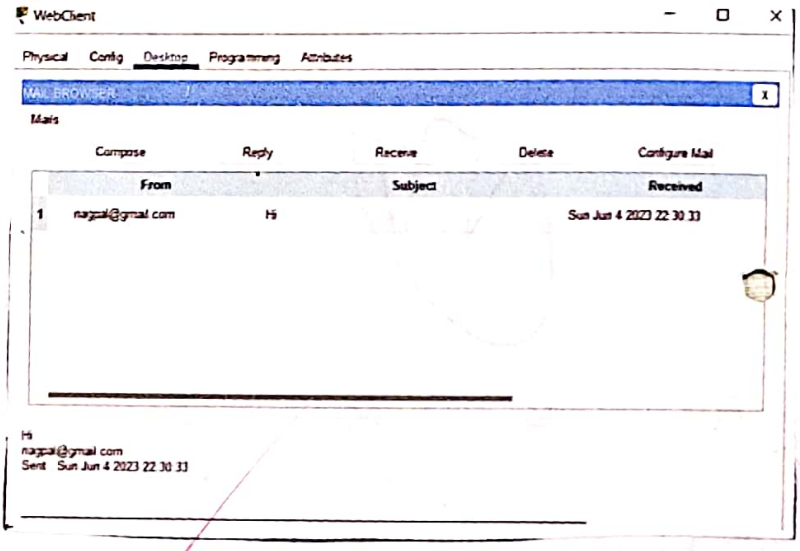
CLASSTIME

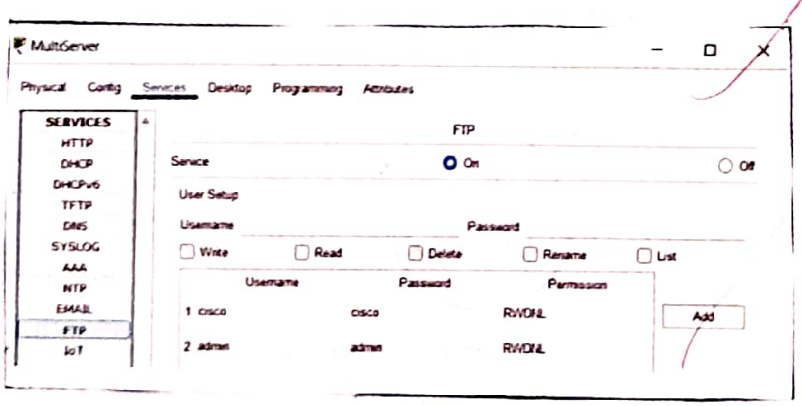
Scanned with OKEN Scanner











Scanned with OKEN Scanner

Topic : ..... Date : ..... Page No. : .....

9) Double Click on Email Client
- Within the desktop Tab select Email option
- In the configure mail box write:
- Name
- Email
- Incoming mail server: 192.168.11.5
- Outgoing mail server: 192.168.11.5
- User Name
- Password.
- Click on Save.

10) Double Click on Multi Server
- Within the services tab, select Email option
- Switch on SMTP & POP3 service.
- Type domain name: gmail.com.
- Under User Setup: Name; Password
- Click on Add
- Under User Setup: Name (diff.); Password
- Click on Add.

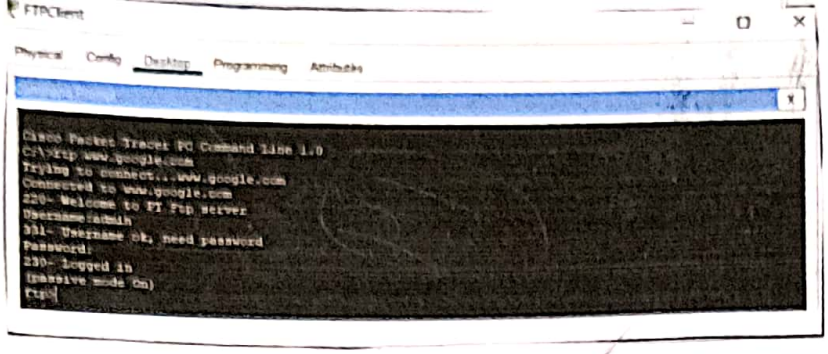
11) Double Click on Web Client
- Within the Desktop tab, select Email option
- Send a mail by composing a mail.
- In the To section write: name@gmail.com.
- Subject: Hi
- Mail Box: Hello
- Click on Send Mail.

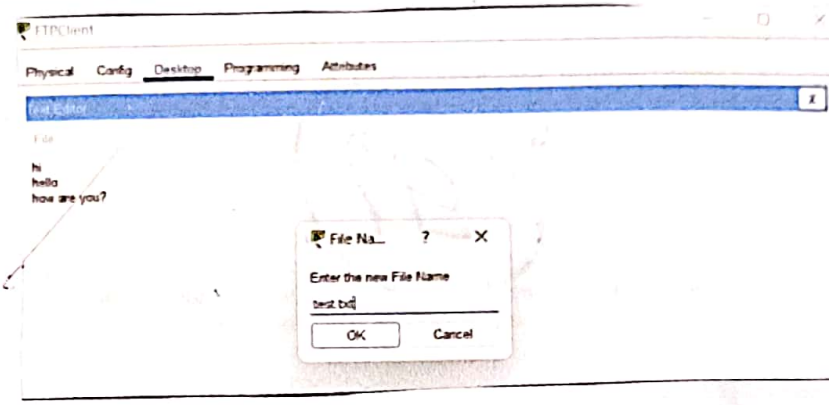
12) Double Click on Email Client
- Within the Desktop, select Email option
- In the popup window, select Receive option.

13) Double Click on Email Client
- Within the Desktop tab, select Email option
- Send a mail by composing a mail
- In the To section write name(diff.)@gmail.com.

CLASSTIME

Scanned with OKEN Scanner






```
ftp>put test.txt

Writing file test.txt to www.google.com:
File transfer in progress...

[Transfer complete - 21 bytes]

21 bytes copied in 0.076 secs (276 bytes/sec)
ftp>dir

Listing /ftp directory from www.google.com:
0    : asa842-k8.bin                                5571584
1    : asa923-k8.bin                                30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
3    : c1841-ipbase-mz.123-14.T7.bin                13832032
4    : c1841-ipbasek9-mz.124-12.bin                 16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin       33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
7    : c2600-i-mz.122-28.bin                        5571584
8    : c2600-ipbasek9-mz.124-8.bin                  13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin              5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin       33591768
14   : c2950-i6q412-mz.121-22.EA4.bin               3058048
15   : c2950-i6q412-mz.121-22.EA8.bin               3117390
16   : c2960-lanbase-mz.122-25.FX.bin               4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin       10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin         33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin        83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin       505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG          159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG          184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin     160968869
27   : ir800-universalk9-mz.SPA.155-3.M             61750062
28   : ir800-universalk9-mz.SPA.156-3.M             63753767
29   : ir800_yocto-1.7.2.tar                        2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar           6912000
31   : pt1000-i-mz.122-28.bin                       5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
33   : test.txt                                     21
ftp>
```

```
ftp>dir

Listing /ftp directory from www.google.com:
0    : asa842-k8.bin                                5571584
1    : asa923-k8.bin                                30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
3    : c1841-ipbase-mz.123-14.T7.bin                13832032
4    : c1841-ipbasek9-mz.124-12.bin                 16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin       33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
7    : c2600-i-mz.122-28.bin                        5571584
8    : c2600-ipbasek9-mz.124-8.bin                  13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin              5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin       33591768
14   : c2950-i6q412-mz.121-22.EA4.bin               3058048
15   : c2950-i6q412-mz.121-22.EA8.bin               3117390
16   : c2960-lanbase-mz.122-25.FX.bin               4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin       10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin         33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin        83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin       505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG          159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG          184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin     160968869
27   : ir800-universalk9-mz.SPA.155-3.M             61750062
28   : ir800-universalk9-mz.SPA.156-3.M             63753767
29   : ir800_yocto-1.7.2.tar                        2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar           6912000
31   : pt1000-i-mz.122-28.bin                       5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
33   : test.txt                                     3117390
```

Scanned with OKEN Scanner

Topic : Date : Page No :

- Subject : Hi
- Mail Box : I receive the mail
- Click on Send mail.

14) Double Click on Web Client
- Within the desktop tab, select Email option
- In the pop-up window, select Receive option.

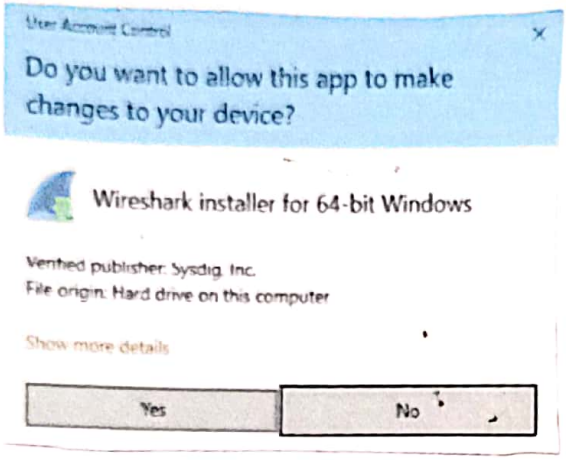
15) Double Click on Multi-Server, from the pop-up window, select services tab.
- Under Services select FTP Service
- Set Username & Password as admin.
- Enable all options : write, read, delete, rename & list
- Click on Add record.

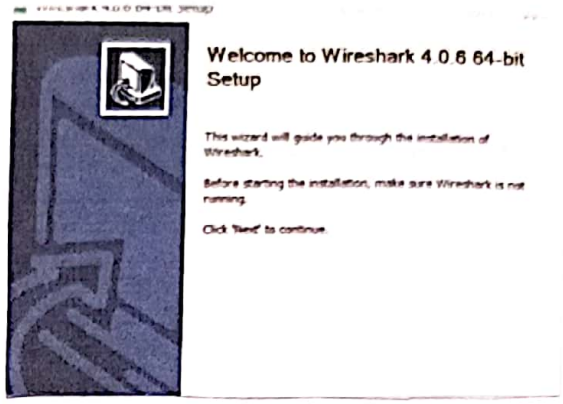
16) Double Click on FTP client,
- Within the Desktop tab select Command Prompt option
- Type ftp www.google.com.
- Username : admin
- Password : admin
- Close the command Prompt window.
- Open Textedit of services
- Type any message & save it as test.txt
- Now open command prompt again.
- Type : put test.txt
- Type : dir.

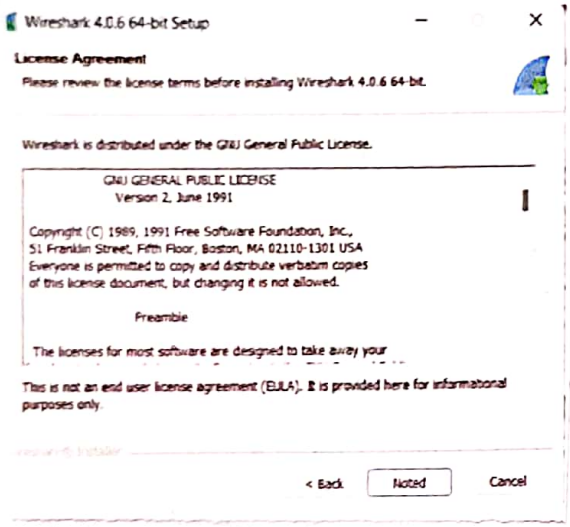
17) Double Click on DNS Client,
- Within the Desktop Tab, select Command Prompt option.
- Type ftp www.google.com.
- Username : admin
- Password : admin
- Type : get test.txt.
- Type : dir (directory option to check whether test.txt is pup up in server or not.)

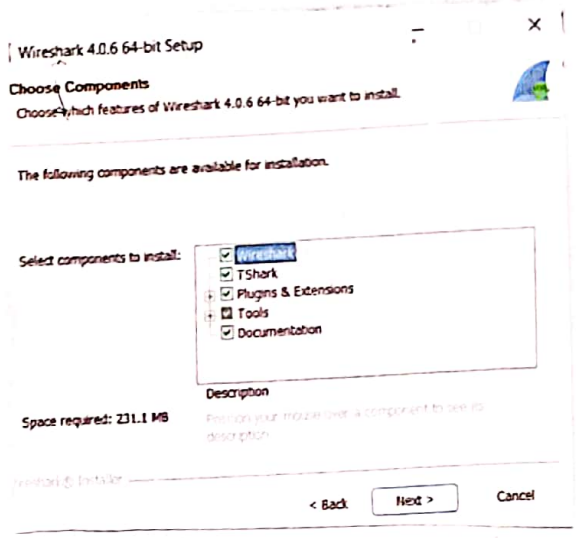
CLASSTIME

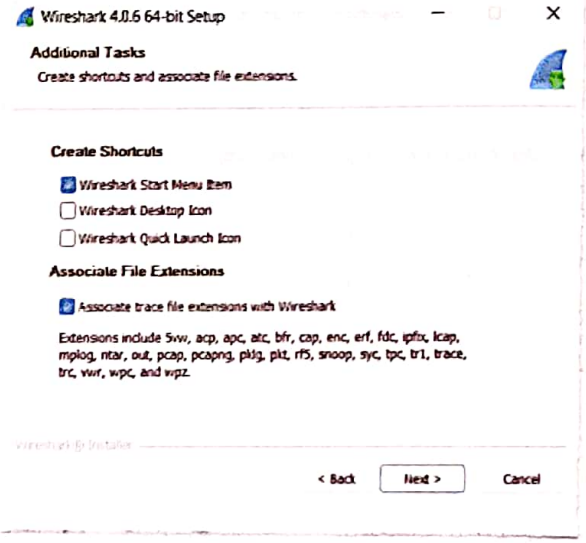
Scanned with OKEN Scanner











Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

Experiment NO. 1

Introduction to basic networking tools: Wire Shark & Network Miner.

Objectives

- Use one of the best packet sniffing tool i.e, "Wire Shark".
- Use "Network Miner" great tools for automatic extraction of files from a packet.
- Control upon ports, protocols & data packets.
- Start capturing & analyzing packet.

What is Wireshark?

It has a very rich history ranging to mid-2006. It is a network packet analyzer which presents captured packet data in detail. It is a measuring device for examining what's happening inside a network cable. It is available for free & is open source.

Benefits of Wireshark

It offers several benefits that make it appealing for everyday use. It is aimed at both single-user & expert packet, & offer a variety of features.

→ Supported Protocols: Wireshark excel in no. of protocols.

→ User-friendliness: GUI based, with very closely written context menu.

→ Cost: Available for free & open source

→ Program support: freely distributed software, relies on its user base to provide support.

Installing Wireshark on Microsoft Windows Systems.

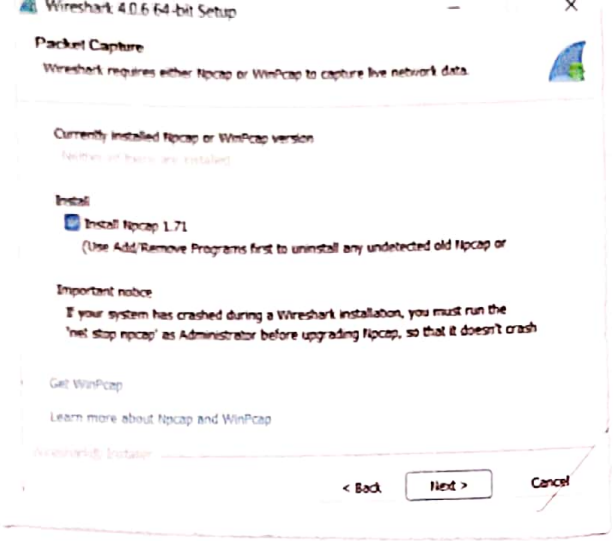
Open Wireshark Web page, http://www.wireshark.org/. Navigate to download section on website & choose a mirror. follow the steps:-

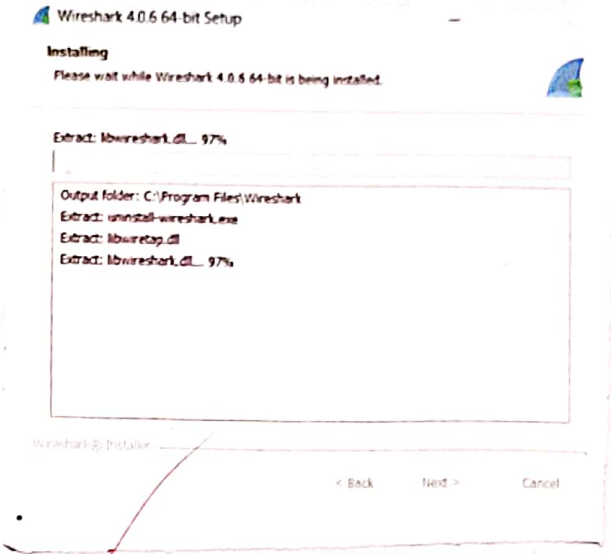
1) Double click .exe file to begin installation, & then click Next in Introductory window.

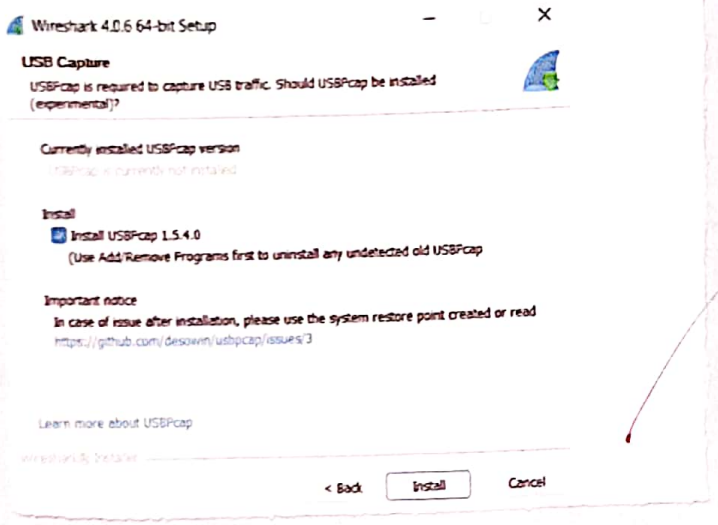
2) Install software. Read licensing agreement, & then click I Agree.

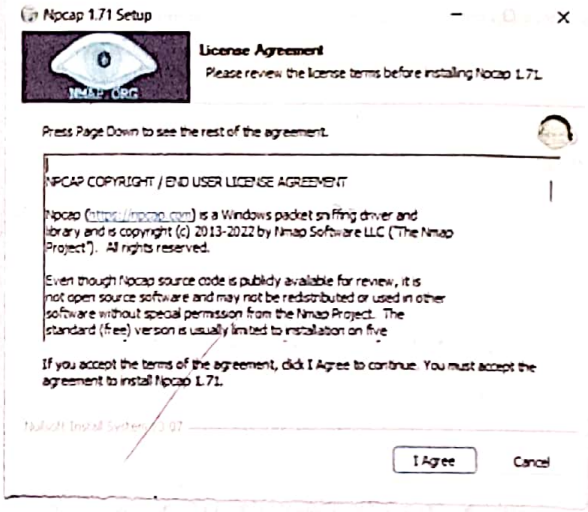
CLASSTIME

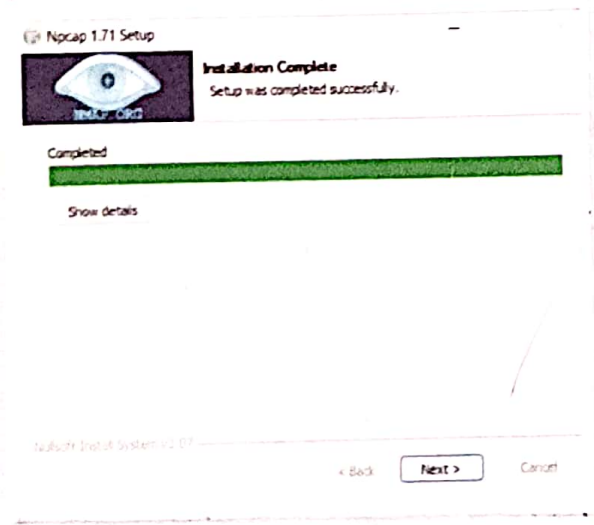
Scanned with OKEN Scanner

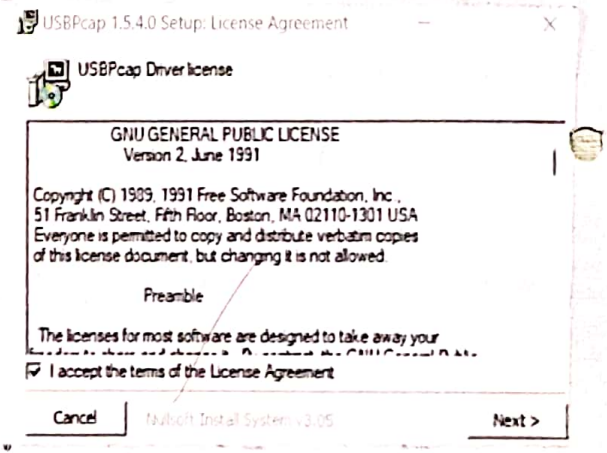












Scanned with OKEN Scanner

Topic : ..... Date. : ..... Page No. : .....

3) Click Next in Additional Task window.
4) Select components of Wireshark to install
5) Select location where you wish to install Wireshark, & then click Next.
6) Make sure install Winpcap box is checked, & then click Install.
7) When Winpcap installation start, click next in introductory window, read license agreement, & then click I Agree.
8) Winpcap installs on computer. After installation is complete, click finish.
9) Wireshark should complete its installation. When its finished, click Next.
10) In installation confirmation window, click finish.

What is Network Miner?

Open source network forensics tool that extracts files, images, emails, & passwords from captured network traffic in PCAP files. Can be used to capture live network traffic by sniffing a network interface.

Benefits of using Network Miner

Easy-to-use, requiring least processing time. Wireshark for packet capture analysis as in extracts & sorts found data into categories of host, file, image, and more by parsing a pcap file.

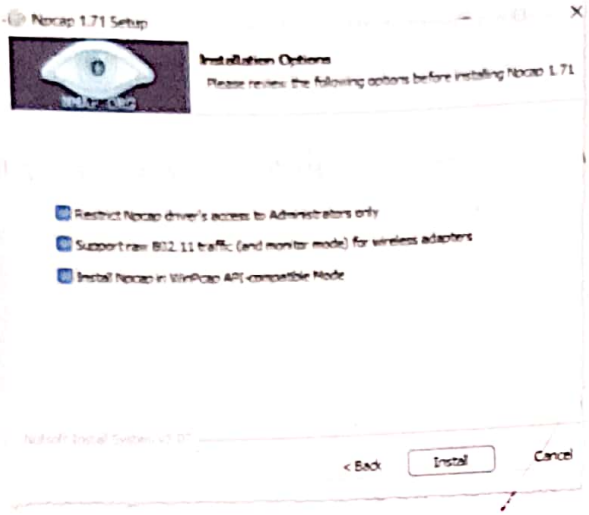
- Easy-to-use, requiring least processing time.
- Can extract user credentials for supported protocols & display under "credential" tab.
- User can search sniffed or sorted data for keywords
- Portable application that doesn't require any installation, which means that USB version, can run directly from USB flash drive.

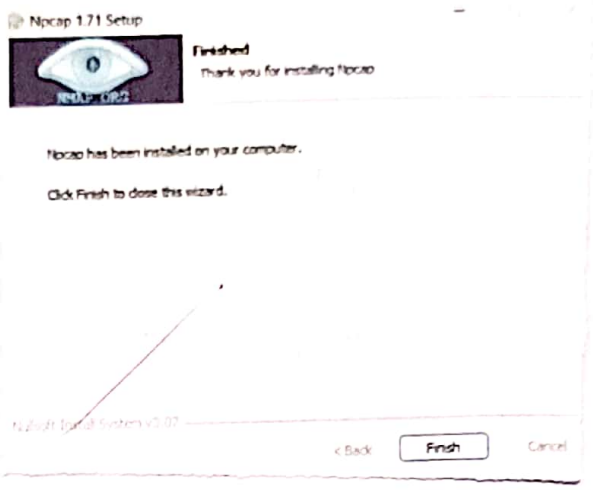
Installing Network Miner on Microsoft Windows System.

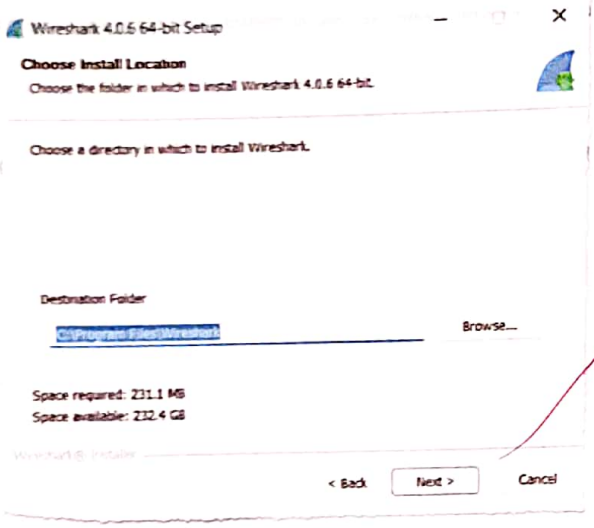
1) Download from link: https://www.netresec.com/?download=NetworkMiner.
2) Right click on the file & select option extract here.
3) Open folder & click on the network miner file.

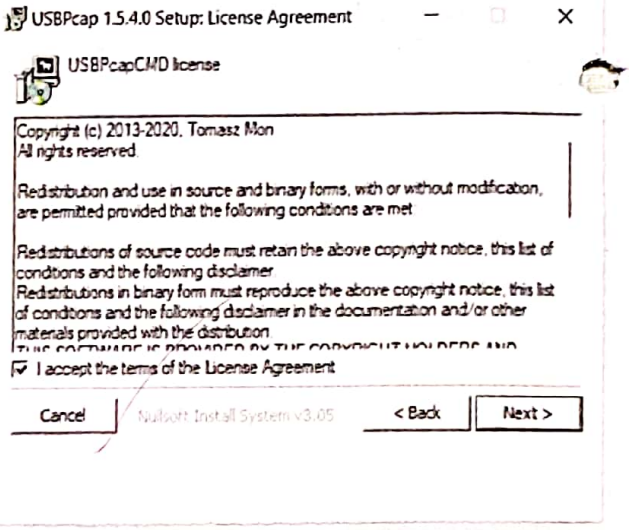
CLASSTIME

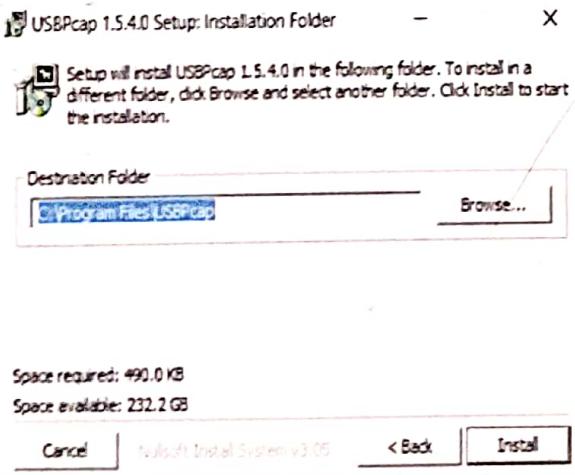
Scanned with OKEN Scanner

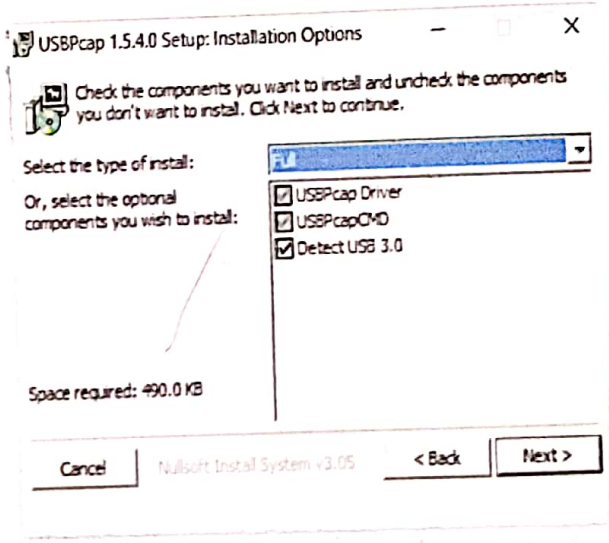












Scanned with OKEN Scanner

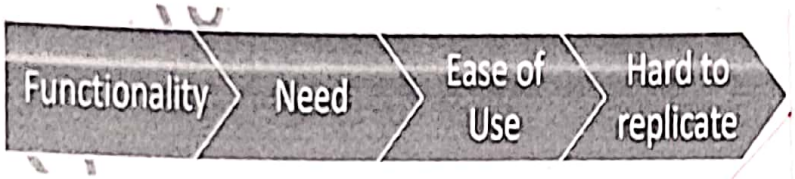
Topic..... Date.....

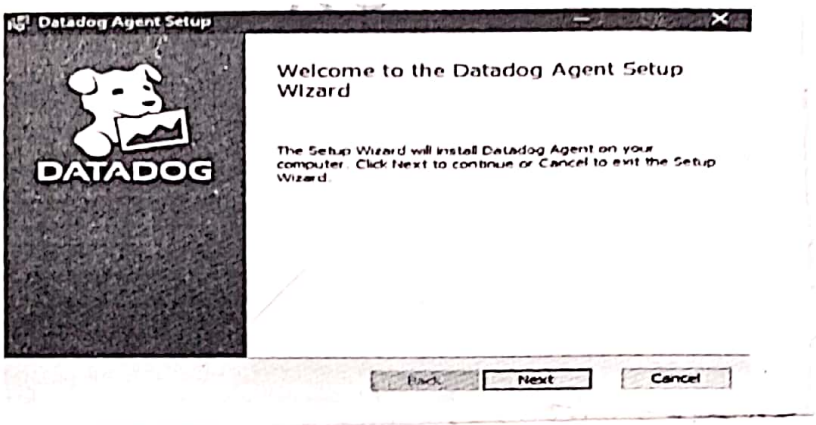
Result:

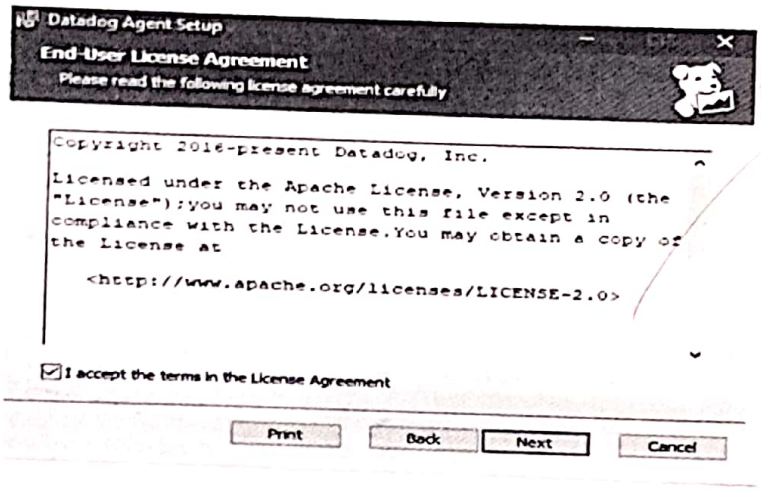
Thus, basic interface, layout & capabilities of networking tools such as WireShark & Network Miner was studied & demonstrated through softcourses.

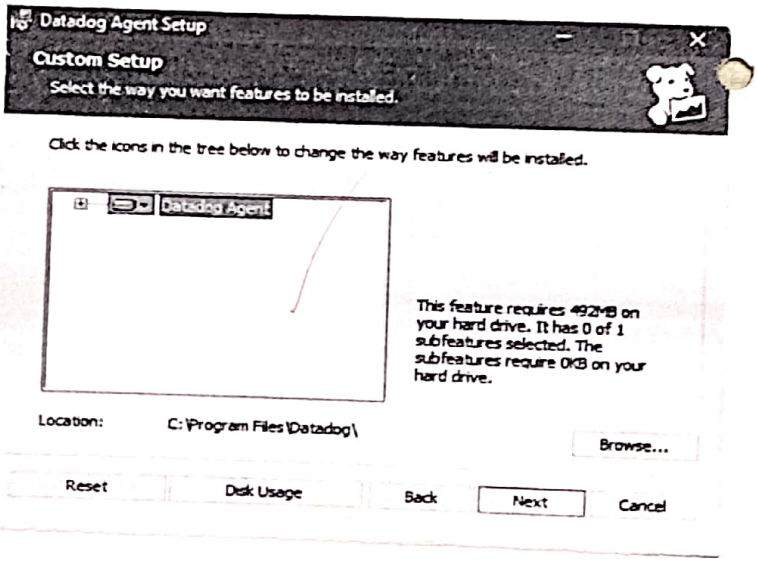
Teacher's Signature: _____

Scanned with OKEN Scanner









Scanned with OKEN Scanner

Topic..... Date.....

Experiment NO. 8

Introduction to Datadog tool for Data Monitoring in Network

Objectives

- To familiarize students with the datadog tool & its capabilities for monitoring network data.
- To train students on how to use the Datadog tool to monitor network data & analyze data trends.

Theory

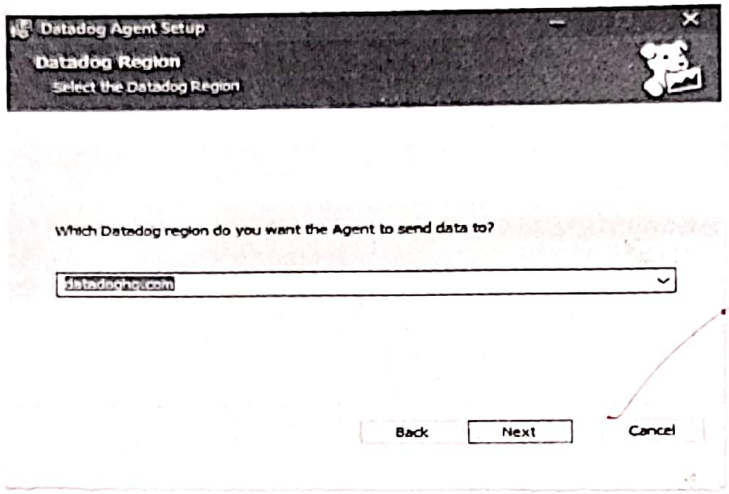
- It is a monitoring service for cloud scale application, providing monitoring of servers databases tools & services through a SaaS-based analytics platform.
- It is used for log management, infrastructure monitoring & app: monitoring.
- It can collect data from servers, databases & cloud services.
- Users can monitor their network in real time & get alerts when anomalies occ
- It makes it easy to integrate services such as Slack & PagerDuty for notification.
- It was found in 2010 by Olivie Pomel & Alexis Le-Quoc.
- It provides functionality in an easy-to-use manner that would be difficult to build & maintain ourselves.
- Has prebuilt integrations to pull data from almost every important service we u
- Generates a consolidated event stream that can be filtered & searched as needed.
- Have nice stream processing capabilities for generating alerts, & it can surface them in services like page of duty & slack.

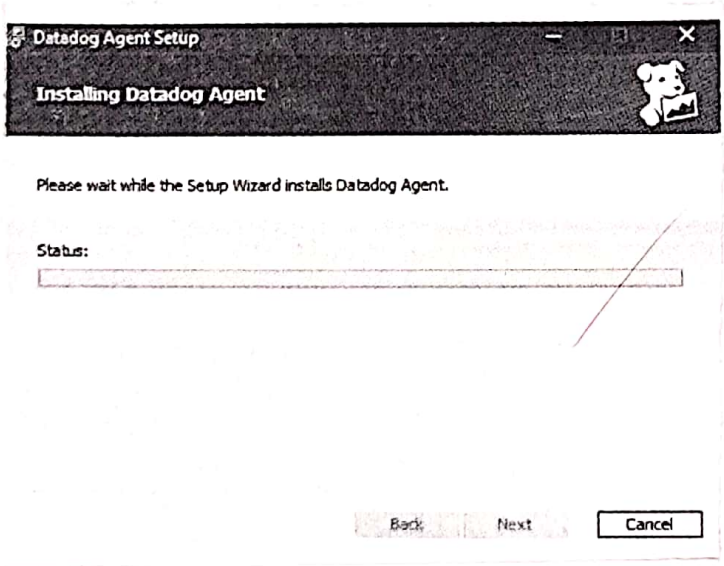
Procedure to Download Data Dog Agent

1) Registers for Data Dog-Monitoring as a service to registers for Data Dog, follow:
- Go to Datadog website https://www.datadoghq.com/
- Click on "start free trial" button on the top right of the website.
- Fill out the form & click on the "Create Account" Button.

Teacher's Signature: _____

Scanned with OKEN Scanner





Scanned with OKEN Scanner

Topic..... Date.....

2) Installation of agents on Window machines: to install Datadog agents on Windows machines, follow the steps:

- log in to your Datadog account.
- Go to the Agents Download page.
- Download the DataDog Agent Installer.
- Run the installer by opening datadog-agent-7-latest.amd-64.msi.
- Follow the prompts, accept the license agreement & enter your datadog API key 68e98ae58bf1b1a95dcf60968e2c02c3.
- Then enter your datadog Region: datadoghq.com.
- follow the on-screen instructions to install the agent on your windows machines
- When the install finishes, you are given the option to launch the Datadog Agent Manager.

3) Connect the agents to the DataDog platform: To connect the installed agents to the Datadog platform, follow the steps:

- log in to your Datadog account.
- Navigate to the Integration page.
- Select the corresponding windows services that you want to monitor.

4) Monitor your network Data with Datadog: To monitor the network data with Datadog, follow the steps:

- log in to your DataDog account.
- Navigate to the monitoring page.
- Customize the dashboard as per your requirements.
- Add widgets for the services that you want to monitor.

Result

In this practical, how to setup Datadog & monitor network data using Procas study Procas described how Datadog helps analyze the data trends & identifies anomalies in real time. It was demonstrated to be effective for monitoring Infrastructure & apps in cloud-based environments, utilizing its user-friendly interface & integration capabilities. Datadog is a valuable tool for network data analysis.

TELC

Teacher's Signature:

Scanned with OKEN Scanner