A Laboratory Manual For

Advanced Computer Network

(22520)

Semester –V

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION • MUMBAI

Maharashtra State

Board of Technical Education, Mumbai

(Autonomous) (ISO 9001 : 2015) (lSO/IEC 27001 : 2013)

,

(Autonomous) (ISO 9001 : 2008) (lSO/IEC 27001 : 2005)

4th Floor, Government Polytechnic Building, 49, Kherwadi, Bandra (East), Mumbai

400051.

(Printed on June, 2019)

MAHARASHTRA STATE

BOARD OF TECHNICAL EDUCATION

Certificate

This is to certify that Mr. / Ms:………………………………………………………………........

Roll No. ...., of Fifth Semester of Diploma in……………………………….......................... of Institute............………………………………………………………… (Code:………......) has completed the term work satisfactorily in course . **Advanced Computer Network (22520)** for the academic year 20…. To 20…… as Prescribed in curriculum.

Place:…………………… Date: ……………………..

Enrollment No:………………………………… Exam. Seat No:……………………………...

Subject Teacher Head of Department Principal

Sr. No.		CO	CO	CO	CO	CO
	Practical Outcome	**a.**	**b.**	**c.**	**d**	**e.**
1.	Capture ICMPv4 packets generated by utility programs and tabulate all the captured parameters using Wireshark.	√				
2.	Configure IPv6 network using any network simulator		√			
3.	Configure IP routing with RIP using relevant software			√		
4.	Configure IP routing with OSPF using relevant software			√		
5.	Configure User Datagram Protocol(UDP) Part-1 using relevant software				√	
6.	Configure User Datagram Protocol(UDP) Part-II using relevant software				√	
7.	Configure Transmission Control Protocol(TCP) using relevant software				√	
8.	Configure Dynamic Host Configuration Protocol(DHCP) using relevant software					√
9.	Configure Domain Name Server (DNS) using relevant software					√
10.	a. Configure File Transfer Protocol (FTP) using relevant software					√
	b. Configure Hypertext Transfer Protocol (HTTP) using relevant software					
11.	a. Use Telnet to Login a remote machine b. Connect remote machine using Secure Shell(SSH)					√
12.	Configure SMTP, POP3 and IMAP using relevant software					√

Sr. No.	Practical Outcome	Page No.	Date of Performance	Date of Submission	Assessment Marks (25)	Dated sign of teacher	Remarks
1.	Capture ICMPv4 packets generated by utility programs and tabulate all the captured parameters using Wireshark						
2.	Configure IPv6 network using any network simulator						
3.	Configure IP routing with RIP using relevant software						
4.	Configure IP routing with OSPF using relevant software						
5.	Configure User Datagram Protocol(UDP) Part-1 using relevant software						
6.	Configure User Datagram Protocol(UDP) Part-II using relevant software						
7.	Configure Transmission Control Protocol(TCP) using relevant software						
8.	Configure Dynamic Host Configuration Protocol(DHCP) using relevant software						
9.	Configure Domain Name Server (DNS) using relevant software						
10.	a. Configure File Transfer Protocol (FTP) using relevant software b. Configure Hypertext Transfer Protocol (HTTP) using relevant software						
11.	• Use Telnet to Login a remote machine • Connect remote machine using Secure Shell(SSH)						
12.	Configure SMTP, POP3						

	and IMAP using relevant software						

Practical No.01: Capture ICMPv4 packets generated by utility programs and tabulate all the captured parameters using Wireshark.

- **Practical Significance**
  - Student should be able to Configure IP routing with RIP using relevant software
- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**

  Ability to install and configure Wireshark.

  Ability to Capture ICMPv4 packets.

- **Relevant Course Outcomes**

  Implement Network Layer Protocols

- **Practical Outcomes (POs)**
  - Understand concept of Wireshark.

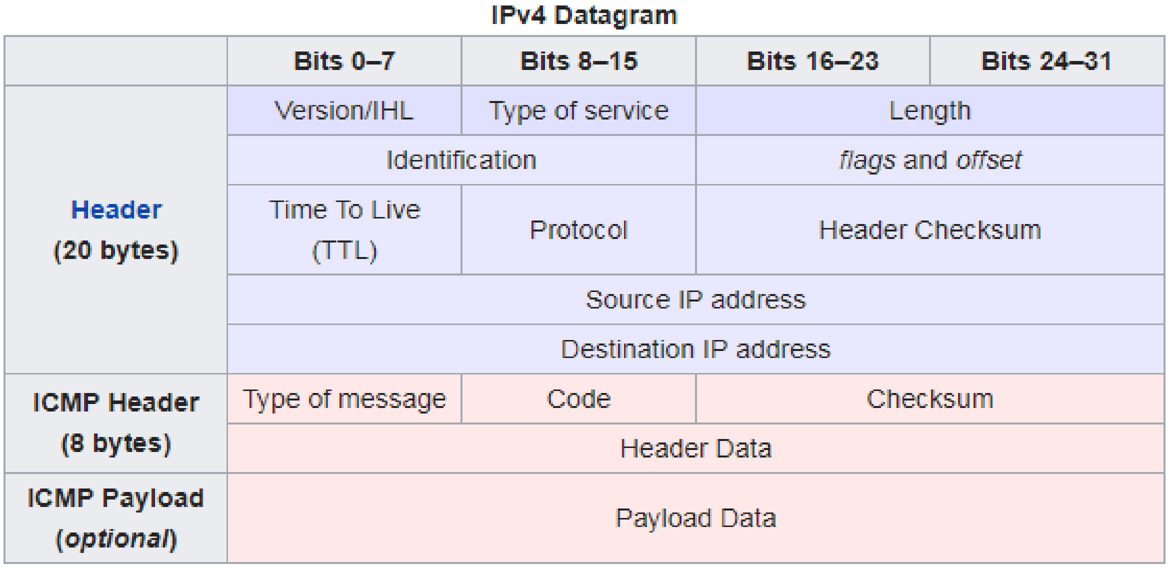
    Understand capturing ICMPv4 packets
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Proposition 1. Introduction to Wireshark:

Wireshark tool which is used for packet capture in the networks. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. It was originally named as etheral. Wireshark puts your network card into promiscuous mode, which basically tells it to accept every packet it receives. It allows the user to see all traffic being passed over the network.

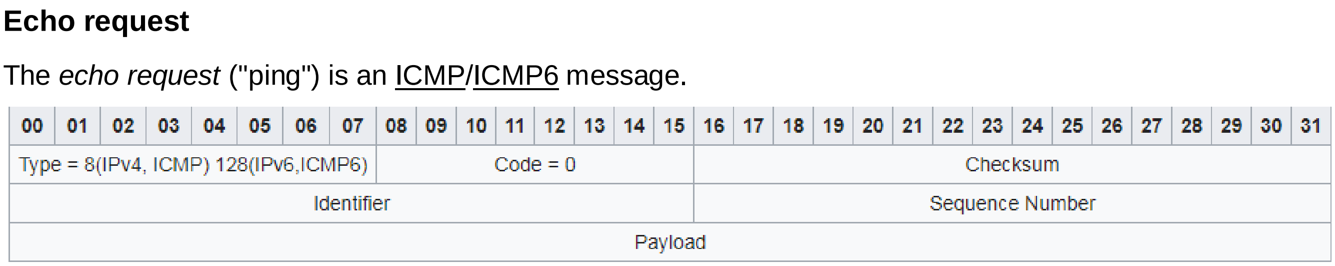
Wireshark uses pcap to capture packets. Basically, pcap is a library of information about various protocols, their packet structure, and different messages passed in those protocols. So it can only capture the packets on the networks supported by pcap.When you install Wireshark you will receive a prompt to install the WinPcap component, which is nothing but the windows version of pcap. For unix like environments, another library by the name libcap is available.

Proposition 2. ICMP IPv4 datagram format:



IPv4 Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header **(20 bytes)**	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header **(8 bytes)**	Type of message	Code	Checksum	
	Header Data			
ICMP Payload **(*optional*)**	Payload Data			



Echo request

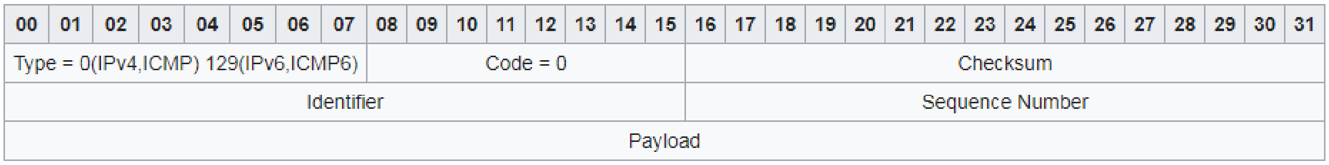
The *echo request* ("ping") is an ICMP/ICMP6 message.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 8(IPv4, ICMP) 128(IPv6,ICMP6)								Code = 0								Checksum															
Identifier																Sequence Number															
Payload																															

The Identifier and Sequence Number can be used by the client to match the reply with the request that caused the reply. In practice, most Linux systems use a unique identifier for every ping process, and sequence number is an increasing number within that process. Windows uses a fixed identifier, which varies between Windows versions, and a sequence number that is only reset at boot time.

Echo reply

The echo reply is an ICMP message generated in response to an echo request; it is mandatory for all hosts, and must include the exact payload received in the request.



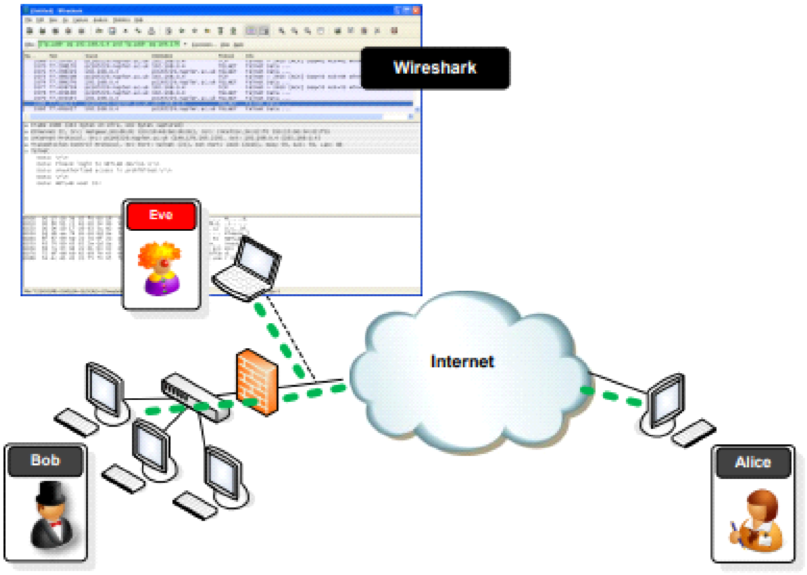
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 0(IPv4,ICMP) 129(IPv6,ICMP6)								Code = 0								Checksum															
Identifier																Sequence Number															
Payload																															

The *identifier* and *sequence number* can be used by the client to associate each echo request with its reply.

VIII. Stepwise Procedure:

Packet Capture (Packet Sniffing)

A packet sniffer is an application which can capture and analyse network traffic which is passing through a system’s Network Interface Card (NIC). The sniffer sets the card to promiscuous mode which means all traffic is read, whether it is addressed to that machine or not. The figure below shows an attacker sniffing packets from the network, and the Wireshark packet sniffer/analyser (formerly known as ethereal).

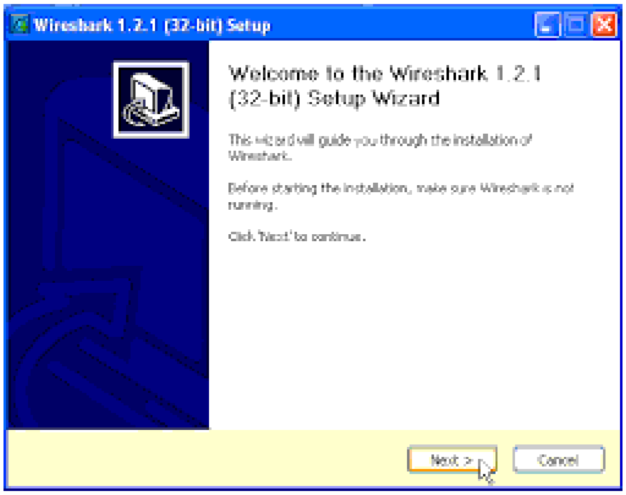


Packet Analysis

Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorising packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

Download and install Wireshark on your PC.

Wireshark is a network packet sniffer (and protocol analyzer) that runs on many platforms, including Windows XP and Vista. If Wireshark is not currently available on your PC, you can download the Latest Windows Version from [here] Wireshark 1.2.6 Windown Installer. Other Versions of Wireshark from http://www.wireshark.org/download.html. The current version of Wireshark, at time of writing, is version 1.2.6. The initial Wireshark installation screen is shown in Figure1



Welcome to the Wireshark 1.2.1 (32-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

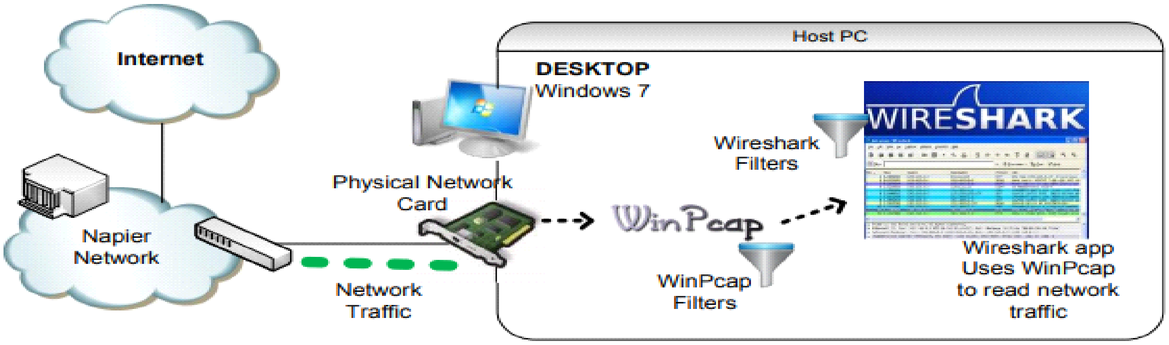
Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Figure 1: Wireshark Installation

Click the I Agree button to the License agreement, then select options (or accept defaults) clicking the Next button on each screen when prompted.

- **Diagrams / Experimental set-up /Work Situation**



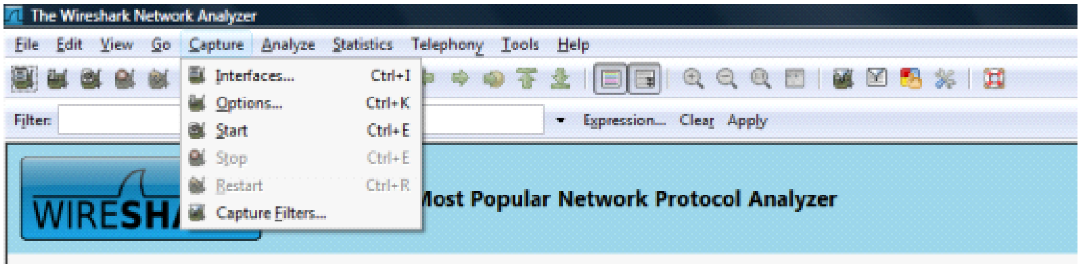
- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Router			
3.	Linux OS			
4.	CORE Network Simulator			

- **Procedure**

Select a Network Interface to Capture Packets through.

Start the Wireshark application. When Wireshark is first run, a default, or blank window is shown. To list the available network interfaces, select the Capture->Interfaces menu option.

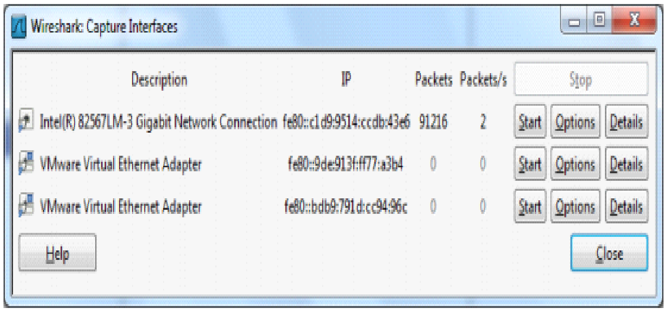


Wireshark should display a popup window such as the one shown in Figure 2. To capture network traffic click the Start button for the network interface you want to capture traffic on. Windows can have a long list of virtual interfaces, before the Ethernet Network Interface Card (NIC).

Questions

Q. Which Interface is connected to a local network (Ethernet)?

Q. How many packets have passed through the interface?



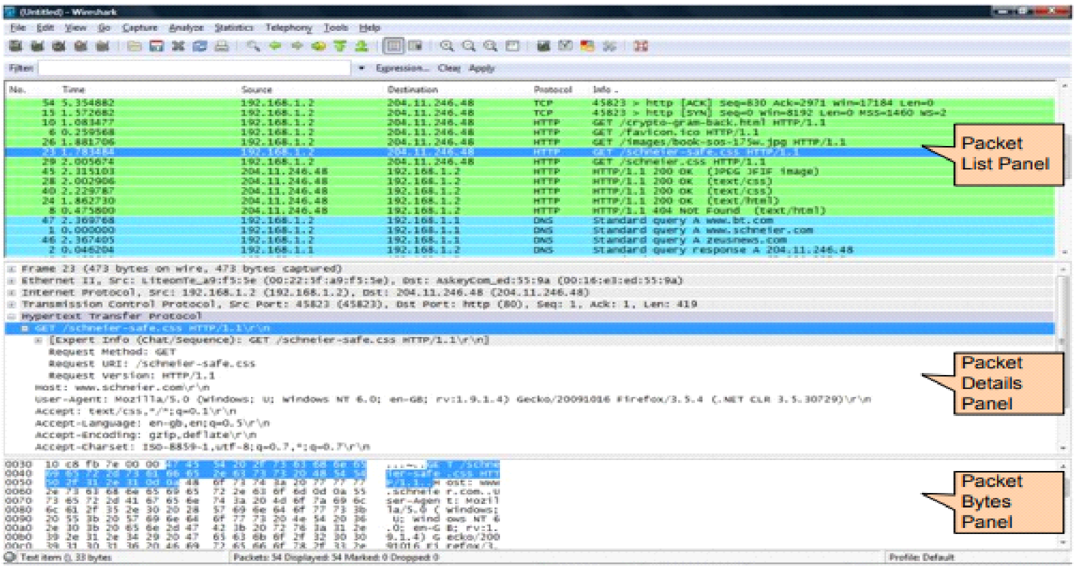
Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop		
Intel(R) 82567LM-3 Gigabit Network Connection	fe80::c1d9:9514:ccdb:43e6	91216	2	Start	Options	Details
VMware Virtual Ethernet Adapter	fe80::9de9:13f:ff77:a3b4	0	0	Start	Options	Details
VMware Virtual Ethernet Adapter	fe80::bdb9:791d:cc94:96c	0	0	Start	Options	Details

Figure 2 - Wireshark Interfaces Window

Note: The total incoming packets, for each interface, are displayed in the column to the left of the Start buttons.

Generate some network traffic with a Web Browser, such as Internet Explorer or Chrome. Your Wireshark window should show the packets, and now look something like



```
No.  Time        Source          Destination     Protocol  Info
 54 5.354882     192.168.1.2     204.11.246.48   TCP       45823 > http [ACK] Seq=830 Ack=2971 Win=17184 Len=0
 15 1.572682     192.168.1.2     204.11.246.48   TCP       45823 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 10 1.083477     192.168.1.2     204.11.246.48   HTTP      GET /crypto-gram-back.html HTTP/1.1
  6 0.259568     192.168.1.2     204.11.246.48   HTTP      GET /favicon.ico HTTP/1.1
 26 1.881706     192.168.1.2     204.11.246.48   HTTP      GET /images/book-sos-175w.jpg HTTP/1.1
 23 1.783484     192.168.1.2     204.11.246.48   HTTP      GET /schneier-safe.css HTTP/1.1
 29 2.005674     192.168.1.2     204.11.246.48   HTTP      GET /schneier.css HTTP/1.1
 45 2.315103     204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (JPEG JFIF image)
 28 2.002906     204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/css)
 40 2.229787     204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/css)
 24 1.862730     204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/html)
  8 0.475800     204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 404 Not Found  (text/html)
 47 2.369768     192.168.1.2     192.168.1.1     DNS       Standard query A www.bt.com
  1 0.000000     192.168.1.2     192.168.1.1     DNS       Standard query A www.schneier.com
 46 2.367405     192.168.1.2     192.168.1.1     DNS       Standard query A zeusnews.com
  2 0.046204     192.168.1.1     192.168.1.2     DNS       Standard query response A 204.11.246.48
```

```
⊞ Frame 23 (473 bytes on wire, 473 bytes captured)
⊞ Ethernet II, Src: LiteonTe_a9:f5:5e (00:22:5f:a9:f5:5e), Dst: AskeyCom_ed:55:9a (00:16:e3:ed:55:9a)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 204.11.246.48 (204.11.246.48)
⊞ Transmission Control Protocol, Src Port: 45823 (45823), Dst Port: http (80), Seq: 1, Ack: 1, Len: 419
⊟ Hypertext Transfer Protocol
  ⊞ GET /schneier-safe.css HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /schneier-safe.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /schneier-safe.css
      Request Version: HTTP/1.1
    Host: www.schneier.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB; rv:1.9.1.4) Gecko/20091016 Firefox/3.5.4 (.NET CLR 3.5.30729)\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: en-gb,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
```

```
0030  10 c8 fb 7e 00 00 47 45  54 20 2f 73 63 68 6e 65   ...~..GE T /schne
0040  69 65 72 2d 73 61 66 65  2e 63 73 73 20 48 54 54   ier-safe .css HTT
0050  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77   P/1.1..H ost: www
0060  2e 73 63 68 6e 65 69 65  72 2e 63 6f 6d 0d 0a 55   .schneie r.com..U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0080  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 3b   la/5.0 ( Windows;
0090  20 55 3b 20 57 69 6e 64  6f 77 73 20 4e 54 20 36    U; Wind ows NT 6
00a0  2e 30 3b 20 65 6e 2d 47  42 3b 20 72 76 3a 31 2e   .0; en-G B; rv:1.
00b0  39 2e 31 2e 34 29 20 47  65 63 6b 6f 2f 32 30 30   9.1.4) G ecko/200
00c0  39 31 30 31 36 20 46 69  72 65 66 6f 78 2f 33 2e   91016 Fi refox/3.
```

```
Text item (), 33 bytes    Packets: 54 Displayed: 54 Marked: 0 Dropped: 0
```

Figure 3 - Wireshark capuring traffic

To stop the capture

Select the Capture->Stop menu option, Ctrl+E, or the Stop toolbar button. What you have created is a Packet Capture or ‘pcap’, which you can now view and analyse using the Wireshark interface, or save to disk to analyse later.

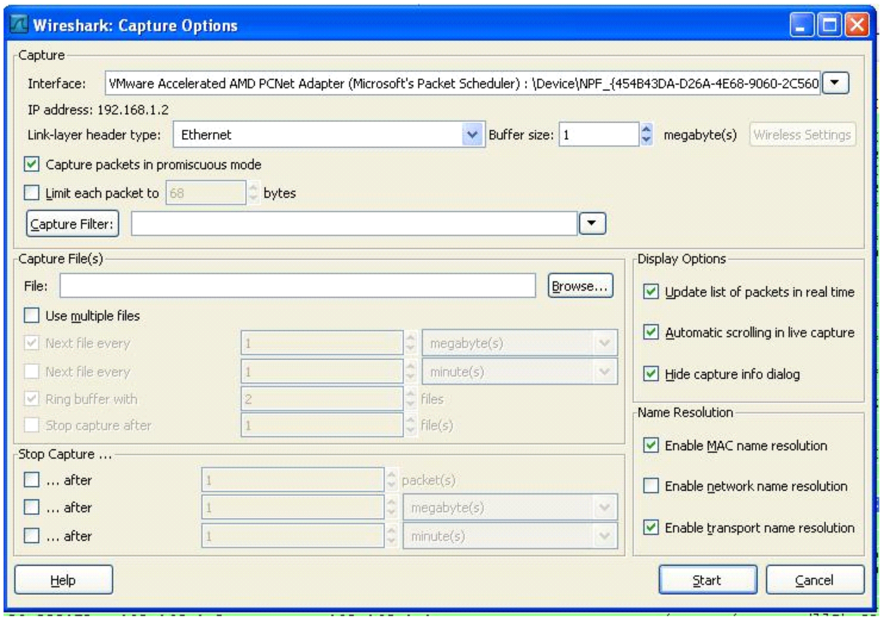
The capture is split into 3 parts:

1. Packet List Panel – this is a list of packets in the current capture. It colours the packets based on the protocol type. When a packet is selected, the details are shown in the two panels below.

2. Packet Details Panel – this shows the details of the selected packet. It shows the different protocols making up the layers of data for this packet. Layers include Frame, Ethernet, IP, TCP/UDP/ICMP, and application protocols such as HTTP.

3. Packet Bytes Panel – shows the packet bytes in Hex and ASCII encodings.

To select more detailed options when starting a capture, select the Capture->Options menu option, or Ctrl+K, or the Capture Options button on the toolbar (the wrench). This should show a window such as shown in Figure 4.



Interface: VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{454B43DA-D26A-4E68-9060-2C560

IP address: 192.168.1.2

Link-layer header type: Ethernet

Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

File:

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

Figure 4 - Wireshark Capture Options

Some of the more interesting options are:

· **Capture Options > Interface** - Again the important thing is to select the correct Network Interface to capture traffic through.

· Capture Options > Capture File – useful to save a file of the packet capture in real time, in case

of a system crash.

· **Display Options > Update** list of packets in real time – A display option, which should be checked if you want to view the capture as it happens (typically switched off to capture straight to a file, for later analysis).

· **Name Resolution > MAC name resolution** – resolves the first 3 bytes of the MAC Address, the

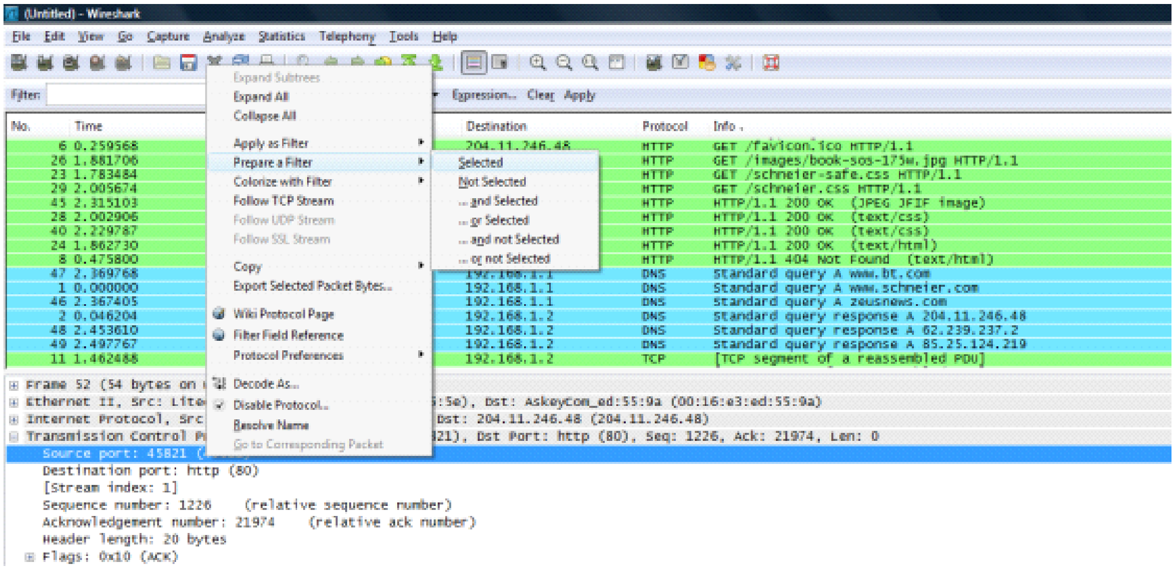
Organisation Unique Identifier (OUI), which represents the Manufacturer of the Card.

· **Name Resolution > Network name resolution** – does a DNS lookup for the IP Addresses captured, to display the network name. Set to off by default, so covert scans do not generate this DNS traffic, and tip off who's packets you are sniffing.

Make sure the MAC name resolution is selected. Start the capture, and generate some Web traffic again, then stop the capture.

Wireshark Display Filters.

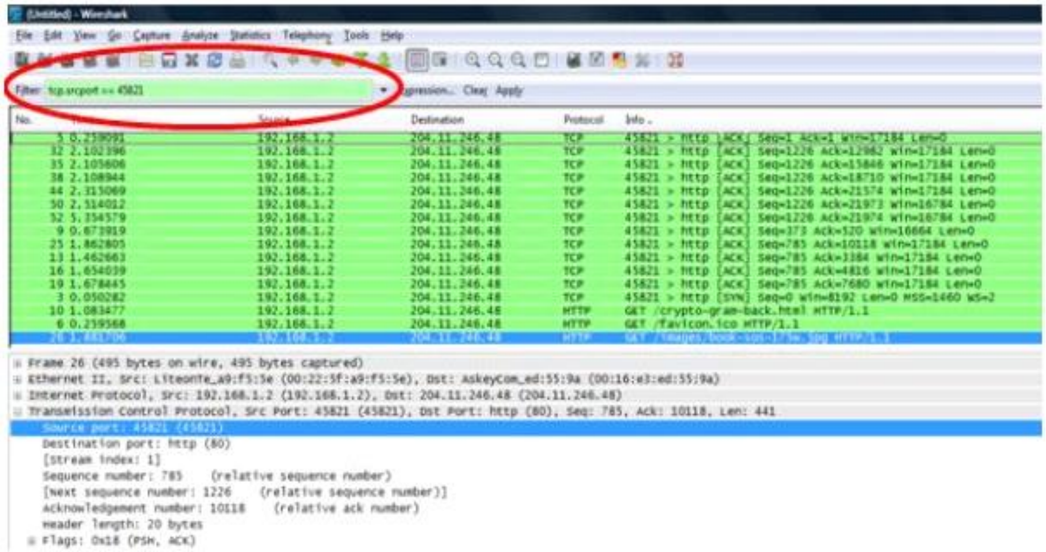
Right click on the Source Port field in the Packet Details Panel. Select Prepare a Filter->Selected



```
No.   Time        Destination      Protocol  Info
  6 0.259568      204.11.246.48    HTTP      GET /favicon.ico HTTP/1.1
 26 1.881706                       HTTP      GET /images/book-sos-175w.jpg HTTP/1.1
 23 1.783484                       HTTP      GET /schneier-safe.css HTTP/1.1
 29 2.005674                       HTTP      GET /schneier.css HTTP/1.1
 45 2.315103                       HTTP      HTTP/1.1 200 OK  (JPEG JFIF image)
 28 2.002906                       HTTP      HTTP/1.1 200 OK  (text/css)
 40 2.229787                       HTTP      HTTP/1.1 200 OK  (text/css)
 24 1.862730                       HTTP      HTTP/1.1 200 OK  (text/html)
  8 0.475800                       HTTP      HTTP/1.1 404 Not Found  (text/html)
 47 2.369768      192.168.1.1      DNS       Standard query A www.bt.com
  1 0.000000      192.168.1.1      DNS       Standard query A www.schneier.com
 46 2.367405      192.168.1.1      DNS       Standard query A zeusnews.com
  2 0.046204      192.168.1.2      DNS       Standard query response A 204.11.246.48
 48 2.453610      192.168.1.2      DNS       Standard query response A 62.239.237.2
 49 2.497767      192.168.1.2      DNS       Standard query response A 85.25.124.219
 11 1.462488      192.168.1.2      TCP       [TCP segment of a reassembled PDU]

⊞ Frame 52 (54 bytes on
⊞ Ethernet II, Src: Lite                 :5e), Dst: AskeyCom_ed:55:9a (00:16:e3:ed:55:9a)
⊞ Internet Protocol, Src                 Dst: 204.11.246.48 (204.11.246.48)
⊟ Transmission Control P                 321), Dst Port: http (80), Seq: 1226, Ack: 21974, Len: 0
    Source port: 45821 (
    Destination port: http (80)
    [Stream index: 1]
    Sequence number: 1226    (relative sequence number)
    Acknowledgement number: 21974    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
```

Figure 5 - Filtering on a protocol field

Wireshark automatically generates a Display Filter, and applies it to the capture. The filter is shown in the Filter Bar, below the button toolbar. Only packets captured with a Source Port of the value selected should be displayed. The window should be similar to that shown in Figure 6. This same process can be performed on most fields within Wireshark, and can be used to include or exclude traffic.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

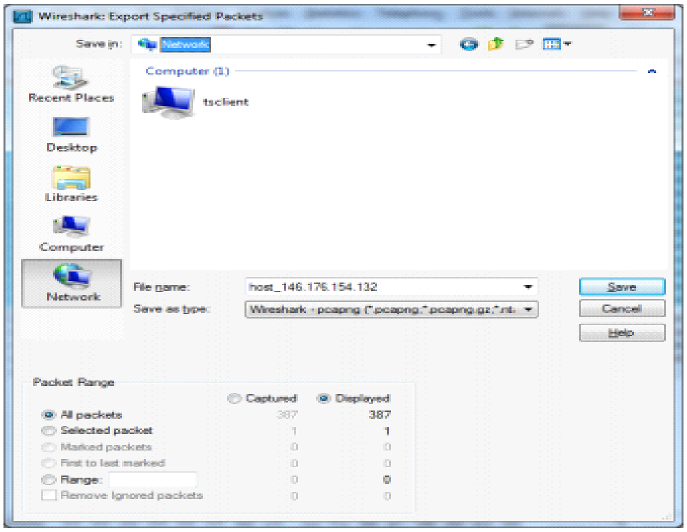
```
Filter: tcp.srcport == 45821

No.   Time        Source           Destination      Protocol  Info
  5 0.259091      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1 Ack=1 Win=17184 Len=0
 32 2.102396      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=12982 Win=17184 Len=0
 35 2.105606      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=15846 Win=17184 Len=0
 38 2.108944      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=18710 Win=17184 Len=0
 44 2.315069      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=21574 Win=17184 Len=0
 50 2.514012      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=21973 Win=16784 Len=0
 52 5.354579      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=1226 Ack=21974 Win=16784 Len=0
  9 0.673919      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=373 Ack=520 Win=16664 Len=0
 25 1.862805      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=785 Ack=10118 Win=17184 Len=0
 13 1.462663      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=785 Ack=3384 Win=17184 Len=0
 16 1.654039      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=785 Ack=4816 Win=17184 Len=0
 19 1.678445      192.168.1.2      204.11.246.48    TCP       45821 > http [ACK] Seq=785 Ack=7680 Win=17184 Len=0
  3 0.050282      192.168.1.2      204.11.246.48    TCP       45821 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 10 1.083477      192.168.1.2      204.11.246.48    HTTP      GET /crypto-gram-back.html HTTP/1.1
  6 0.259568      192.168.1.2      204.11.246.48    HTTP      GET /favicon.ico HTTP/1.1
 26 1.881706      192.168.1.2      204.11.246.48    HTTP      GET /images/book-sos-175w.jpg HTTP/1.1

⊞ Frame 26 (495 bytes on wire, 495 bytes captured)
⊞ Ethernet II, Src: Liteonte_a9:f5:5e (00:22:5f:a9:f5:5e), Dst: AskeyCom_ed:55:9a (00:16:e3:ed:55:9a)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 204.11.246.48 (204.11.246.48)
⊟ Transmission Control Protocol, Src Port: 45821 (45821), Dst Port: http (80), Seq: 785, Ack: 10118, Len: 441
    Source port: 45821 (45821)
    Destination port: http (80)
    [Stream index: 1]
    Sequence number: 785    (relative sequence number)
    [Next sequence number: 1226    (relative sequence number)]
    Acknowledgement number: 10118    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
```

Figure 6 - Wireshark Display Filter

Saving Packet Captures

Often captures should be saved to disc, for later analysis. To save a capture, select File->Save As and save the trace. By default this creates a Wireshark pcapng file, or if you select pcap a file many tools can read and write this. For example a tcpdump output file is in this format and can be read into Wireshark for analysis. This saves all the captured packets to the file. **Paste the display filter** back into the Filter Bar, and Apply it.

To save only the displayed packets, select File-> Export Specified Packets, and make sure the Displayed radio button is selected rather than the Captured option. This creates a pcap file, with only the packets filtered by the current display filter.

- 

File name: host_146.176.154.132

Save as type: Wireshark - pcapng (*.pcapng;*.pcapng.gz;*.nt:

Packet Range

	○ Captured	● Displayed
● All packets	387	387
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	**Name of Resource**	**Specification**
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resources	

- **Result**

……

……

……

………………

- **Practical Related Questions**
  - What is ICMP packet?
  - How to capture ICMPv4 packet?
  - What is Wireshark?
  - State any four Wireshark Capture Options
- **Exercise**

  Student should setup Wireshark and Capture the packets of different protocol

(Space for Answer)

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

…………………………………………………………………………………………...…..

……………………………………………………………………………………………………

…………………………………………………………………

…………………………………………………………………………..……………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

....

....

....

....

....

....

....

....

....

....

....

....

....

....

- **References/ Suggestions for further Reading**

  https://www.wireshark.org/

  http://www.networksorcery.com/enp/protocol/icmp.htm

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

………………………………………………..

………………………………………………..

…………………………………………..........

………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.02: Create IPv6 environment in a small network using simulator

- **Practical Significance**

  Know the use IPv6

  Create IPv6 Environment

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.

- **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**
  - Create IPv6 Environment using simulator
- **Relevant Course Outcomes**

  Configure IPv6 Network
- **Practical Outcomes (POs)**

  IPv6 environment
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Proposition 1.

The characteristics of IPv6

- **Larger address space:** Increased address size from 32 bits to 128 bits
- **Streamlined protocol header:** Improves packet-forwarding efficiency
- **Stateless autoconfiguration:** The ability for nodes to determine their own address
- **Multicast:** Increased use of efficient one-to-many communications
- **Jumbograms:** The ability to have very large packet payloads for greater efficiency
- **Network layer security:** Encryption and authentication of communications
- **Quality of service (QoS) capabilities:** QoS markings of packets and flow labels that help identify priority traffic
- **Anycast:** Redundant services using nonunique addresses
- **Mobility:** Simpler handling of mobile or roaming nodes

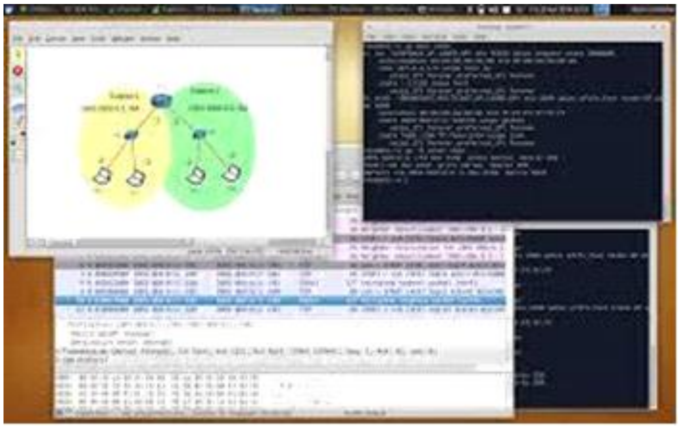


Fig.IPV6 addressing in a network simulator

- **Diagrams / Experimental set-up /Work Situation**

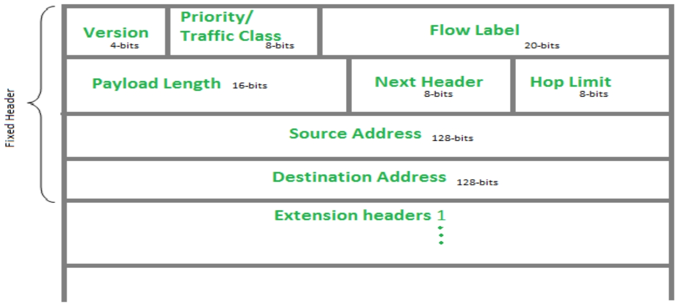


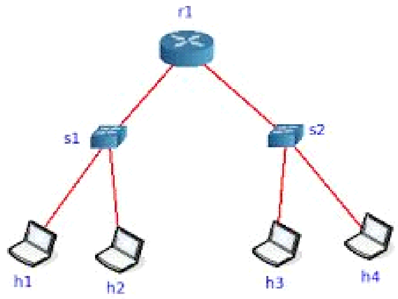
Fig. IPv6 Header

- **Resources Required**

Sr.No	**Name of Resource**	**Specification**	**Quantity**	**Remarks/Use**
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	CORE Network Simulator			

- **Procedure**

Set up the network configuration

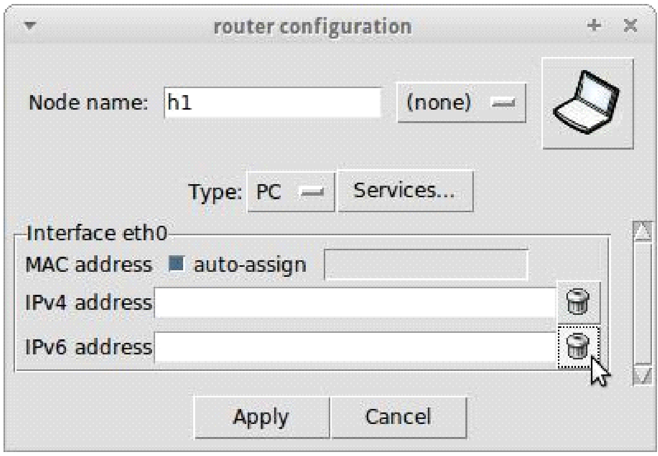


Use the CORE Network Simulator to set up the network shown in the diagram below with one router, two switches, and four hosts. We will investigate IPv6 addressing fundamentals using this simple network.

To make the network diagram easier to read, use the View → Show menu command to hide all information except node names (to clean up the display). Also, you can click on Selection Tool and grab the text that represents each node name and move it to a spot where it is not hidden by the link. Then, use the Configure right-click menu command on each node to change the node name so that the network look like the following image:

Configure the simulated nodes

We want to study the same procedures we would use in a real network without allowing the CORE Network Emulator to set the network configurations for us, so we will clear the IP addresses that the CORE Network Emulator configures by default on every interface before starting the simulation.



Node name: h1 (none)

Type: PC

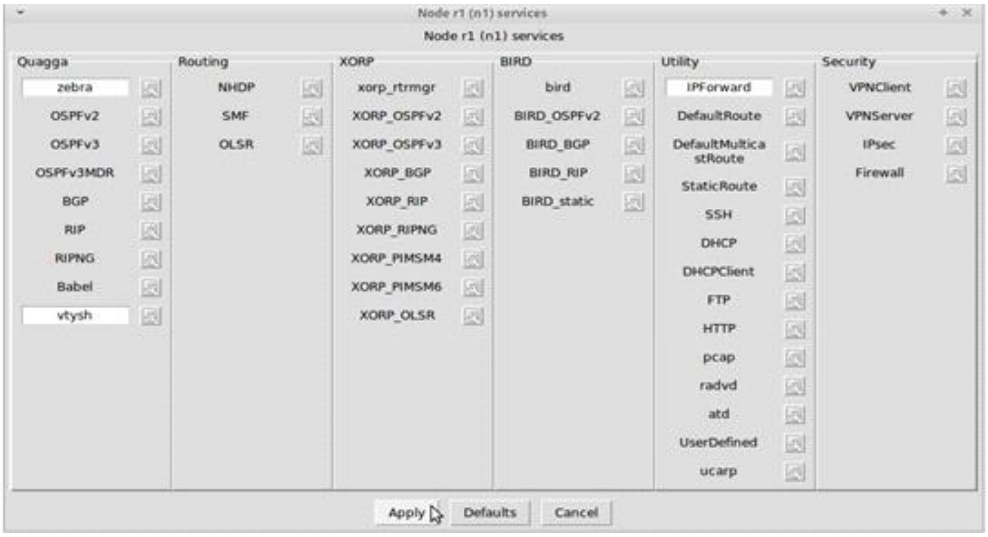
MAC address ■ auto-assign

IPv4 address

IPv6 address

Right-click on each router and host and select the Configure contextual menu command. Then, clear the IPv4 address and IPv6 address field on every node.

Also, since we will not use dynamic routing in this scenario, we will change the settings on the router r1 so that dynamic routing protocols are not started when the node starts up.



In the Configure dailogue box, after clearing the IP addresses on both of the router's interfaces, click on the Services… button, then clear the OSPFv2 and OSPFv3 services. Also clear the radvd service (because we will explore stateless address auto configuration in a later post). Then press the Apply button.

Start the simulation

Start the network emulation by clicking in the *start the session* icon in the tool bar or by clicking on the menu command, *Session → Start*.

Examine the link-local unicast IPv6 addresses

After we start the network simulation we created, we expect to observe that the interfaces on each simulated router and on each simulated host have link-local IPv6 addresses automatically configured.

We will also run some simple network tests and observe the results. With the current configuration, nodes on the same link should be able to communicate with each other but nodes that are separated by the router should not be able to communicate with each other1. For example, host *h1* should be able to ping host *h2*, but not host *h4*.

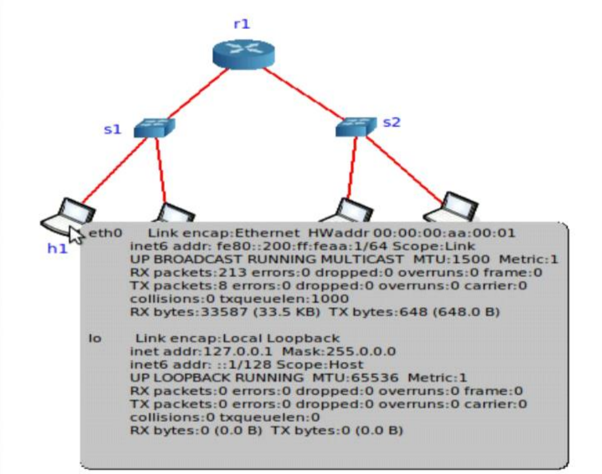
Link-local unicast IPv6 address, defined

When an IPv6 interface starts up, it is required to automatically configure itself with a *link-local*unicast IPv6 address2. Link-local IPv6 addresses consist of a specific 64-bit IPv6 prefix, fe80::/64, and a unique 64-bit *interface identifier* derived from the MAC address of the interface3.

Link-Local unicast IPv6 addresses are created for purposes such as auto-address configuration and neighbor discovery on a single link. A link may be a point-to-point connection between two interfaces or a switched layer-2 domain such as an Ethernet network.

Link-local unicast addresses only work on the link on which they are configured because IPv6 routers are required to not forward any packets with link-local source or destination addresses to other links.

Using the *ifconfig* Observer Widget



```
eth0    Link encap:Ethernet  HWaddr 00:00:00:aa:00:01
        inet6 addr: fe80::200:ff:feaa:1/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:213 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:33587 (33.5 KB)  TX bytes:648 (648.0 B)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

We can use the Core Network*Observer*Emulator's*Widget*toolto view the interface configuration on each node and take note of the IPv6 address on each interface. Click on the Observer Widget tool (the magnifying glass icon in the toolbar) and select the *ifconfig* widget. Then, hover the mouse pointer over each node to see the displayed interface configuration.

Using the *ip* command

Alternatively, we can open up a terminal window on each node running in the simulated network and use normal Linux
commands to view the configuration
Double-click on any node to open a terminal window (for example, host *h1*). Then, execute the command.

Record all IPv6 addresses

Write down the IP addresses and MAC addresses on each node in a table for future reference. This will be useful when we are running programs like *ping* where we need to know the IPv6 address of the destination node. Knowing the MAC addresses is useful when we are analyzing packets in the *Wireshark* protocol analyzer.

In our example, the CORE Network Emulator assigns MAC addresses, in numerical order4, starting with 00:00:00:aa:00:00 and incrementing by one for every other interface attached to a link.
After inspecting each node using either the *Observer Widget* or the Linux *ip* command, we generate the following table:

Node name	Interface	MAC address	IPv6 addresses
Router *r1*	**eth0**	**00:00:00:aa:00:00**	**fe80::200:ff:feaa:0/64**
	eth1	**00:00:00:aa:00:03**	**fe80::200:ff:feaa:3/64**
Host *h1*	**eth0**	**00:00:00:aa:00:01**	**fe80::200:ff:feaa:1/64**
Host *h2*	**eth0**	**00:00:00:aa:00:02**	**fe80::200:ff:feaa:2/64**

Host *h3*	**eth0**	**00:00:00:aa:00:04**	**fe80::200:ff:feaa:4/64**
Host *h4*	**eth0**	**00:00:00:aa:00:05**	**fe80::200:ff:feaa:5/64**

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resources	

- **Result**

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………

- **Practical Related Questions**
  - Differentiate between IPv4 and IPv6
  - Explain IPv6 Packet Format
  - List the characteristics of IPv6.
  - What is IPV6 address?
  - What is network simulator?
- **Exercise**

Student should setup IPv6 Environment using Simulator

(Space for Answer)

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

……..…..……………………………………………………………………………………

……………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

…………………………………………

………………………………………………………………………………………………

……

- **References/ Suggestions for further Reading**

  https://getipv6.info/display/IPv6/Educating+Yourself+about+IPv6

  http://www.brianlinkletter.com/tag/core/

- **Assessment Scheme**

Performance indicator	**Weightage**
Process Related(35 Marks)	**75%**

1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

………………………………………………..

………………………………………………..

………………………………………….........

………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.03: Configure IP routing with RIP using relevant software

- **Practical Significance**

  Student should be able to Configure IP routing with RIP using relevant software

- **Relevant Programs Outcomes (POs)**

  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.

- **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**
  - Ability configure IP routing
  - Ability to understand concept of RIP.
- **Relevant Course Outcomes**

  Choose routing protocol in the given network situation

- **Practical Outcomes (POs)**

  Understand configuration of RIP
  Understand configuration of IP routing
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Proposition 1. RIP Overview

The Routing Information Protocol (RIP) uses broadcast UDP data packets to exchange routing information. Cisco software sends routing information updates every 30 seconds, which is termed advertising. If a device does not receive an update from another device for 180 seconds or more, the receiving device marks the routes served by the nonupdating device as unusable. If there is still no update after 240 seconds, the device removes all routing table entries for the nonupdating device.A device that is running RIP can receive a default network via an update from another device that is running RIP, or the device can source the default network using RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

Features of RIP Routing Protocol

Some of the of key features of RIP protocol are:

- It supports maximum 15 hops in a path.

- It uses hops count metric to calculate the best path from a source to a destination network.
- It sends routing updates (entire routing table) after every 30 seconds and when the network changes.
- It uses UDP broadcast packets to exchange routing information.
- The Administrative Distance (AD) value of the RIP protocol is 120.
- It has two versions: RIPv1 and RIPv2.

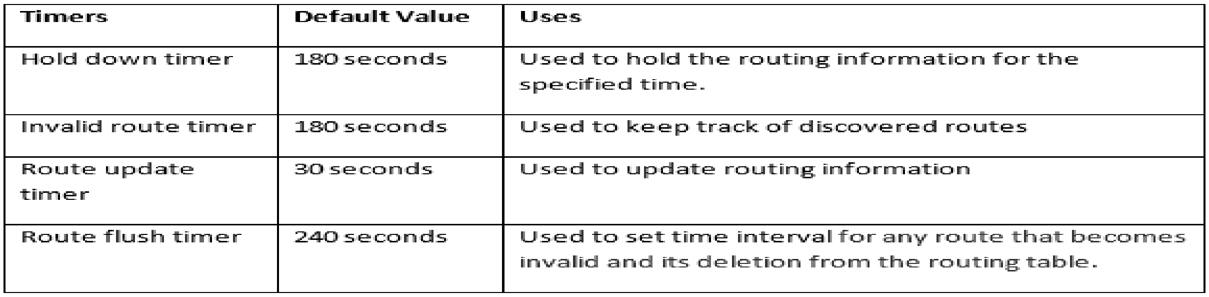
Routing Loops

If you want to configure RIP protocol on your network, you have to be familiar with the routing loops. Sometimes routing loops create a big issue on an RIP-based network. However, RIP protocol has some mechanisms that can be used to prevent the routing loops and maintain the network stability. These mechanisms are:

- **Split horizon:** In the split horizon, route information is not sent back out through the interface from which it was received. Thus, allowing to prevent routing loops.
- **Hop-count limit:** Limiting the hop-count prevents routing loops from continuing indefinitely.
- **Poison reverse:** In this mechanism, a router marks a route (that is not accessible) as unreachable and set the hop count to 16. The router then passes this route out to the neighbor router, and the neighbor router removes the unreachable route from its routing table.
- **Hold-down timers:** When the hold-down timers are set, routers ignore the routing update information for the set period of time.

RIP Timers

Routing protocols use timers to optimize the network performance. The following table lists the various types of timers used by the RIP protocol to optimize the network performance.

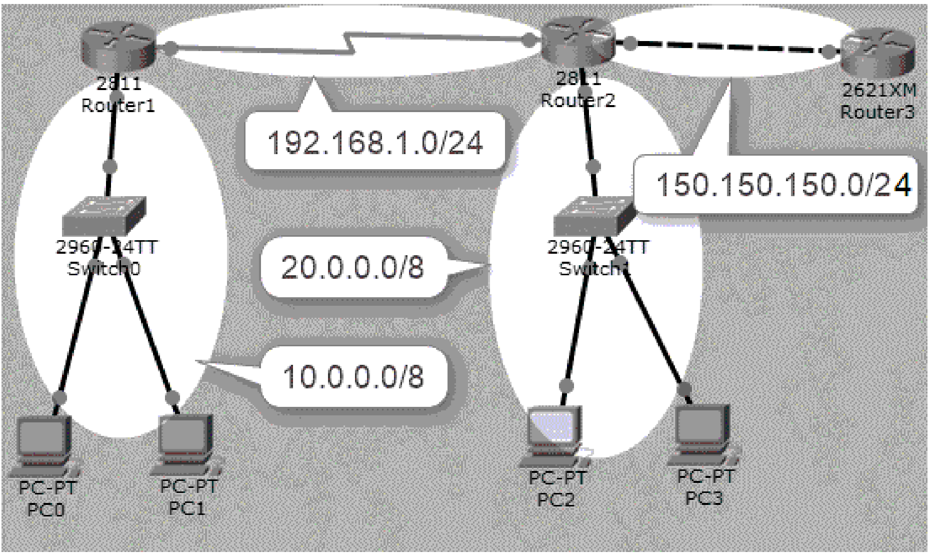


Timers	Default Value	Uses
Hold down timer	180 seconds	Used to hold the routing information for the specified time.
Invalid route timer	180 seconds	Used to keep track of discovered routes
Route update timer	30 seconds	Used to update routing information
Route flush timer	240 seconds	Used to set time interval for any route that becomes invalid and its deletion from the routing table.

- **Diagrams / Experimental set-up /Work Situation**

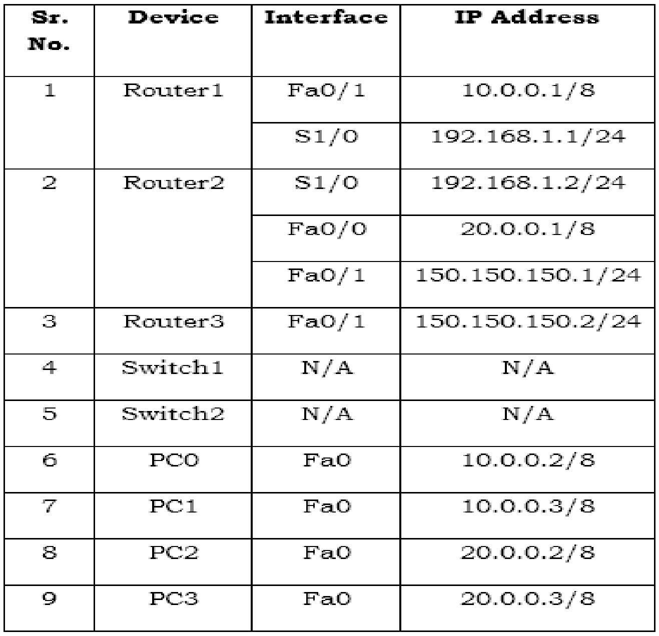
RIP Configuration

To demonstrate how to **configure RIP in Cisco Packet Tracer**, we will use the following network topology. If you are using a simulator, such as Cisco Packet Tracer or GNS3, create the following topology and configure the IP addresses as mentioned in the topology.



.

If you are using a simulator, such as Cisco Packet Tracer or GNS3, create the preceding topology and configure the devices as per the values mentioned in the following table



Sr. No.	Device	Interface	IP Address
1	Router1	Fa0/1	10.0.0.1/8
		S1/0	192.168.1.1/24
2	Router2	S1/0	192.168.1.2/24
		Fa0/0	20.0.0.1/8
		Fa0/1	150.150.150.1/24
3	Router3	Fa0/1	150.150.150.2/24
4	Switch1	N/A	N/A
5	Switch2	N/A	N/A
6	PC0	Fa0	10.0.0.2/8
7	PC1	Fa0	10.0.0.3/8
8	PC2	Fa0	20.0.0.2/8
9	PC3	Fa0	20.0.0.3/8

For example, to configure TCP/IP addresses on Router1, execute the following commands:

Router1(config)#interface fa0/1

Router1(config-if)#ip add 10.0.0.1 255.0.0.0

Router(config-if)#no shut

Router1(config-if)#exit

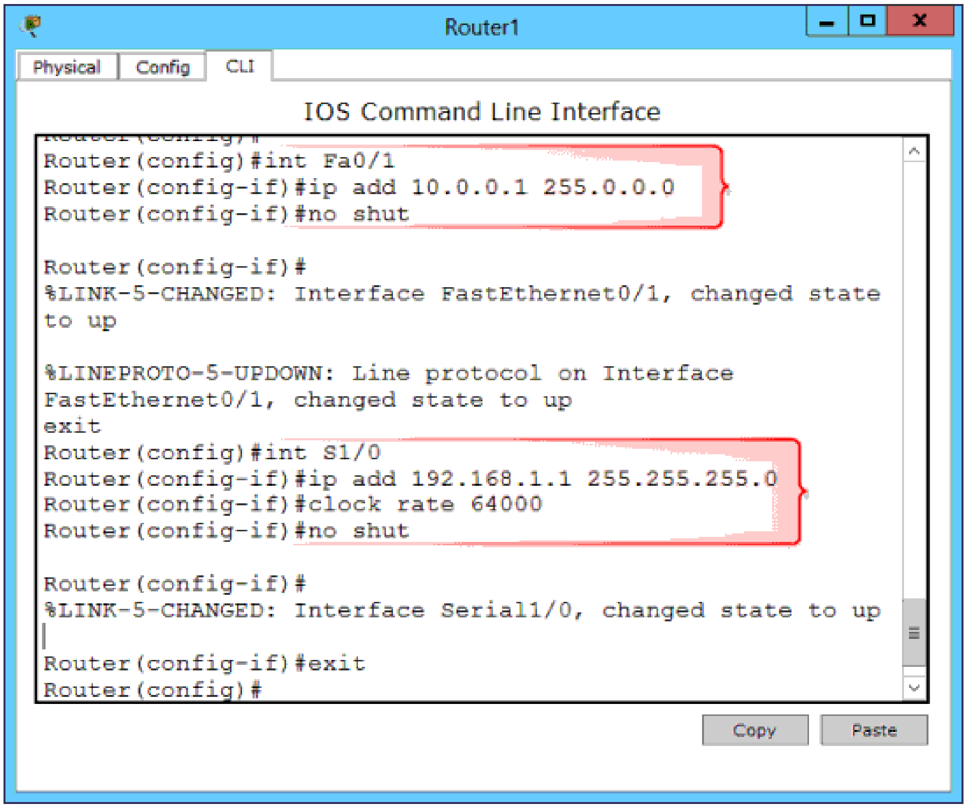
Router1(config)#interface S1/0

Router1(config-if)#ip add 192.168.1.1 255.255.255.0

Router1(config-if)#clock rate 64000

Router(config-if)#no shut

The following figure shows the IP configuration of Router1.



```
Router(config)#
Router(config)#int Fa0/1
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
exit
Router(config)#int S1/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial1/0, changed state to up

Router(config-if)#exit
Router(config)#
```

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		
3.	Crossover Cable			

- **Procedure**

Steps to Configure RIP Routing

Once you have configured the appropriate IP addresses on each device, perform the following steps to configure RIP routing. The default version of RIP is RIPv1. In the later section, we will also configure RIPv2 routing.

- On **Router1**, execute the following commands to configure **RIP** routing.

```
Router1(config)#router rip
Router1(config-router)#network 10.0.0.0
Router1(config-router)#network 192.168.1.0
Router1(config-router)#exit
```

1. On **Router2**, execute the following commands to configure **RIP** routing.

```
Router2(config)#router rip
Router2(config-router)#network 20.0.0.0
Router2(config-router)#network 192.168.1.0
Router2(config-router)#network 150.150.150.0
Router2(config-router)#exit
Router2(config)#
```

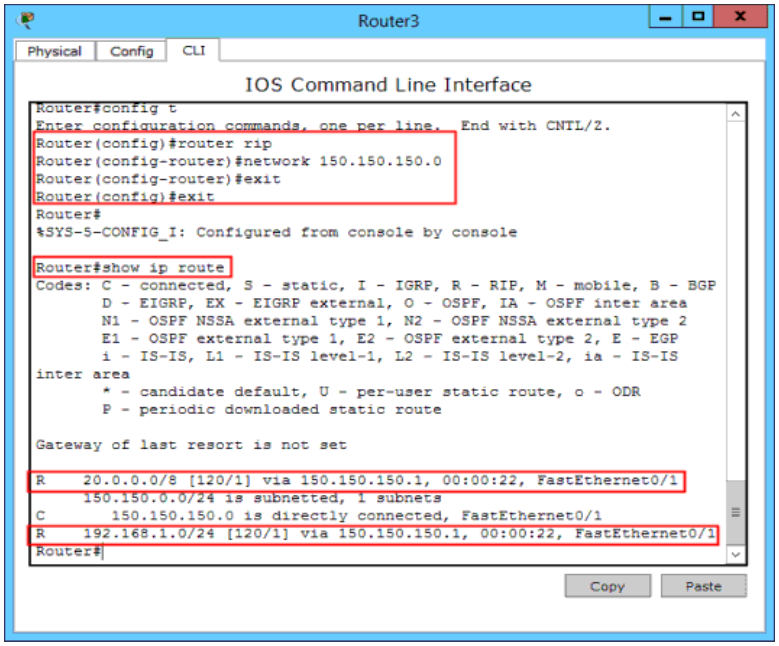
1. On **Router3**, execute the following commands to configure **RIP** routing.

```
2. Router3(config)#router rip
3. Router3(config-router)#network 150.150.150.0
   Router3(config-if)#exit
```

1. Once you have configured RIP routing protocol on each router, wait for a few seconds (let complete the convergence process), and then execute the **show ip route** command on any router to show the routing information.

```
Router(config)#do show ip route
```

1. In the following figure, you can see the routes learned by the RIP protocol on Router3.



```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 150.150.150.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    20.0.0.0/8 [120/1] via 150.150.150.1, 00:00:22, FastEthernet0/1
     150.150.0.0/24 is subnetted, 1 subnets
C       150.150.150.0 is directly connected, FastEthernet0/1
R    192.168.1.0/24 [120/1] via 150.150.150.1, 00:00:22, FastEthernet0/1
Router#
```

Verifying RIP Configuration

To verify and test the RIP configuration, perform the following steps:

- To verify which routing protocol is configured, use the **show ip protocols** command.

Router#show ip protocols

1. To view the RIP messages being sent and received, use the **debug ip rip** command.

Router#debug ip rip

1. To stop the debugging process, use the **undebug all** command.

Router#undebug all

Removing RIP Routing Configuration

If you have added a wrong network or route, you can remove that network from the routing table. In this section, we will learn how to remove the routes learned by the RIP protocol. To do this, perform the following tasks.

- On **Router1**, execute the following commands.

Router1(config)#router rip

Router1(config-router)#no network 10.0.0.0

Router1(config-router)#no network 192.168.1.0

Router1(config-router)#exit

- On **Router2**, execute the following commands.

Router2(config)#router rip

```
Router2(config-router)#no network 20.0.0.0
Router2(config-router)#no network 192.168.1.0
Router2(config-router)#no network 150.150.150.0
Router2(config-router)#exit
```

- On **Router3**, execute the following commands.

```
Router3(config)#router rip
Router3(config-router)#no network 150.150.150.0
Router3(config-router)#exit
```

Now, execute the **show ip route** command and verify that the routes learned by the RIP routing protocol are deleted. If the routes are still available in the routing table, execute the **clear ip route *** command.

Enabling RIP and Configuring RIP Parameters

SUMMARY STEPS

1. enable
2. configure terminal
3. router rip
4. network ip-address
5. neighbor ip-address
6. offset-list [access-list-number | access-list-name] {in | out} offset [interface-type interface-number]
7. timers basic update invalid holddown flush [sleeptime]
8. end

- **Precaution**
    - Handle Computer System and peripherals with care
    - Follow Safety Practices
- **Resources Used**

Sr.No	**Name of Resource**	**Specification**
1.	Crossover Cable	
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
3.	Switch (min. 8 ports)	8 ports
4.	Any other Resource	

- **Result/Conclusion**

……

……

……

………

- **Practical Related Questions**
    - List Applications of RIP
    - Why do we use RIP
    - How RIP works?
- **Exercise**
    - Configure RIP

(Space for Answer)

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……………………………………………………………………………

……

……

……

……

....

....

....

....

....

....

....

....

....

....

- **References/ Suggestions for further Reading**

  https://www.certificationkits.com/ccna-concept-routing-information-protocol-rip/

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

  ……………………………………………..

  ……………………………………………..

  ……………………………………….........

Marks Obtained			Dated Signature of Teacher
Process Related(35)	**Product Related (15)**	**Total(50)**	

……………………………………………..

Practical No.04: Configure IP routing with OSPF using relevant software

- **Practical Significance**

  Know the use of OFPF

  Configure OFPF **(**Open Shortest Path First)

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**
  - Create OSPF Environment using software
- **Relevant Course Outcomes**

  Implement different Network Layer Protocol

- **Practical Outcomes (POs)**

  Understand configuration of OSPF

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

OSPF (Open Shortest Path First) is a link state routing protocol. Because it is an open standard, it is implemented by a variety of network vendors. OSPF will run on most routers that doesn't necessarily have to be Cisco routers (unlike EIGRP which can be run only on Cisco routers).

Here are the most important features of OSPF:

- a classless routing protocol
- supports VLSM, CIDR, manual route summarization, equal cost load balancing
- incremental updates are supported
- uses only one parameter as the metric – the interface cost.
- the administrative distance of OSPF routes is, by default, 110.
- uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates.

Routers running OSPF have to establish neighbor relationships before exchanging routes. Because OSPF is a link state routing protocol, neighbors don't exchange routing tables. Instead, they exchange information about network topology. Each OSFP router then runs SFP algorithm to calculate the best routes and adds those to the routing table. Because each router knows the entire topology of a network, the chance for a routing loop to occur is minimal.

Each OSPF router stores routing and topology information in three tables:

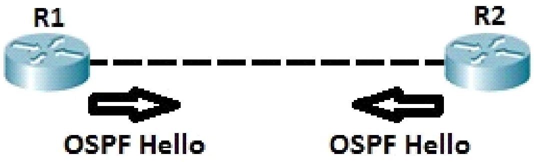
- **Neighbor table** – stores information about OSPF neighbors
- **Topology table** – stores the topology structure of a network
- **Routing table** – stores the best routes

VIII. Diagrams / Experimental set-up /Work Situation

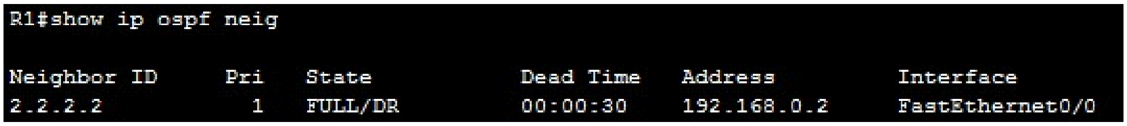
OSPF neighbors

OSPF routers need to establish a neighbor relationship before exchanging routing updates. OSPF neighbors are dynamically discovered by sending Hello packets out each OSPF-enabled interface on a router. Hello packets are sent to the multicast IP address of 224.0.0.5.

The process is explained in the following figure:



Routers R1 and R2 are directly connected. After OSFP is enabled both routers send Hellos to each other to establish a neighbor relationship. You can verify that the neighbor relationship has indeed been established by typing the *show ip ospf neighbors* command.



```
R1#show ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:30    192.168.0.2     FastEthernet0/0
```

In the example above, you can see that the router-id of R2 is 2.2.2.2. Each OSPF router is assigned a router ID. A router ID is determined by using one of the following:

1. using the router-id command under the OSPF process.
2. using the highest IP address of the router's loopback interfaces.
3. using the highest IP address of the router's physical interfaces.

The following fields in the Hello packets must be the same on both routers in order for routers to become neighbors:

- subnet
- area id
- hello and dead interval timers
- authentication
- area stub flag
- MTU

By default, OSPF sends hello packets every 10 second on an Ethernet network (Hello interval). A dead timer is four times the value of the hello interval, so if a routers on an Ethernet network doesn’t receive at least one Hello packet from an OSFP neighbor for 40 seconds, the routers declares that neighbor to be down.

OSPF neighbor states

Before establishing a neighbor relationship, OSPF routers need to go through several state changes. These states are explained below.

1. Init state – a router has received a Hello message from the other OSFP router

2. 2-way state – the neighbor has received the Hello message and replied with a Hello message of his own

3. Exstart state – beginning of the LSDB exchange between both routers. Routers are starting to exchange link state information.

4. Exchange state – DBD (Database Descriptor) packets are exchanged. DBDs contain LSAs headers. Routers will use this information to see what LSAs need to be exchanged.

5. Loading state – one neighbor sends LSRs (Link State Requests) for every network it doesn’t know about. The other neighbor replies with the LSUs (Link State Updates) which contain information about requested networks. After all the requested information have been received, other neighbor goes through the same process

6. Full state – both routers have the synchronized database and are fully adjacent with each other.

OSPF areas

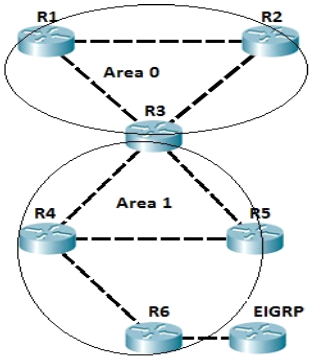
OSPF uses the concept of areas. An area is a logical grouping of contiguous networks and routers. All routers in the same area have the same topology table, but they don’t know about routers in the other areas. The main benefits of creating areas is that the size of the topology and the routing table on a router is reduced, less time is required to run the SFP algorithm and routing updates are also reduced.

Each area in the OSPF network has to connect to the backbone area (area 0). All router inside an area must have the same area ID to become OSPF neighbors. A router that has interfaces in more than one area (area 0 and area 1, for example) is called **Area Border Router (ABR)**. A router that connects an OSPF network to other routing domains (EIGRP network, for example) is called **Autonomous System Border Router (ASBR)**.

NOTE

In OSPF, manual route summarization is possible only on ABRs and ASBRs.

To better understand the concept of areas, consider the following example.



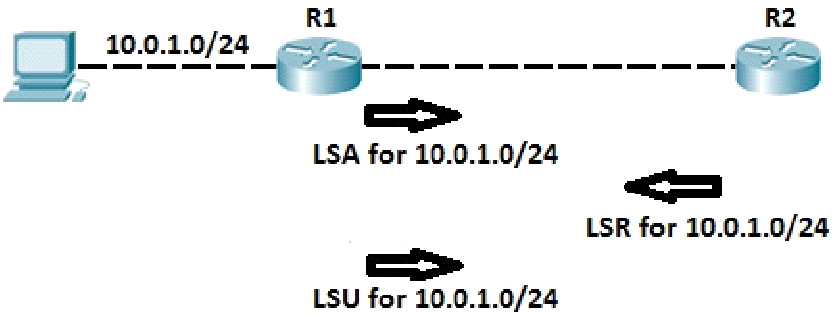
All routers are running OSPF. Routers R1 and R2 are inside the backbone area (area 0). Router R3 is an ABR, because it has interfaces in two areas, namely area 0 and area 1. Router R4 and R5 are inside area 1. Router R6 is an ASBR, because it connects OSFP network to another routing domain (an EIGRP domain in this case). If the R1's directly connected subnet fails, router R1 sends the routing update only to R2 and R3, because all routing updates all localized inside the area.

NOTE

The role of an ABR is to advertise address summaries to neighboring areas. The role of an ASBR is to connect an OSPF routing domain to another external network (e.g. Internet, EIGRP network…). **LSA, LSU and LSR**

The **LSAs (Link-State Advertisements)** are used by OSPF routers to exchange topology information. Each LSA contains routing and toplogy information to describe a part of an OSPF network. When two neighbors decide to exchange routes, they send each other a list of all LSAa in their respective topology database. Each router then checks its topology database and sends a Link State Request (LSR) message requesting all LSAs not found in its topology table. Other router responds with the Link State Update (LSU) that contains all LSAs requested by the other neighbor.

The concept is explained in the following example:



After configuring OSPF on both routers, routers exchange LSAs to describe their respective topology database. Router R1 sends an LSA header for its directly connected network 10.0.1.0/24. Router R2 check its topology database and determines that it doesn't have information about that network. Router R2 then sends Link State Request message requesting further information about that network. Router R1 responds with Link State Update which contains information about subnet 10.0.1.0/24 (next hop address, cost…).

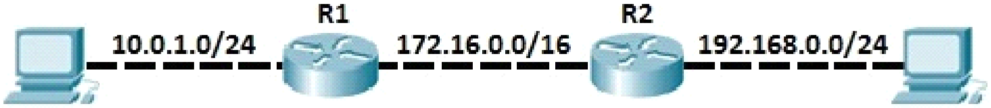
Configuring OSPF 1

OSPF basic configuration is very simple. Just like with other routing protocols covered so far (RIP, EIGRP) first you need to enable OSPF on a router. This is done by using the *routerospf PROCESS-ID* global configuration command. Next, you need to define on which interfaces OSPF will run and what networks will be advertised. This is done by using the *network IP_ADDRESS WILDCARD_MASK AREA_ID* command from the ospf configuration mode.

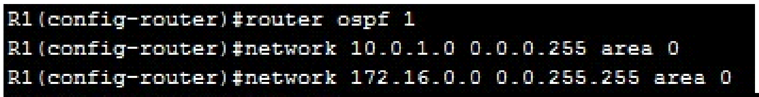
NOTE

The OSPF process number doesn't have to be the same on all routers in order to establish a neighbor relationship, but the Area ID has to be the same on all neighboring routers in order for routers to become neighbors.

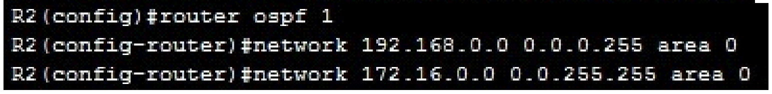
Let's get started with some basic OSPF configuration. We will use the following network topology:



First, we need to enable OSPF on both routers. Then we need to define what network will be advertised into OSPF. This can be done by using the following sequence of commands on both routers:

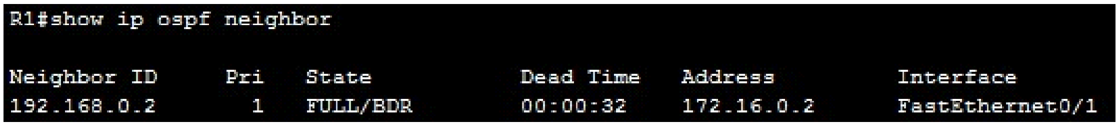


```
R1(config-router)#router ospf 1
R1(config-router)#network 10.0.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.0.0 0.0.255.255 area 0
```



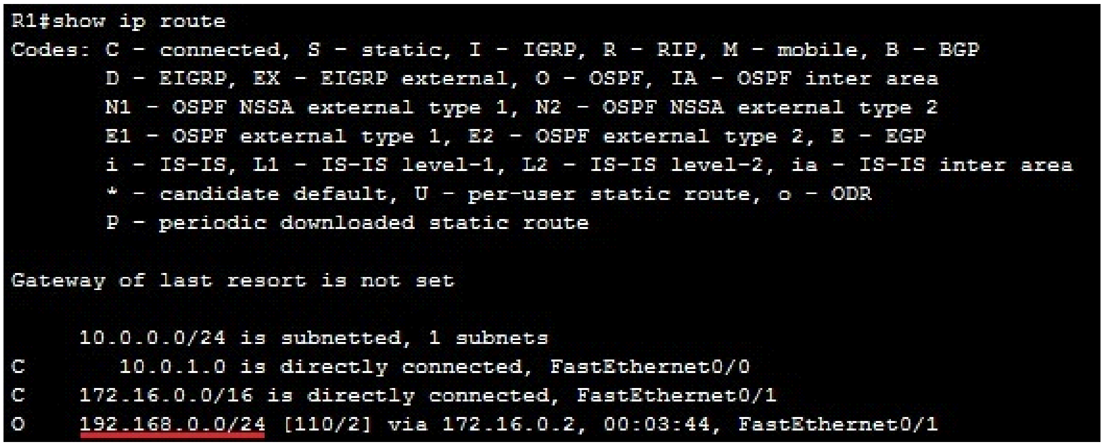
```
R2(config)#router ospf 1
R2(config-router)#network 192.168.0.0 0.0.0.255 area 0
R2(config-router)#network 172.16.0.0 0.0.255.255 area 0
```

The *network* commands entered on both routers include subnets directly connected to both routers. We can verify that the routers have become neighbors by typing the *show ip ospf neighbors* command on either router:



```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.0.2       1   FULL/BDR        00:00:32    172.16.0.2      FastEthernet0/1
```

To verify if the routing updated were exchanged, we can use the *show ip route* command. All routes marked with the character **O** are OSPF routes. For example, here is the output of the command on R1:



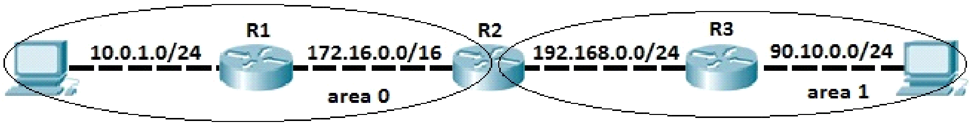
```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/1
O    192.168.0.0/24 [110/2] via 172.16.0.2, 00:03:44, FastEthernet0/1
```

You can see that R1 has learned about the network 192.168.0.0/24 through OSPF.

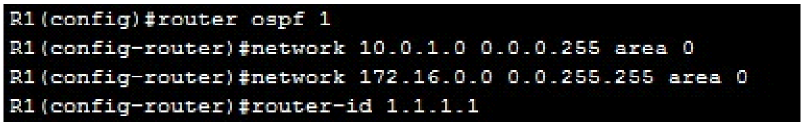
Configuring OSPF 2

Although basic OSPF configuration can be very simple, OSPF provides many extra features that can get really complex. In this example, we will configure multiarea OSPF network and some other OSPF features.

Consider the following multiarea OSPF network:



In this example we have two OSPF areas – area 0 and area 1. As you can see from the network topology depicted above, routers R1 and R3 are in the area 0 and area 1, respectively. Router 2 connects to both areas, which makes him an **ABR (Area Border Router)**. Our goal is to advertise the subnets directly connected to R1 and R3. To do that, the following configuration on R1 will be used:



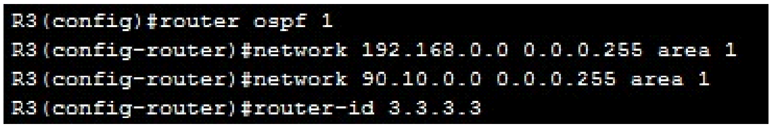
```
R1(config)#router ospf 1
R1(config-router)#network 10.0.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.0.0 0.0.255.255 area 0
R1(config-router)#router-id 1.1.1.1
```

NOTE

We have used the **router-id 1.1.1.1** command to manually specify the router ID of this router. OSPF process will use that RID (router-id) when communicating with other OSPF neighbors.

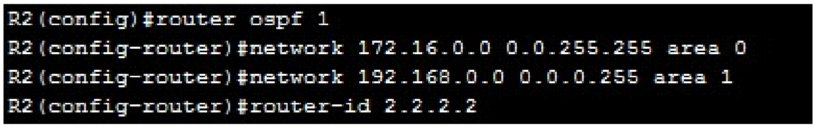
Because R1 connects only to R2, we only need to establish a neighbor relationship with R2 and advertise directly connected subnet into OSPF.

Configuration of R3 looks similar, but with one difference, namely area number. R3 is in the area 1.



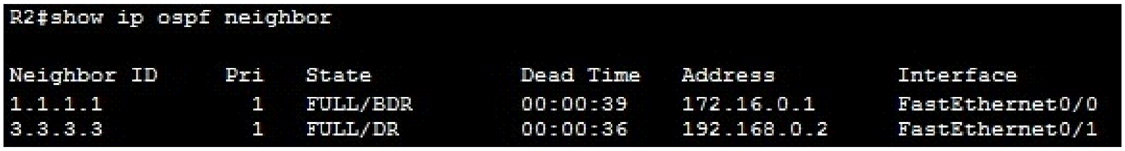
```
R3(config)#router ospf 1
R3(config-router)#network 192.168.0.0 0.0.0.255 area 1
R3(config-router)#network 90.10.0.0 0.0.0.255 area 1
R3(config-router)#router-id 3.3.3.3
```

What about R2? Well, because R2 is an ABR, we need to establish neighbor relationship with both R1 and R3. To do that, we need to specify different area ID for each neighbor relationship, 0 for R1 and 1 for R2. We can do that using the following sequence of commands:



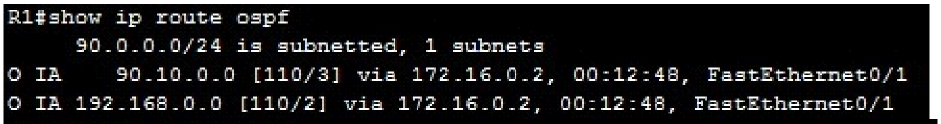
```
R2(config)#router ospf 1
R2(config-router)#network 172.16.0.0 0.0.255.255 area 0
R2(config-router)#network 192.168.0.0 0.0.0.255 area 1
R2(config-router)#router-id 2.2.2.2
```

Now R2 should have neighbor relationship with both R1 and R3. We can verify that by using the *show ip ospf neighbor* command:

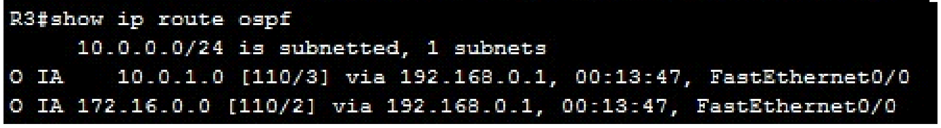


```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:39    172.16.0.1      FastEthernet0/0
3.3.3.3           1   FULL/DR         00:00:36    192.168.0.2     FastEthernet0/1
```

To verify if directly connected subnets are really advertised into the different area, we can use the *show ip route ospf* command on both R1 and R3:



```
R1#show ip route ospf
     90.0.0.0/24 is subnetted, 1 subnets
O IA    90.10.0.0 [110/3] via 172.16.0.2, 00:12:48, FastEthernet0/1
O IA 192.168.0.0 [110/2] via 172.16.0.2, 00:12:48, FastEthernet0/1
```



```
R3#show ip route ospf
     10.0.0.0/24 is subnetted, 1 subnets
O IA    10.0.1.0 [110/3] via 192.168.0.1, 00:13:47, FastEthernet0/0
O IA 172.16.0.0 [110/2] via 192.168.0.1, 00:13:47, FastEthernet0/0
```

Characters **IA** in front of the routes indicate that these routes reside in different areas.

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		

- **Procedure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf cost** *cost*	Explicitly specifies the cost of

	Example: `Device(config-if)# ip ospf cost 65`	sending a packet on an OSPF interface.
Step 5	**ip ospf retransmit-interval** *seconds* **Example:** `Device(config-if)# ip ospf retransmit-interval 1`	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
Step 6	**ip ospf transmit-delay** *seconds* **Example:** `Device(config-if)# ip ospf transmit-delay`	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
Step 7	**ip ospf priority** *number-value* **Example:** `Device(config-if)# ip ospf priority 1`	Sets priority to help determine the OSPF designated router for a network.
Step 8	**ip ospf hello-interval** *seconds* **Example:** `Device(config-if)# ip ospf hello-interval 1`	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.
Step 9	**ip ospf dead-interval** *seconds* **Example:** `Device(config-if)# ip ospf dead-interval 1`	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.
Step 10	**ip ospf authentication-key** *key* **Example:** `Device(config-if)# ip ospf authentication-key 1`	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password

		authentication.
Step 11	**ip ospf message-digest-key** *key-id* **md5** *key* **Example:** `Device(config-if)# ip ospf message-digest-key 1 md5 23456789`	Enables OSPF MD5 authentication. The values for the *key-id* and *key* arguments must match values specified for other neighbors on a network segment.
Step 12	**ip ospf authentication** [**message-digest** | **null**] **Example:** `Device(config-if)# ip ospf authentication message-digest`	Specifies the authentication type for an interface.

Step 13	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

- **Precaution**
    - Handle Computer System and peripherals with care
    - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resource	

- **Result/Conclusion**

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………

- **Practical Related Questions**
    - What is OSPF?

    - Why we use OSPF?
    - How OSPF Works?
- **Exercise**
    - Configure OSPF and understand OSPF

(Space for Answer)

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

……………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

…………………………………………………………………………………………

- **References/ Suggestions for further Reading**

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-15-mt-book/iro-cfg.html

  https://study-ccna.com/ospf-configuration/

  https://www.cisco.com/c/en/us/products/ios-nx-os-software/open-shortest-path-first-ospf/index.html

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

  ………………………………………………..

  ………………………………………………..

  ……………………………………….........

  ………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.05: Configure User Datagram Protocol(UDP) Part-1 using relevant software

- **Practical Significance**

  Know the use of UDP

  Configure User Datagram Protocol

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**

  Create UDP Environment using simulator

- **Relevant Course Outcomes**

Implement different Transport Layer Protocol

- **Practical Outcomes (POs)**

  Understand configuration of UDP

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices

- **Minimum Theoretical Background**

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP’s simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

Description:

UDP is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams (using Datagram Sockets) to one another. UDP is sometimes called the Universal Datagram Protocol. The protocol was designed by David P. Reed in 1980.

UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient, for applications that do not need guaranteed delivery. Time-sensitive applications often use UDP because dropped packets are preferable to delayed packets. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. Unlike TCP, UDP is compatible with packet broadcast (sending to all on local network) and multicasting (send to all subscribers).

UDP is part of the TCP/IP protocol suite.

UDP is a simpler message-based **connectionless protocol**. In connectionless protocols, there is no effort made to setup a dedicated end-to-end connection. Communication is achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there, or if it is prepared to receive the information. With UDP messages (packets) cross the network in independent units.

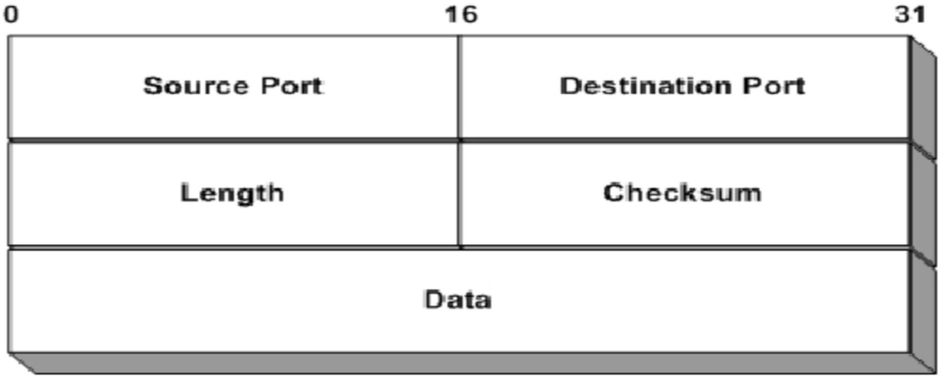
Unreliable - When a message is sent, it cannot be known if it will reach its destination; it could get lost along the way. There is no concept of acknowledgment, retransmission and timeout.

Not ordered - If two messages are sent to the same recipient, the order in which they arrive cannot be predicted.

Lightweight - There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.

Datagrams - Packets are sent individually and are guaranteed to be whole if they arrive. Packets have definite bounds and no split or merge into data streams may exist.

UDP packet format:



Source port - This is the source port of the packet, describing where a reply packet should be sent. This can actually be set to zero if it doesn't apply. For example, sometimes we don't require a reply packet, and the packet can then be set to source port zero. In most implementations, it is set to some port number.

Destination port - The destination port of the packet. This is required for all packets, as opposed to the source port of a packet.

Length -The length field specifies the length of the whole packet in octets, including header and data portions. The shortest possible packet can be 8 octets long.
Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)

Checksum - The checksum is the same kind of checksum as used in the TCP header, except that it contains a different set of data. In other words, it is a one's complement of the one's complement sum of parts of the IP header, the whole UDP header, the UDP data and padded with zeroes at the end when necessary.

This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP)

User Interface

A user interface should allow

- the creation of new receive ports,
- receive operations on the receive ports that return the data octets and an indication of source port and source address,
- an operation that allows a datagram to be sent, specifying the data, source and destination ports and addresses to be sent.

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		

- **Procedure**

  To configure UDP port:

Step 1.

Navigate to your Control Panel menu by clicking "Start" and "Control Panel."

Step 2.

Click the preference that says "Security." Click "Windows Firewall" and then click the preference displayed on the upper-left corner that says "Allow a program through Windows Firewall".

Step 3.

Click the icon that says "Add port." Give the UDP port any name you want , then enter it in the "Name" text bar. This can be the name of the service using the port.

Step 4.

Type the number of the port you want to enable UDP process for in the "Port number" field. Click the "UDP" check-mark in the "Protocol" section, then click "OK" to save the changes. You have enabled UDP process for the desired port.

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Network Interface Card	Manufacturer: Cisco
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
3.	Switch (min. 8 ports)	8 ports
4.	Any other Resource	

- **Result/Conclusion**

……………………………………………………………………………………………………

……………………………………………………………………………………………………

…………………………………………………………………………………………………

………

- **Practical Related Questions**
  - What is UDP
  - Explain Datagram Format of UDP
  - Explain different features of UDP
- **Exercise**
  - Configure UDP port.

(Space for Answer)

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………**References/ Suggestions for further Reading** http://www.tieline.com/manuals/TLR5200D/en/v2_14/index.html?configuring_tcp_udp_ports.htm

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

  ……………………………………………………..

  ……………………………………………………..

  …………………………………………….........

  ……………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.06: Configure User Datagram Protocol(UDP) Part-2 using relevant software

- **Practical Significance**

  Know the use of UDP

  Configure User Datagram Protocol

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**
  - Create UDP Environment using simulator
- **Relevant Course Outcomes**

  Implement different Transport Layer Protocol

- **Practical Outcomes (POs)**

  Understand configuration of UDP

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

  User Datagram Protocol (UDP) are transportation protocols which are some of the core protocols of the Internet protocol suite. Both TCP and UDP work at the transport layer of the TCP/IP model. TCP uses a three-way handshake to establish the reliable connection, whereas UDP is unreliable but faster when compared to TCP. The network device offers some of the services which use either TCP or UDP for easy management of the device. The services can be enabled or disabled based on the requirement.

The TCP and UDP services information are shown in the TCP and UDP Service tables of the web-based utility page of the switch. The information showed in these tables depict the current status of the enabled TCP and UDP services. You can use this information to manage and troubleshoot any of the enabled services on the switch.

Diagrams / Experimental set-up /Work Situation

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		

- **Procedure**

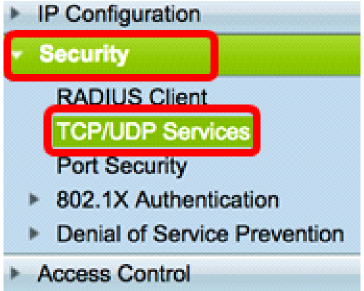
Configure UDP Services on your Switch

Configure UDP Services

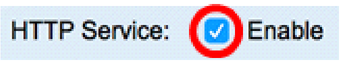
The UDP Services page enables UDP-based services on the device, usually for security reasons. Follow these steps to enable or disable a specific service:

Step 1. Log in to the web-based utility of your switch then choose **Security** > **TCP/UDP Services**.

Note: The available options may vary depending on the exact model of your device. In this example, SG350X-48MP switch is used.

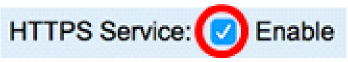


Step 2. Check the **Enable** HTTP to enable the Hyper Text Transfer Protocol (HTTP) service on your switch. By default, Cisco Small Business Switches can be configured through the web-based utility using a web browser thus this service is checked by default.



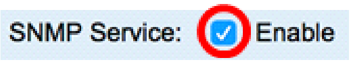
HTTP Service: ☑ Enable

Step 3. Check the **Enable** HTTPS to enable the Hyper Text Transfer Protocol Secure (HTTPS) service on your switch. Connectivity between the administrator and the switch using HTTP is unencrypted. You can enable the HTTPS service which works with Secure Socket Layer (SSL) protocol to offer to the administrator a more secure web browser connection with the configuration utility of the switch. This service is enabled by default.



HTTPS Service: ☑ Enable

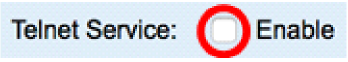
Step 4. Check the **Enable** SNMP to enable the Simple Network Management Protocol (SNMP) service on your switch. SNMP is an application layer protocol that is used to manage and monitor a network. For the different SNMP features to work properly, you first need to enable the SNMP service.



SNMP Service: ☑ Enable

Note: In this example, SNMP Service is enabled.

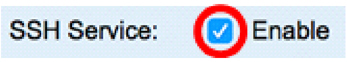
Step 5. Check the **Enable** Telnet Service check box to enable the Telnet service on your switch. Telnet is a network protocol that allows a device to be controlled by a command line interface over the Internet or a LAN. When Telnet is enabled, an administrator can configure the switch through the use of a Telnet client application. However, since Telnet messages are not encrypted, it is recommended that you use SSH service.



Telnet Service: □ Enable

Note: In this example, Telnet Service is disabled.

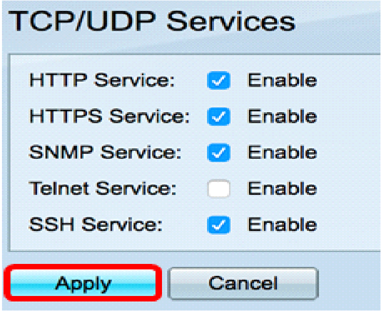
Step 6. Check the **Enable** SSH Service check box to enable the Secure Shell (SSH) service on your switch. SSH allows the administrator to configure the switch through a command line interface (CLI) with a third party program. In CLI mode via SSH, the administrator can execute more advanced configurations in a secure connection.



SSH Service: ☑ Enable

Note: In this example, Telnet Service is enabled.

Step 7. Click **Apply** to save the settings.



HTTP Service: ☑ Enable

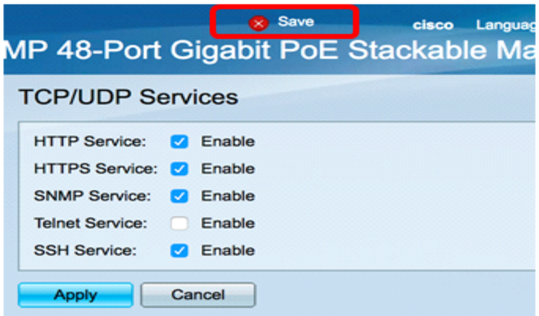
HTTPS Service: ☑ Enable

SNMP Service: ☑ Enable

Telnet Service: □ Enable

SSH Service: ☑ Enable

Step 8. (Optional) Click **Save** to save settings to the startup configuration file.



HTTP Service: ☑ Enable

HTTPS Service: ☑ Enable

SNMP Service: ☑ Enable

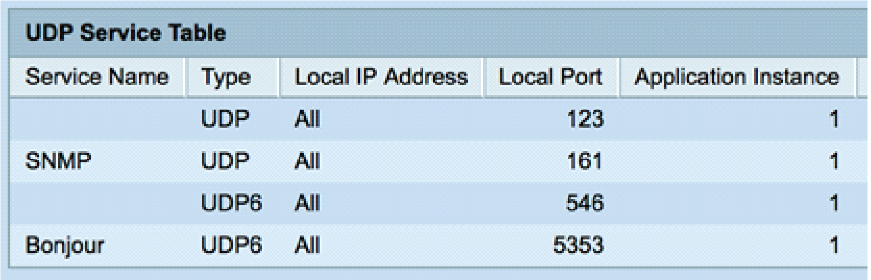
Telnet Service: □ Enable

SSH Service: ☑ Enable

You should now have configured the UDP Services on your switch.

View UDP Service Table

The UDP Service table displays the next information:



UDP Service Table

Service Name	Type	Local IP Address	Local Port	Application Instance
	UDP	All	123	1
SNMP	UDP	All	161	1
	UDP6	All	546	1
Bonjour	UDP6	All	5353	1

- Service Name — The different access services currently enabled for UDP connections.
- Type — The UDP type used by each service. The two types are:

  - UDP — offers a connection between IPv4 hosts.

  - UDP6 — offers a connection between both IPv4 and IPv6 hosts.
- Local IP Address — The IP address used by the switch to offer UDP connections.
- Local Port — The port number used by the switch for each UDP service to receive connection requests.
- Application Instance — The current UDP service instance.

You should now have viewed the UDP Service Table on your switch.

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices

- **Resources Used**

Sr.No	**Name of Resource**	**Specification**
1.	Crossover Cable	
2.	Network Interface Card	Manufacturer: Cisco
3.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
4.	Switch (min. 8 ports)	8 ports
5.	Any other Resource	

- **Result/Conclusion**

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

………………

- **Practical Related Questions**
  - Why we use UDP
  - When we use UDP
  - How UDP Works?
- **Exercise**
  - Understand and configure UDP.

(Space for Answer)

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……

……

……

……

………………………………………………………

……

……

……

……

……

……

……

……

……

……

……

……

……

………………………………………………………………………

- **References/ Suggestions for further Reading**

  https://www.cisco.com/c/en/us/td/docs/ios/sw_upgrades/interlink/r2_0/api_con/actcp.html

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

  ………………………………………………..

  ………………………………………………..

  …………………………………………..........

  ………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.07: Configure Transmission Control Protocol (TCP) using relevant software

- **Practical Significance**

  Know the use of TCP

  Configure Transmission Control Protocol

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.

- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**

  Configure Transmission Control Protocol

- **Relevant Course Outcomes**

  Implement different Transport Layer Protocol

- **Practical Outcomes (POs)**

  Understand configuration of TCP

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices

- **Minimum Theoretical Background**

  Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are transportation protocols which are some of the core protocols of the Internet protocol suite. Both TCP and UDP work at the transport layer of the TCP/IP model. TCP uses a three-way handshake to establish the reliable connection, whereas UDP is unreliable but faster when compared to TCP. The network device offers some of the services which use either TCP or UDP for easy management of the device. The services can be enabled or disabled based on the requirement.

  The TCP and UDP services information are shown in the TCP and UDP Service tables of the web-based utility page of the switch. The information showed in these tables depict the current status of the enabled TCP and UDP services. You can use this information to manage and troubleshoot any of the enabled services on the switch.

  This article provides instructions on how to configure the TCP and UDP services on your switch.

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		
3.	Crossover Cable			

- **Procedure**

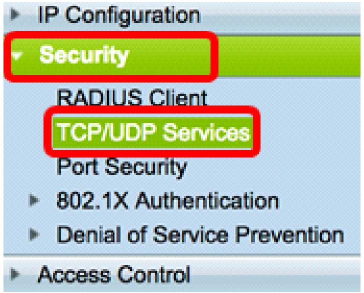
Configure TCP/UDP Services on your Switch

Configure TCP/UDP Services

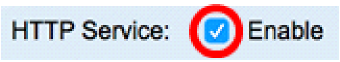
The TCP/UDP Services page enables TCP or UDP-based services on the device, usually for security reasons. Follow these steps to enable or disable a specific service:

Step 1. Log in to the web-based utility of your switch then choose **Security** > **TCP/UDP Services**.

Note: The available options may vary depending on the exact model of your device. In this example, SG350X-48MP switch is used.

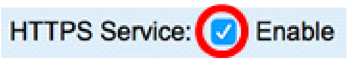


Step 2. Check the **Enable** HTTP to enable the Hyper Text Transfer Protocol (HTTP) service on your switch. By default, Cisco Small Business Switches can be configured through the web-based utility using a web browser thus this service is checked by default.



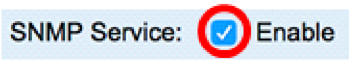
HTTP Service: ☑ Enable

Step 3. Check the **Enable** HTTPS to enable the Hyper Text Transfer Protocol Secure (HTTPS) service on your switch. Connectivity between the administrator and the switch using HTTP is unencrypted. You can enable the HTTPS service which works with Secure Socket Layer (SSL) protocol to offer to the administrator a more secure web browser connection with the configuration utility of the switch. This service is enabled by default.



HTTPS Service: ☑ Enable

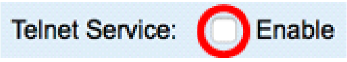
Step 4. Check the **Enable** SNMP to enable the Simple Network Management Protocol (SNMP) service on your switch. SNMP is an application layer protocol that is used to manage and monitor a network. For the different SNMP features to work properly, you first need to enable the SNMP service.



SNMP Service: ☑ Enable

Note: In this example, SNMP Service is enabled.

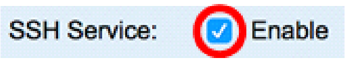
Step 5. Check the **Enable** Telnet Service check box to enable the Telnet service on your switch. Telnet is a network protocol that allows a device to be controlled by a command line interface over the Internet or a LAN. When Telnet is enabled, an administrator can configure the switch through the use of a Telnet client application. However, since Telnet messages are not encrypted, it is recommended that you use SSH service.



Telnet Service: □ Enable

Note: In this example, Telnet Service is disabled.

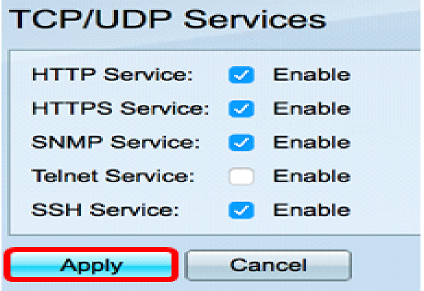
Step 6. Check the **Enable** SSH Service check box to enable the Secure Shell (SSH) service on your switch. SSH allows the administrator to configure the switch through a command line interface (CLI) with a third party program. In CLI mode via SSH, the administrator can execute more advanced configurations in a secure connection.



SSH Service: ☑ Enable

Note: In this example, Telnet Service is enabled.

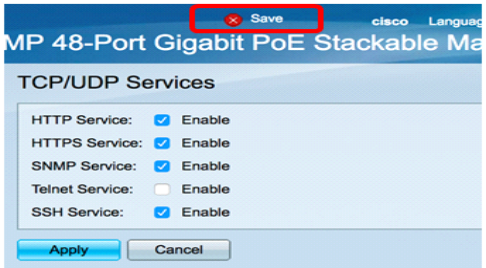
Step 7. Click **Apply** to save the settings.



TCP/UDP Services

HTTP Service: ☑ Enable
HTTPS Service: ☑ Enable
SNMP Service: ☑ Enable
Telnet Service: □ Enable
SSH Service: ☑ Enable

Step 8. (Optional) Click **Save** to save settings to the startup configuration file.



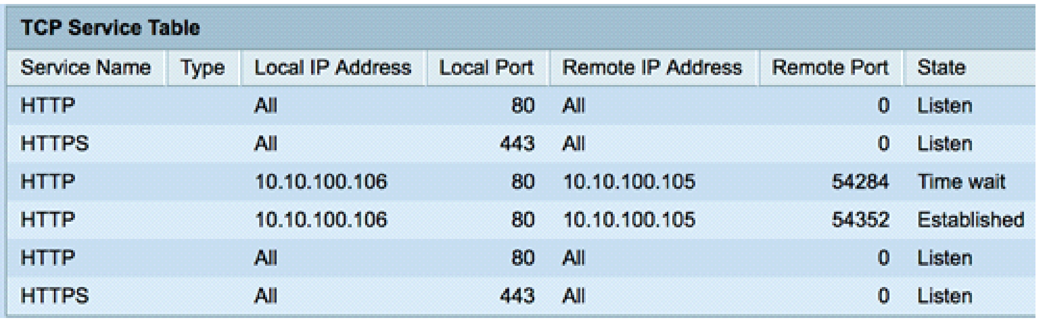
TCP/UDP Services

HTTP Service: ☑ Enable
HTTPS Service: ☑ Enable
SNMP Service: ☑ Enable
Telnet Service: □ Enable
SSH Service: ☑ Enable

You should now have configured the TCP/UDP Services on your switch.

View TCP Service Table

The TCP Service table displays the next information:



TCP Service Table

Service Name	Type	Local IP Address	Local Port	Remote IP Address	Remote Port	State
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen
HTTP		10.10.100.106	80	10.10.100.105	54284	Time wait
HTTP		10.10.100.106	80	10.10.100.105	54352	Established
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen

- Service Name — The different access services currently enabled for TCP connections.
- Type — The TCP type used by each service. The two types are:
  - TCP — offers a reliable connection between IPv4 hosts.
  - TCP6 — offers a reliable connection between both IPv4 and IPv6 hosts.
- Local IP Address — The IP address used by the switch to offer TCP connections.
- Local Port — The port number used by the switch for each TCP service to receive connection requests.
- Remote IP Address — The IP address of the device that requests a TCP connection through the specified TCP service.
- Remote Port — The port number used by the remote device to connect to the specified TCP service.
- State — The current state of the connection. Some of the states are:
  - Listen — The switch takes any connection for this Service on the Local Port.
  - Established — Indicates an active connection.
  - Time wait — Indicates a connection that has been closed, but tracked so that out-of-order packets can still arrive to the destination.

You should now have viewed the TCP Service Table on your switch.

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices

- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resource	

- **Result/Conclusion**

…………………………………………………………………………………………………

…………………………………………………………………………………………………

………………………………………………………………………………………………………

………………

- **Practical Related Questions**
  - Why we use TCP?
  - How TCP works?
  - Differentiate between TCP and UDP.
- **Exercise**
  - Configure and understand TCP

(Space for Answer)

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………

………

………

………

………………

………

………

………

………………

………

………

…………

- **References/ Suggestions for further Reading**

  https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-250-series-smart-switches/smb2009-configure-transmission-control-protocol-tcp-and-user-datagra.html

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

  ………………………………………………..

  ………………………………………………..

  …………………………………………..........

  …………………………………………..........

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.08: Configure Dynamic Host Configuration Protocol(DHCP)using relevant software

- **Practical Significance**
  - Student should be able to install windows server 2008 and DHCP.

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**
  - Ability to install the network Operating System
  - Ability to work with the Networking Operating System
- **Relevant Course Outcomes**

Implement different Transport Layer Protocol

- **Practical Outcomes (POs)**

  Understand configuration of UDP

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices

- **Minimum Theoretical Background**

Proposition 1. Network Operating System (NOS)

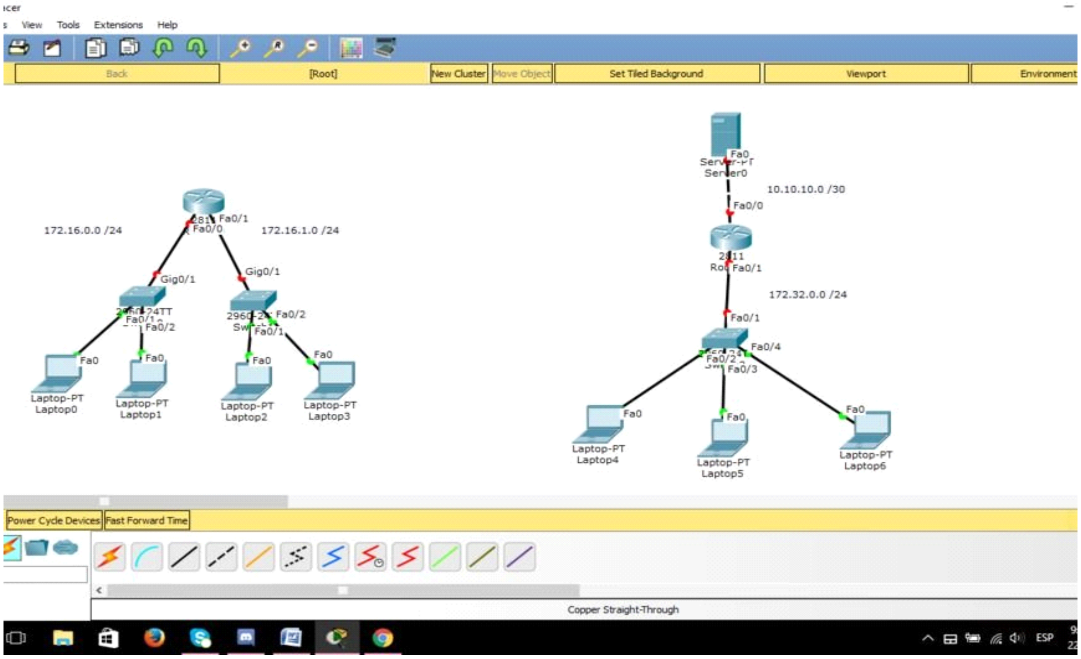
- Network Operating System is software that implements computer networking oriented operating system. It includes special functions for connecting computers and devices into a local-area network (LAN). Some operating systems. such as UNIX and he mac OS, have networking functions built in. The term Network Operating System can also be referred as software that enhances a basic operating system by adding networking features. For example, Operating System that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions is a Network Operating System. It is designed to allow shared file and printer access among multiple computers in a network. Novell Netware, Artisoft's LANtastic, Microsoft Windows Server, and Windows NT are examples of an NOS.

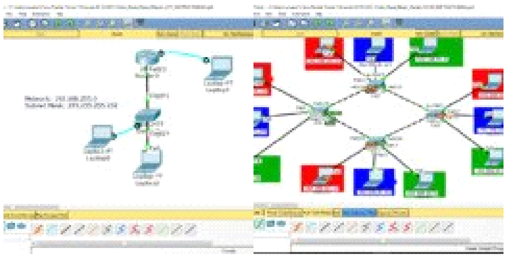
- **Resources Required**

Sr.No	**Name of Resource**	**Specification**	**Quantity**	**Remarks/Use**
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		

- **Procedure**

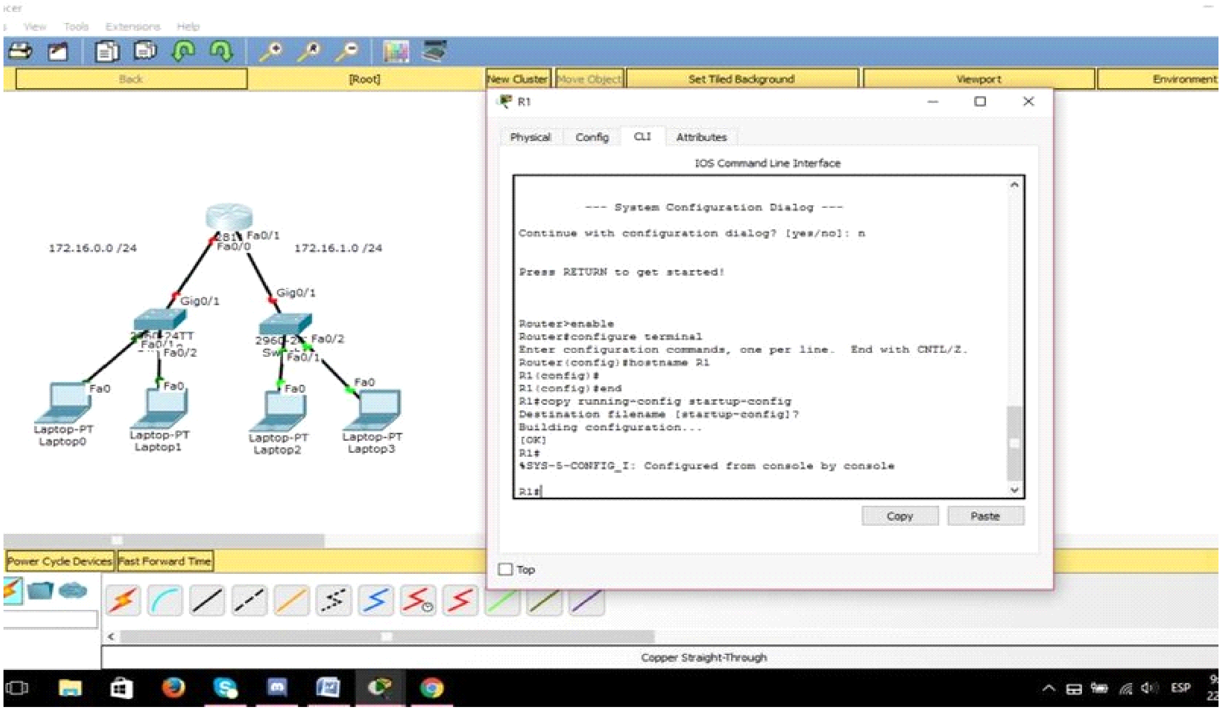
How to Configure DHCP in Cisco Packet Tracer



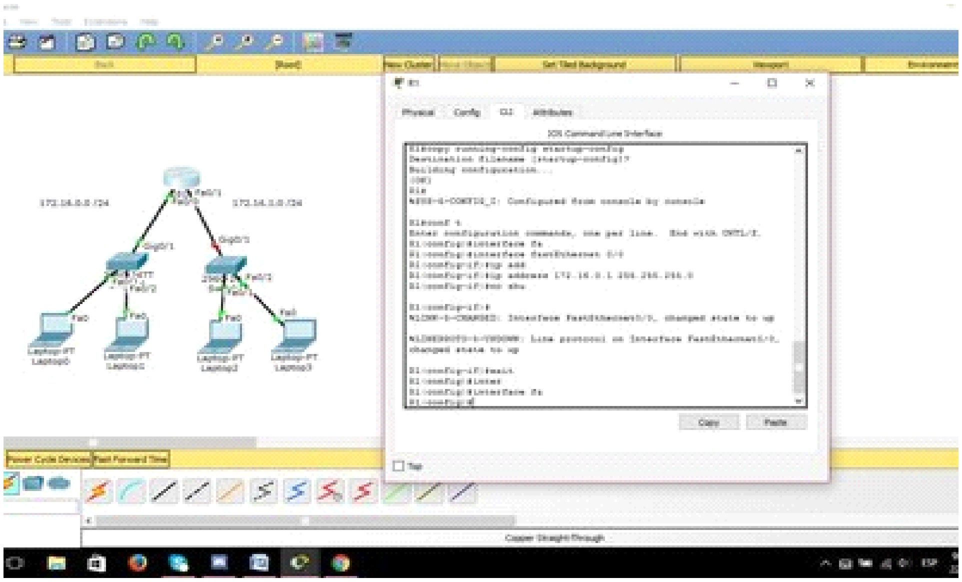


In this tutorial we will configure IP addresses dynamically, for this will be done two examples configuring DHCP. The first configuration is through the router and the second is through a server.

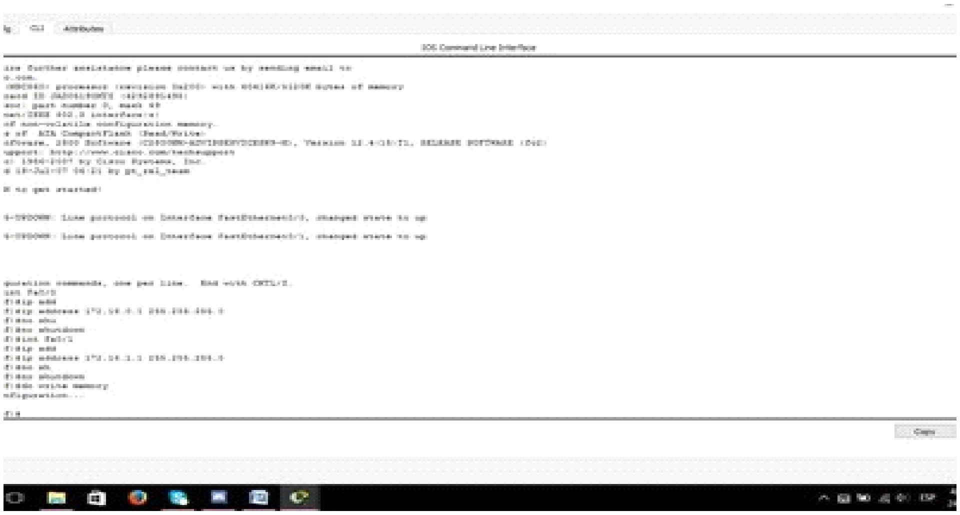
Step 1:



```
        --- System Configuration Dialog ---

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


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#end
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```



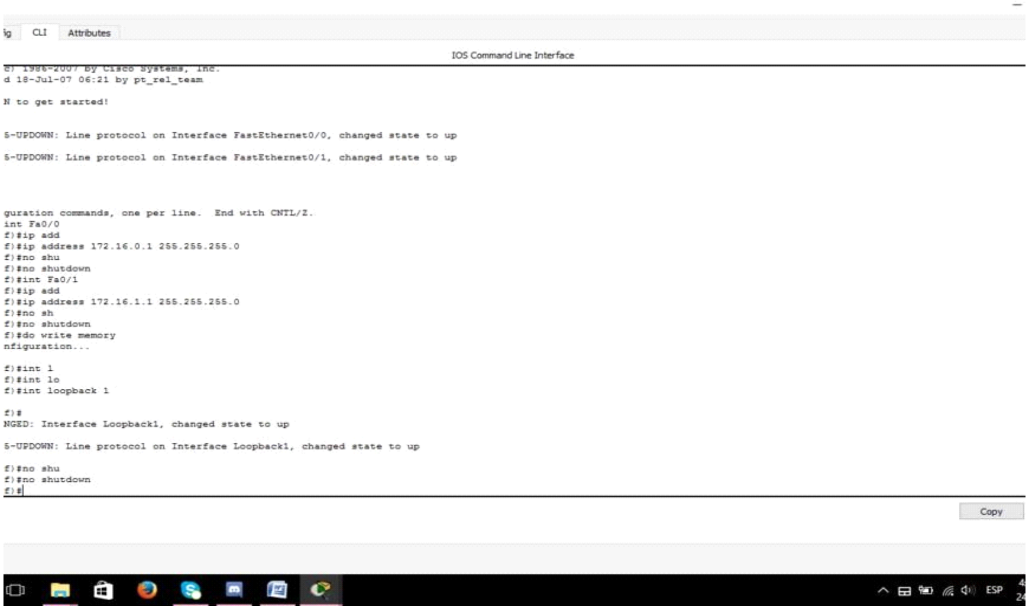
```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip add
R1(config-if)#ip address 172.16.0.1 255.255.255.0
R1(config-if)#no shu

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

R1(config-if)#exit
R1(config)#inter
R1(config)#interface fa
R1(config)#
```



```
ire further assistance please contact us by sending email to
o.com.
(MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
oard ID JAD05190MTZ (4292891495)
sor: part number 0, mask 49
net/IEEE 802.3 interface(s)
of non-volatile configuration memory.
e of ATA CompactFlash (Read/Write)
oftware, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
upport: http://www.cisco.com/techsupport
c) 1986-2007 by Cisco Systems, Inc.
d 18-Jul-07 06:21 by pt_rel_team

N to get started!

5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up



guration commands, one per line.  End with CNTL/Z.
int Fa0/0
f)#ip add
f)#ip address 172.16.0.1 255.255.255.0
f)#no shu
f)#no shutdown
f)#int Fa0/1
f)#ip add
f)#ip address 172.16.1.1 255.255.255.0
f)#no sh
f)#no shutdown
f)#do write memory
nfiguration...

f)#
```

Step 1: First configure the DHCP service on the router, so
we will first enable the two interfaces and place their respective IP addresses with their Subnet Mask.
To do this, the following commands will be written in global configuration for the R1 router:
Int Fa0/0
Ip address 172.16.0.1 255.255.255.0
No shutdown
Int Fa0/1
Ip address 172.16.1.1 255.255.255.0
No shutdown
Do write memory

Step 2:



```
c) 1986-2007 by Cisco Systems, Inc.
d 18-Jul-07 06:21 by pt_rel_team

N to get started!

5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up



guration commands, one per line.  End with CNTL/Z.
int Fa0/0
f)#ip add
f)#ip address 172.16.0.1 255.255.255.0
f)#no shu
f)#no shutdown
f)#int Fa0/1
f)#ip add
f)#ip address 172.16.1.1 255.255.255.0
f)#no sh
f)#no shutdown
f)#do write memory
nfiguration...

f)#int 1
f)#int lo
f)#int loopback 1

f)#
NGED: Interface Loopback1, changed state to up

5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

f)#no shu
f)#no shutdown
f)#
```

Step 2: Now you will proceed to enable a logical interface inside the router, this type of interfaces are very useful since these are always on if the router is on too. But it is good practice to always make sure that the logical interface is turned on.

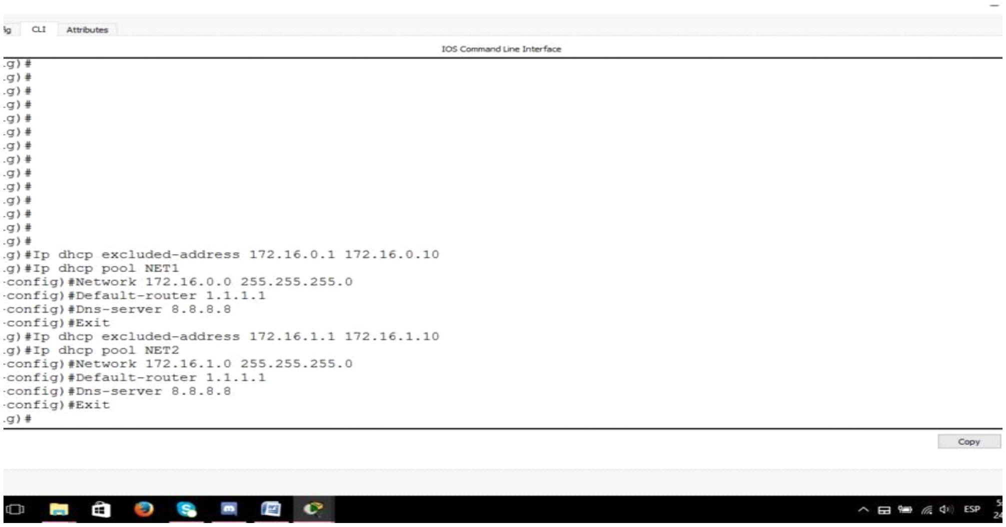
To do this we will place the following commands in the global configuration:

Int loopback 1

Ip address 1.1.1.1 255.255.255.255

No shutdown

Step 3:



```
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#Ip dhcp excluded-address 172.16.0.1 172.16.0.10
.g)#Ip dhcp pool NET1
-config)#Network 172.16.0.0 255.255.255.0
-config)#Default-router 1.1.1.1
-config)#Dns-server 8.8.8.8
-config)#Exit
.g)#Ip dhcp excluded-address 172.16.1.1 172.16.1.10
.g)#Ip dhcp pool NET2
-config)#Network 172.16.1.0 255.255.255.0
-config)#Default-router 1.1.1.1
-config)#Dns-server 8.8.8.8
-config)#Exit
.g)#
```

Step 3: To configure the DHCP you must know which network address we want to provide, which is the Subnet Mask and which is the Default Gateway on the network. As optional we can also exclude certain IP addresses to reserve them or simply because we do not want to use them and we can also configure a DNS service where we will place an address that we want, it is worth repeating that these last two configurations are optional since the DHCP service can Work perfectly well without these.

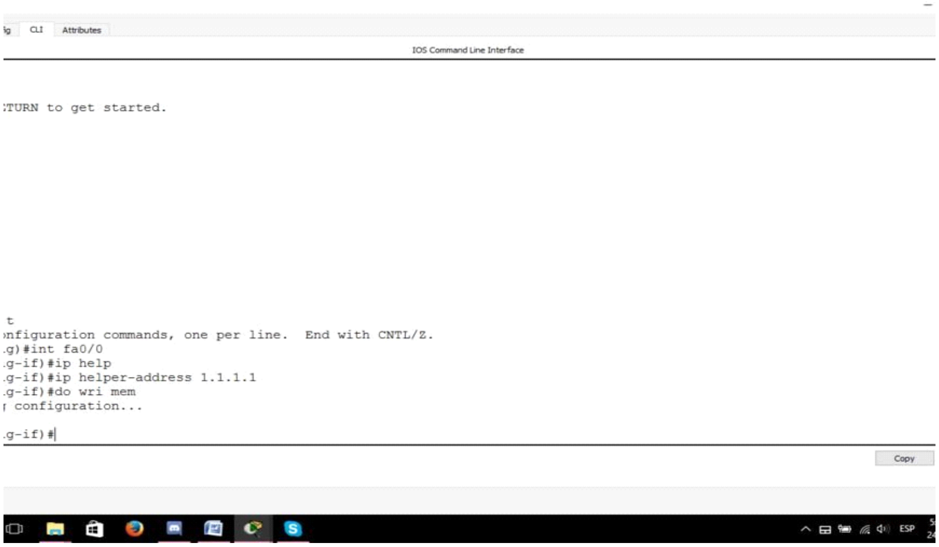
The commands to use are as follows:

Ip dhcp excluded-address 172.16.0.1 172.16.0.10
Ip dhcp pool NET1
Network 172.16.0.0 255.255.255.0
Default-router 1.1.1.1
Dns-server 8.8.8.8
Exit
Ip dhcp excluded-address 172.16.1.1 172.16.1.10
Ip dhcp pool NET2
Network 172.16.1.0 255.255.255.0
Default-router 1.1.1.1
Dns-server 8.8.8.8
Exit

Note that for the Default Gateway we will use the loopback address 1, we could also have put any address of the physical interfaces of the router R1 but for ease we will place in default-router

1.1.1.1. It should also be mentioned that the address 8.8.8.8 that was put in the DNS service is like a demonstrative purpose.

Step 4:



```
:TURN to get started.





t
›nfiguration commands, one per line.  End with CNTL/Z.
.g)#int fa0/0
.g-if)#ip help
.g-if)#ip helper-address 1.1.1.1
.g-if)#do wri mem
; configuration...

.g-if)#
```

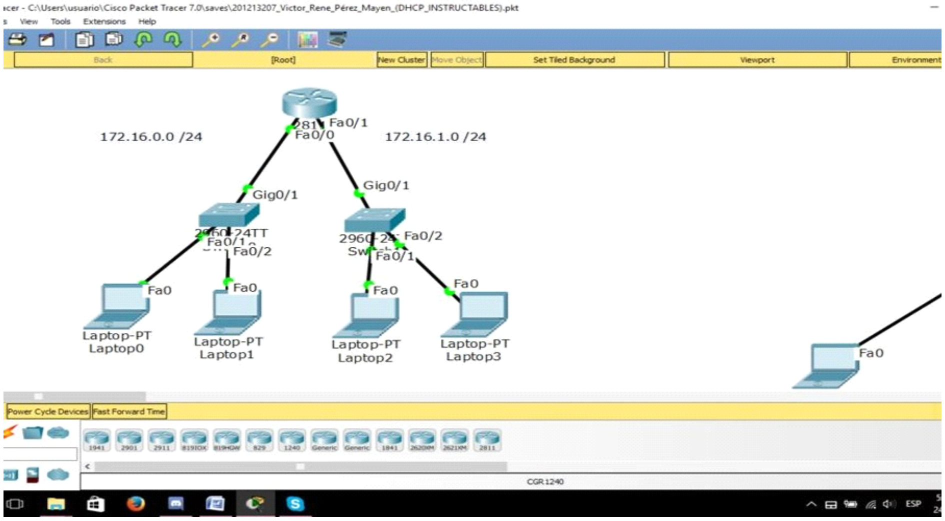
Step 4: We now need to require DCHP services on the respective physical interfaces of the router. We must be very careful that we are requiring the DHCP service in the correct interface, for this we must note that the address of the interface matches the address of the DHCP together with the subnet mask, to require the service we must use the address of the Default-router.

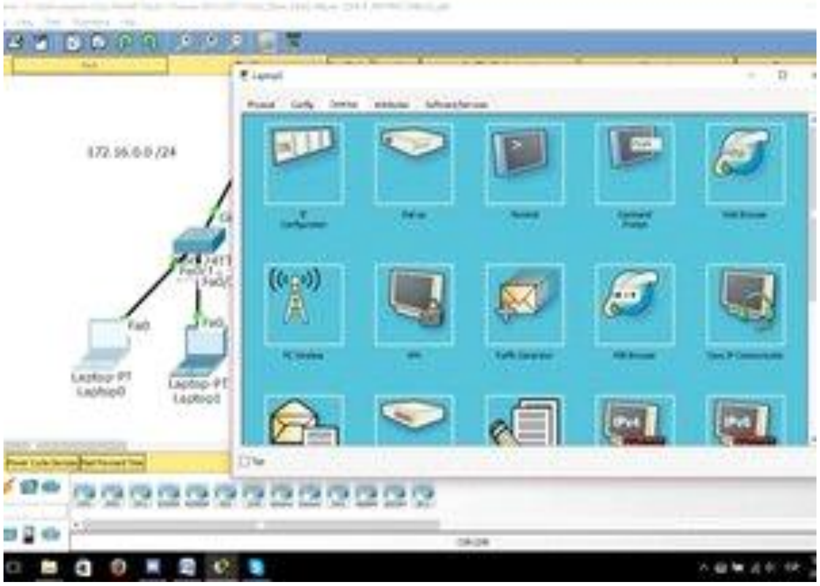
To prevent confusions in this step we will only configure the DHCP request on the Fa0/0 interface. The commands are:

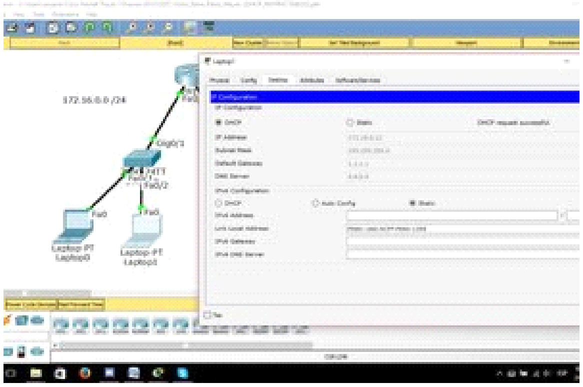
Int Fa0/0

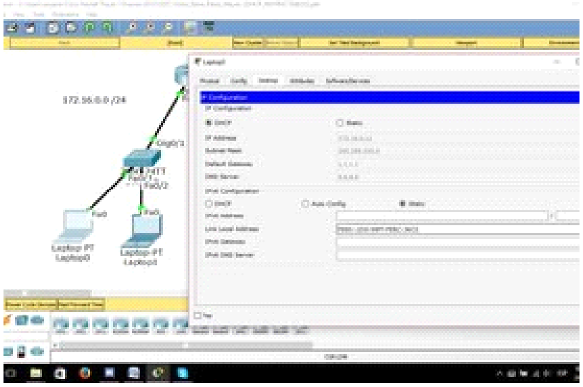
Ip helper-address 1.1.1.1

Step 5:





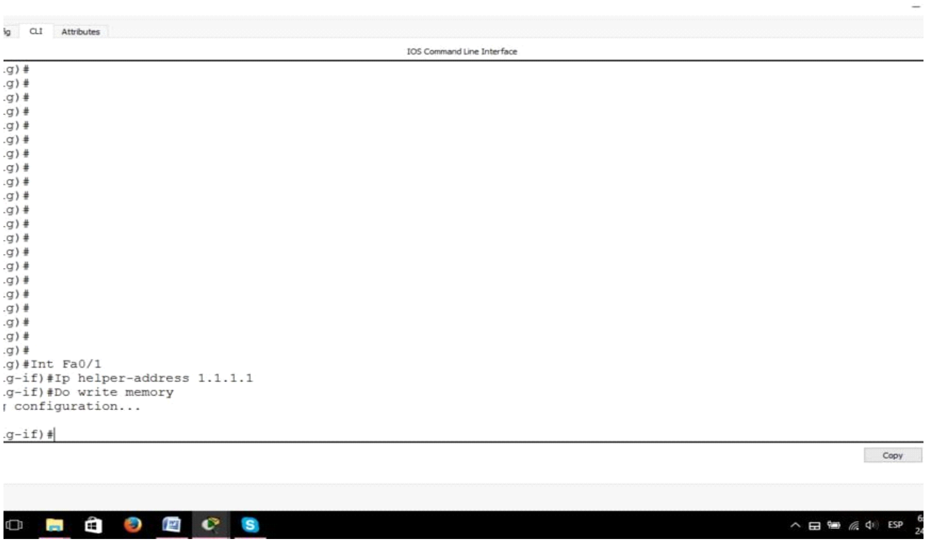




Step 5: Now proceed to verify that if the IP addresses have been automatically distributed for the final devices that are connected to the Fa0/0 interface.

To do this we go to a laptop and select the IP Configuration option, then we have to click the DHCP option. It may take some time to give the address automatically but if we are sure that our configuration is fine we will not have to worry, there is a possibility that it will be late to give the address automatically, for that we can select the Static option and then DHCP again to get the IP address.

Step 6:



```
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#
.g)#Int Fa0/1
.g-if)#Ip helper-address 1.1.1.1
.g-if)#Do write memory
 configuration...

.g-if)#
```

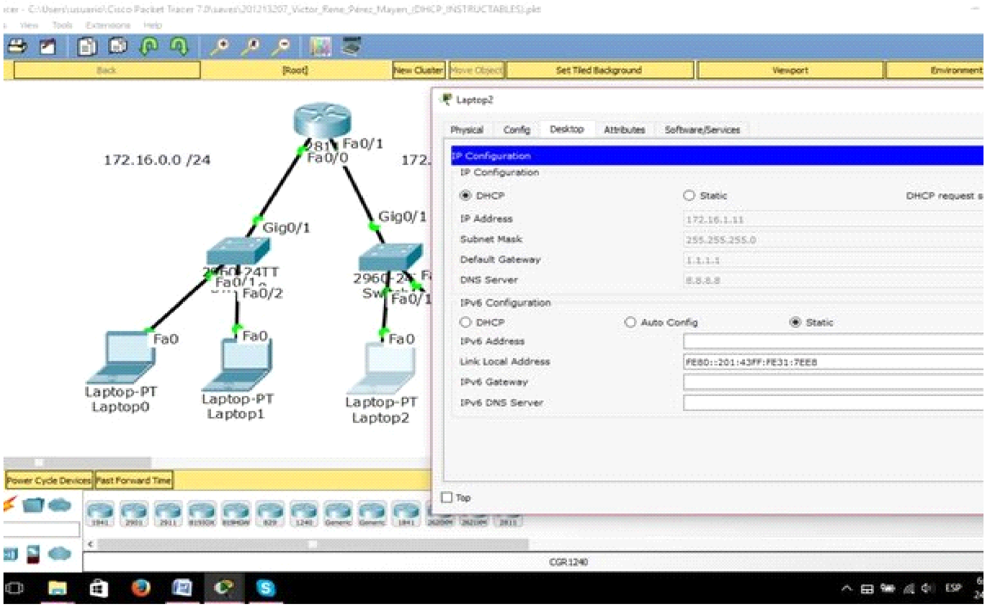
Step 6: In this part we will configure the DHCP service for the Fa0/1 interface as it was done in Step 4, the commands we will use are:

Int Fa0/1

Ip helper-address 1.1.1.1

Do write memory

Step 7:



Laptop2

IP Configuration

IP Configuration

● DHCP ○ Static DHCP request s

IP Address 172.16.1.11

Subnet Mask 255.255.255.0

Default Gateway 1.1.1.1

DNS Server 8.8.8.8

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

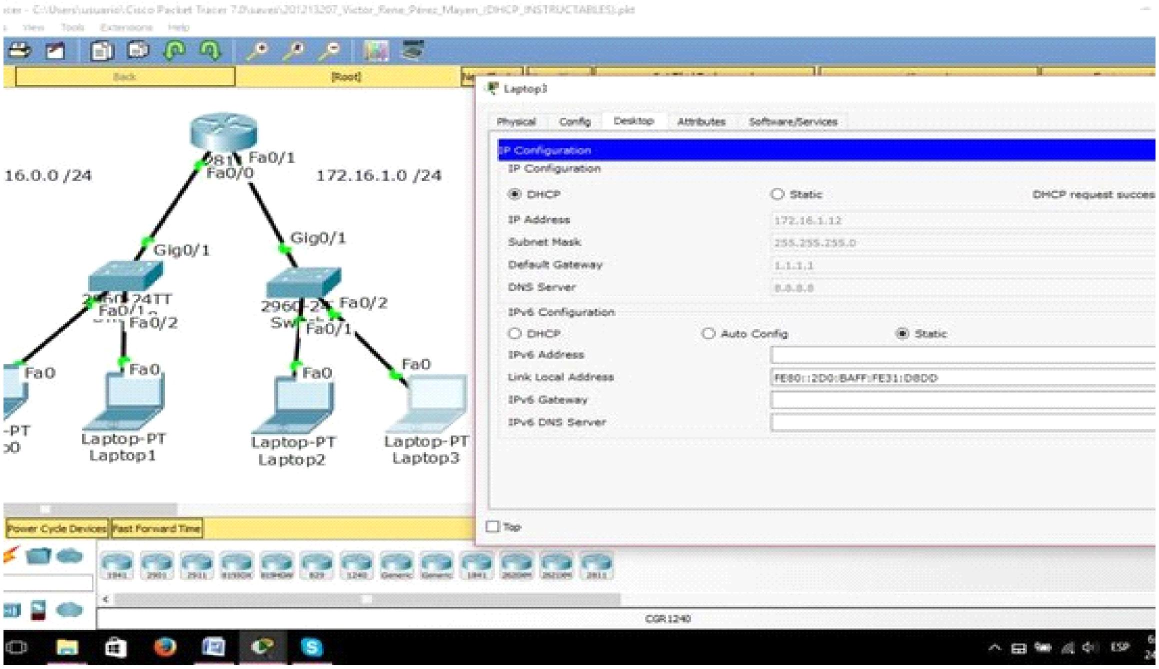
IPv6 Address

Link Local Address FE80::201:43FF:FE31:7EE8

IPv6 Gateway

IPv6 DNS Server

□ Top



Laptop3

IP Configuration

● DHCP ○ Static DHCP request succes

IP Address 172.16.1.12

Subnet Mask 255.255.255.0

Default Gateway 1.1.1.1

DNS Server 8.8.8.8

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address

Link Local Address FE80::2D0:BAFF:FE31:D8DD

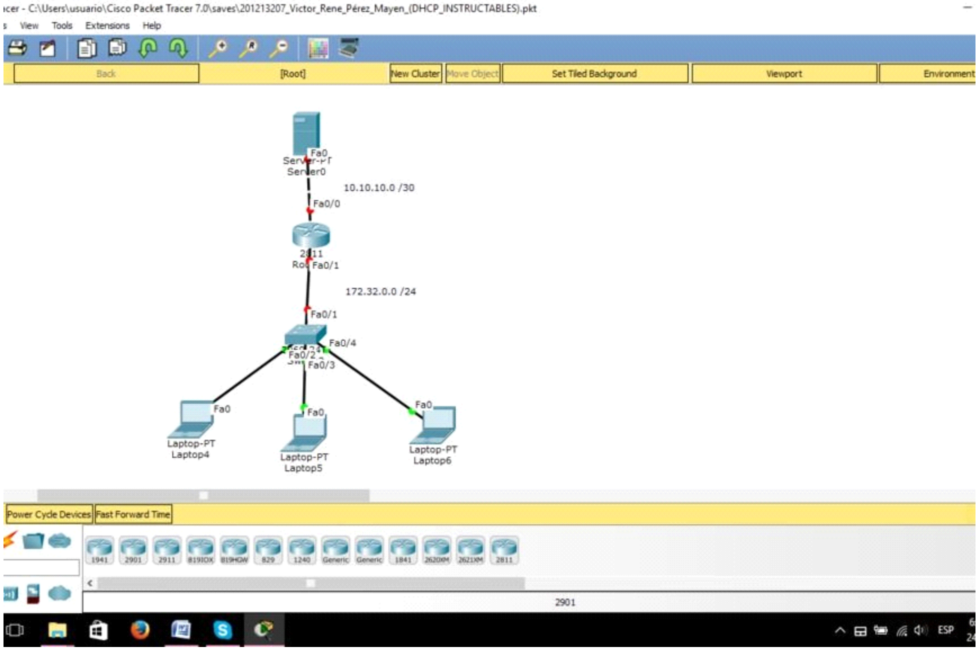
IPv6 Gateway

IPv6 DNS Server

□ Top

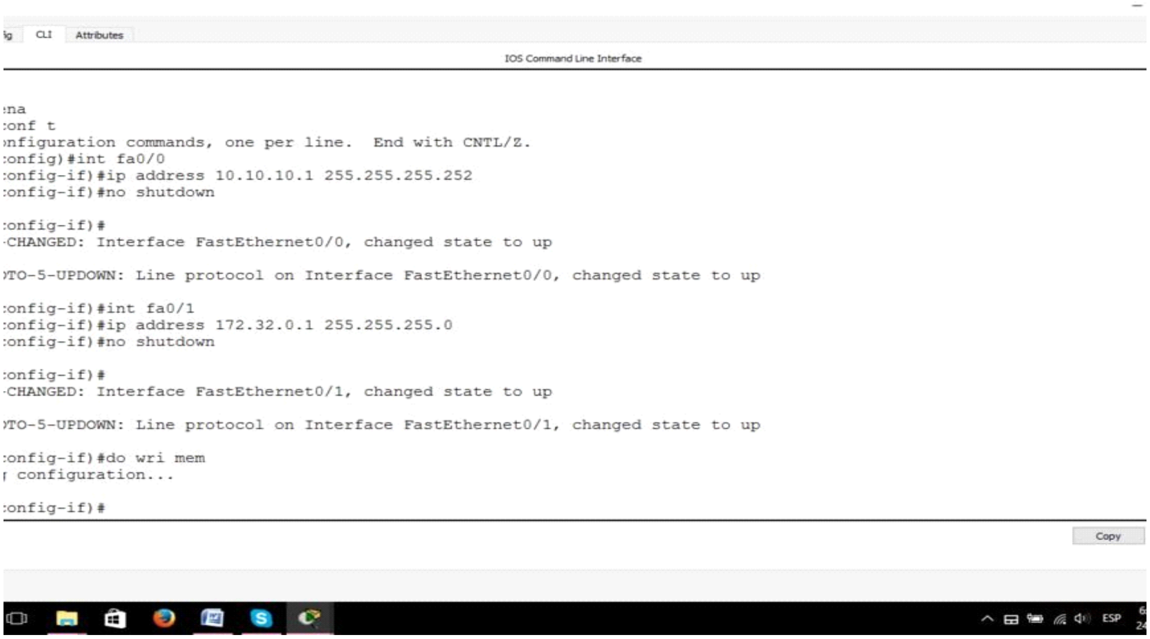
Step 7: We need to select the DHCP option on the laptops that are connected to the Fa0/1 interface as was done in Step 5.

Step 8:



Step 8: Now proceed to configure the DHCP service of the second form, in this method we have to configure it on a Server.

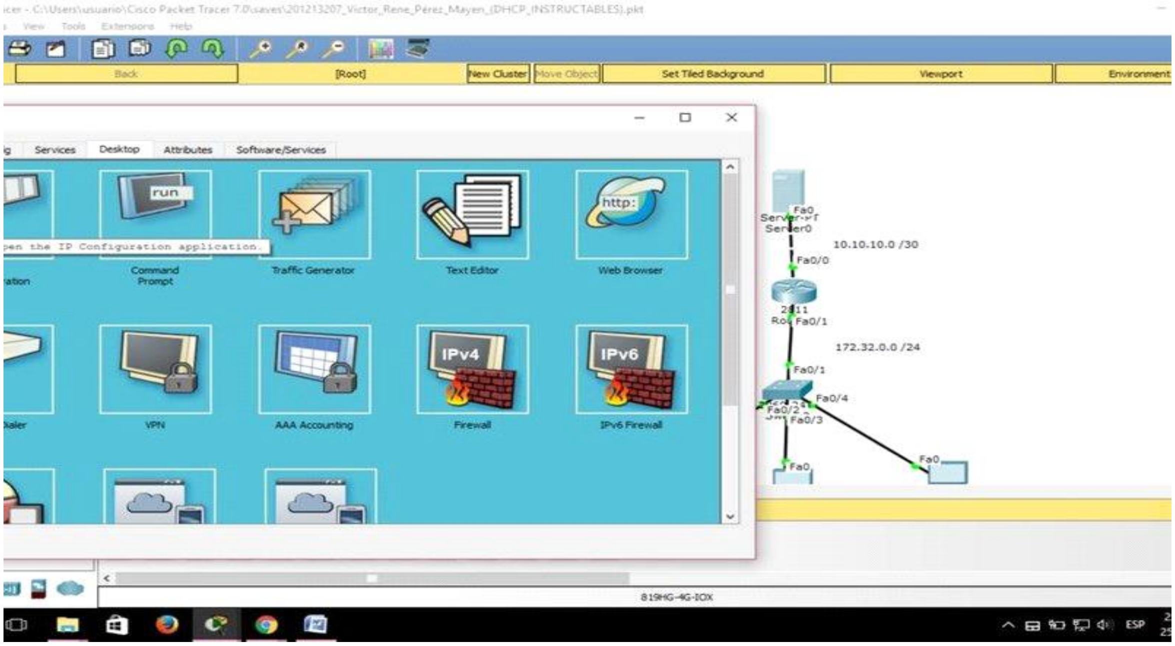
Step 9:

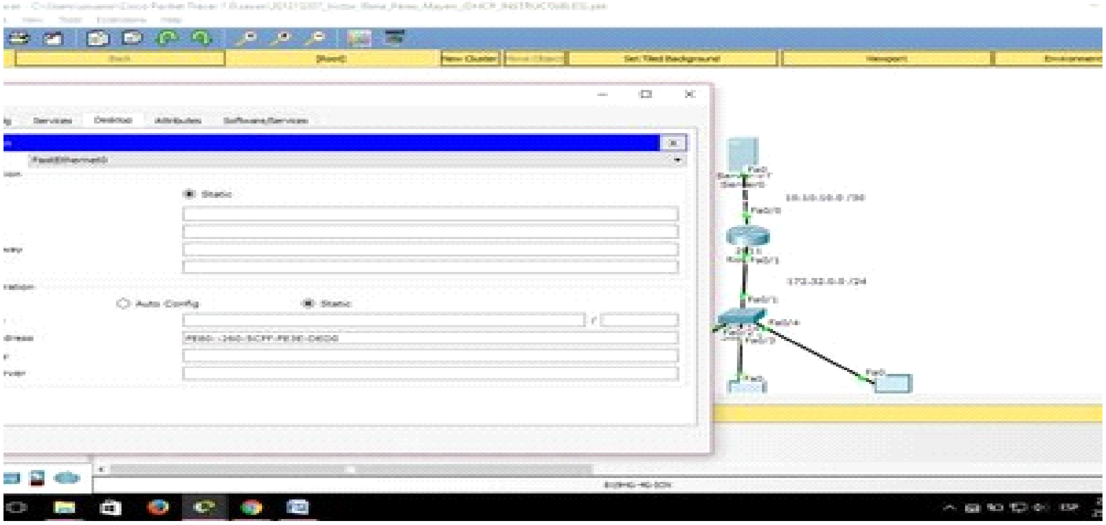


```
:na
:onf t
›nfiguration commands, one per line.  End with CNTL/Z.
:onfig)#int fa0/0
:onfig-if)#ip address 10.10.10.1 255.255.255.252
:onfig-if)#no shutdown

:onfig-if)#
-CHANGED: Interface FastEthernet0/0, changed state to up

›TO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

:onfig-if)#int fa0/1
:onfig-if)#ip address 172.32.0.1 255.255.255.0
:onfig-if)#no shutdown

:onfig-if)#
-CHANGED: Interface FastEthernet0/1, changed state to up

›TO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

:onfig-if)#do wri mem
; configuration...

:onfig-if)#
```

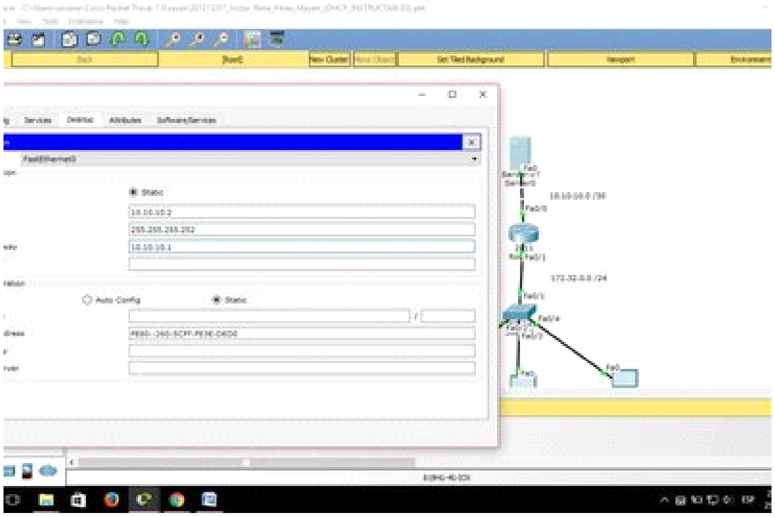
Step 9: In this step we will configure the IP addresses for the physical interfaces. The programming will be done in the global configuration with the following commands:
Int fa0/0
Ip address 10.10.10.1 255.255.255.252
No shutdown
Int fa0/1
Ip address 172.32.0.1 255.255.255.0
No shutdow
*Do write m*emory

Step 10:





FE80::260:5CFF:FE3E:D6D0



10.10.10.2

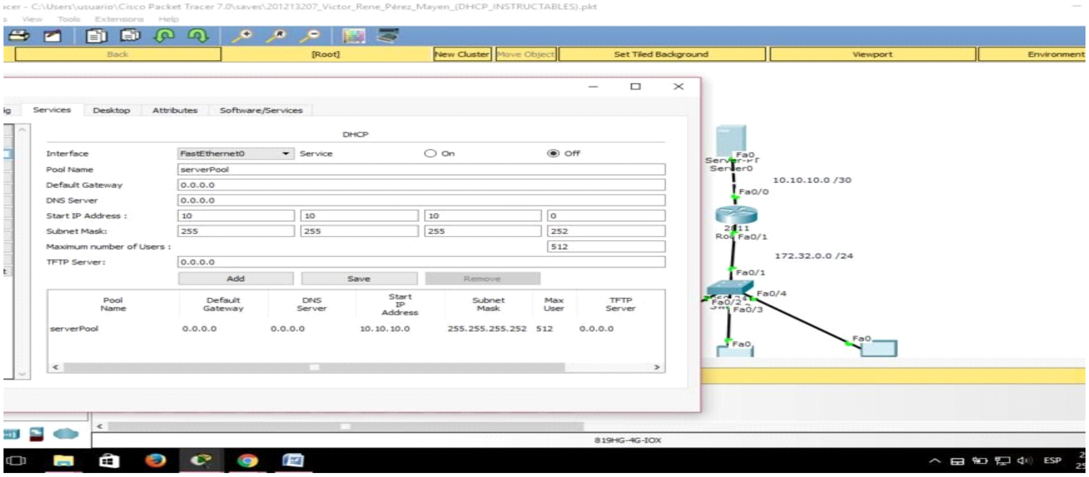
255.255.255.252

10.10.10.1

FE80::260:5CFF:FE3E:D6D0

Step 10: In this step, select the server by selecting and clicking the Desktop option, then selecting IP Configuration to place an IP address together with the Subnet Mask and its default Gateway that matches the physical interface of the Router that is connected.

Step 11:



DHCP

Interface: FastEthernet0 Service ○ On ● Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 10 10 10 0

Subnet Mask: 255 255 255 252

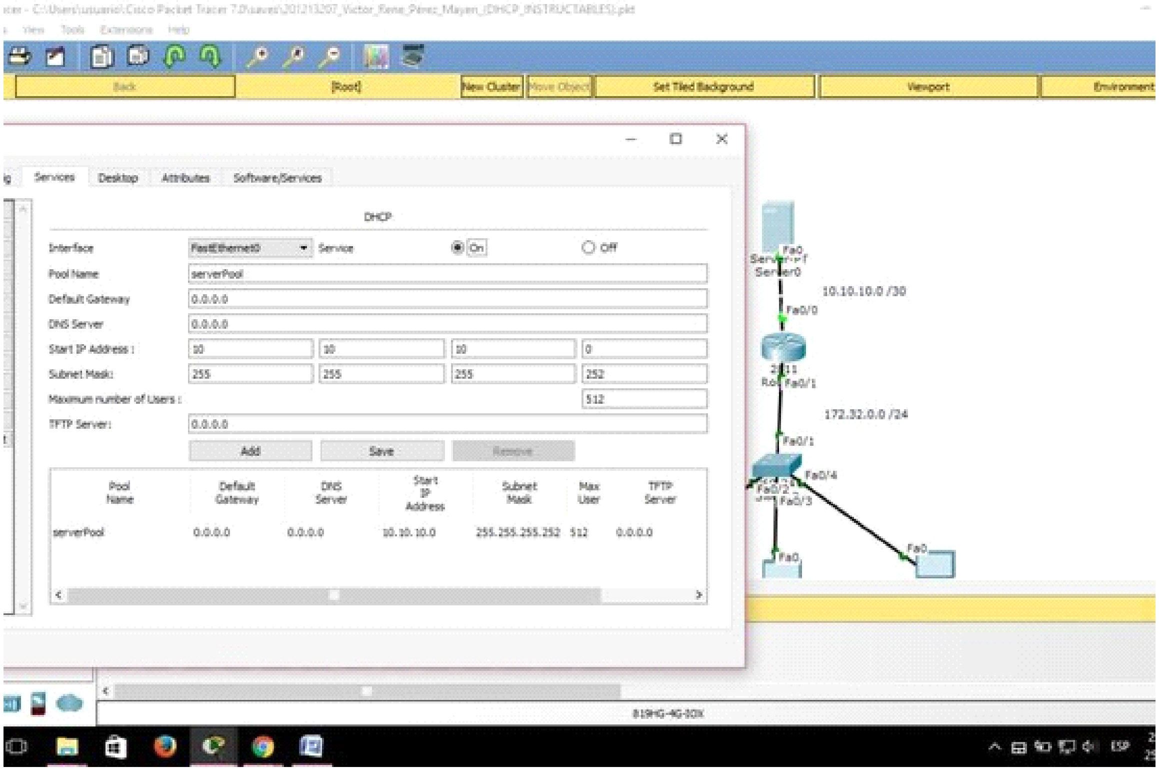
Maximum number of Users : 512

TFTP Server: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
serverPool	0.0.0.0	0.0.0.0	10.10.10.0	255.255.255.252	512	0.0.0.0

Step 11: Now select the Services option and then the DHCP service.

Step 12:



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

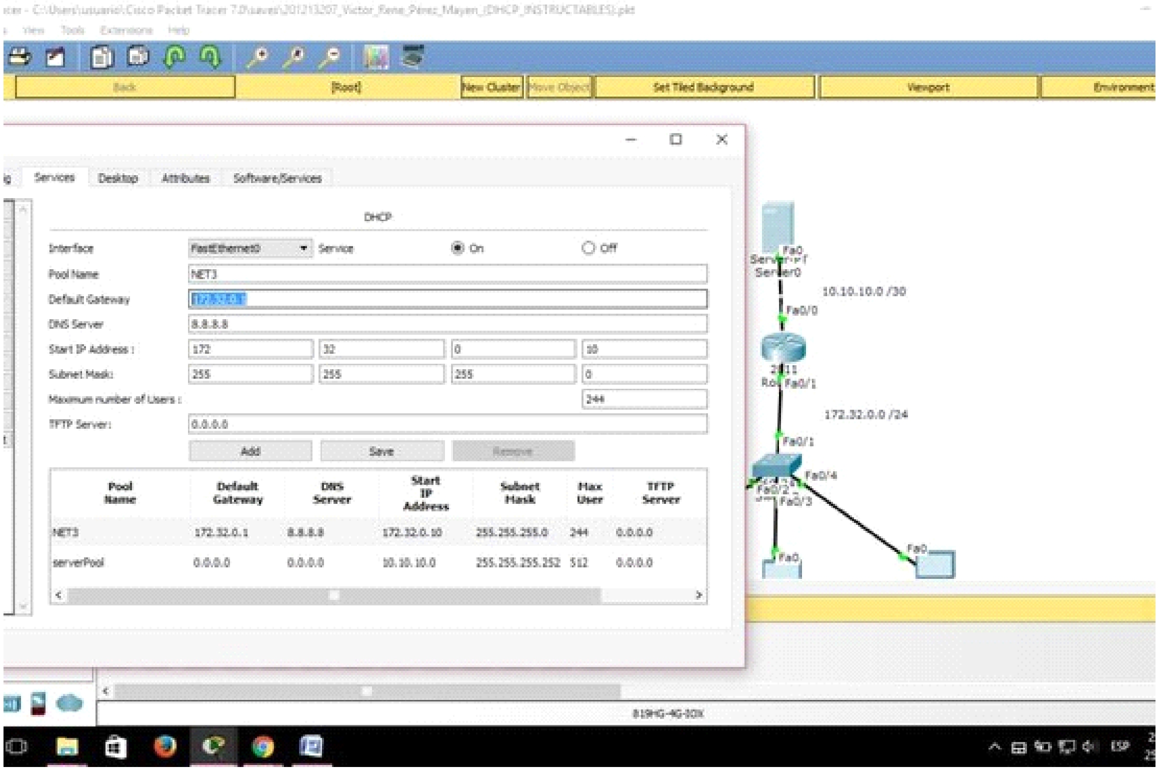
Start IP Address : 10 10 10 0

Subnet Mask: 255 255 255 252

Maximum number of Users : 512

TFTP Server: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
serverPool	0.0.0.0	0.0.0.0	10.10.10.0	255.255.255.252	512	0.0.0.0



DHCP

Interface: FastEthernet0 — Service: ● On ○ Off

Pool Name: NET3

Default Gateway: 172.32.0.1

DNS Server: 8.8.8.8

Start IP Address : 172 . 32 . 0 . 10

Subnet Mask: 255 . 255 . 255 . 0

Maximum number of Users : 244

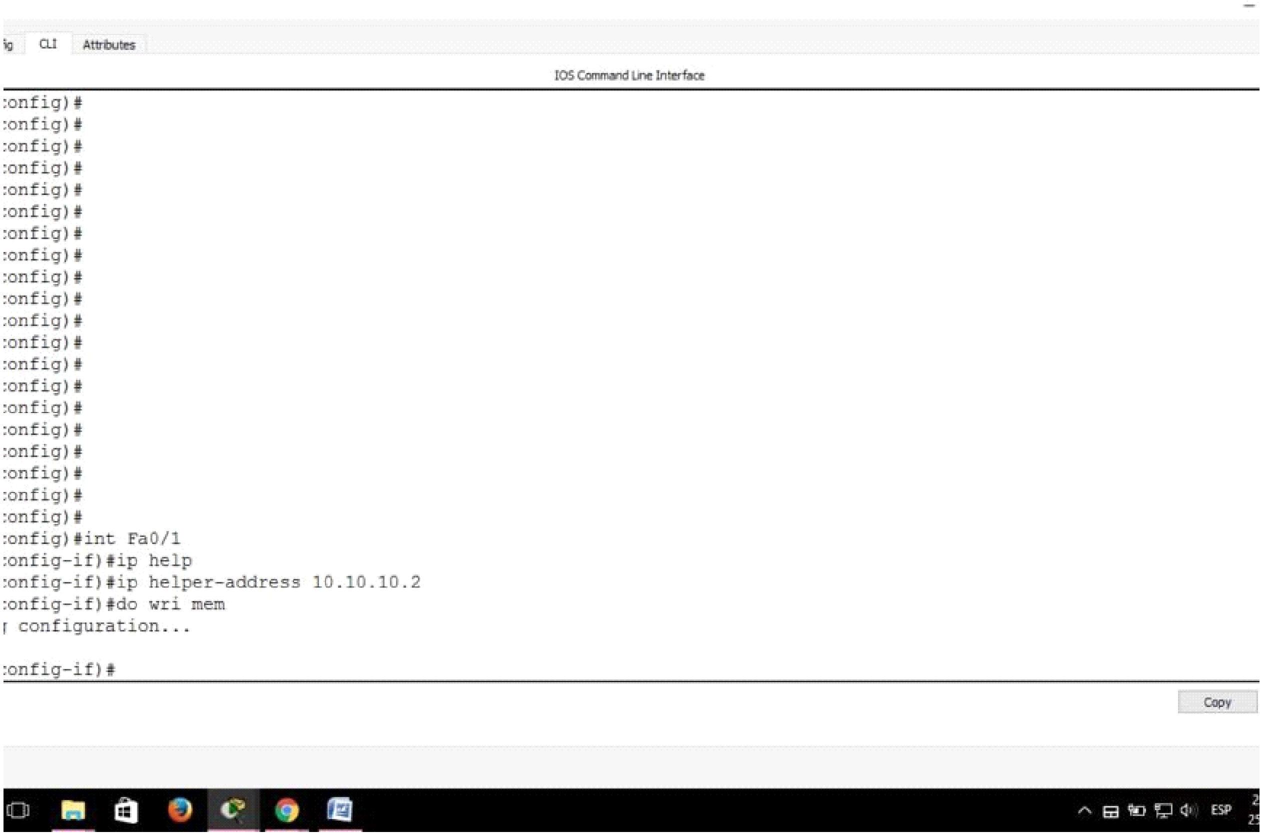
TFTP Server: 0.0.0.0

Add — Save — Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
NET3	172.32.0.1	8.8.8.8	172.32.0.10	255.255.255.0	244	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.10.10.0	255.255.255.252	512	0.0.0.0

Step 12: At this moment we have to select the option On to start the service and proceed to configure it, just like the DHCP programming on the router, it must match the network address we want to give you the service Ip addresses automatically.We must take into account that the Default Gateway must be the Ip address of the interface where we will request the service, when we have everything configured we will click the Add button and then the Save button.

Step 13:



```
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#
:onfig)#int Fa0/1
:onfig-if)#ip help
:onfig-if)#ip helper-address 10.10.10.2
:onfig-if)#do wri mem
g configuration...

:onfig-if)#
```

Step 13: Then we will return to the configuration of the router to require the DHCP service of the Server, for this we must note that the service will be requested based on the IP address of the Server. The commands to be used will be programmed in the global configuration.

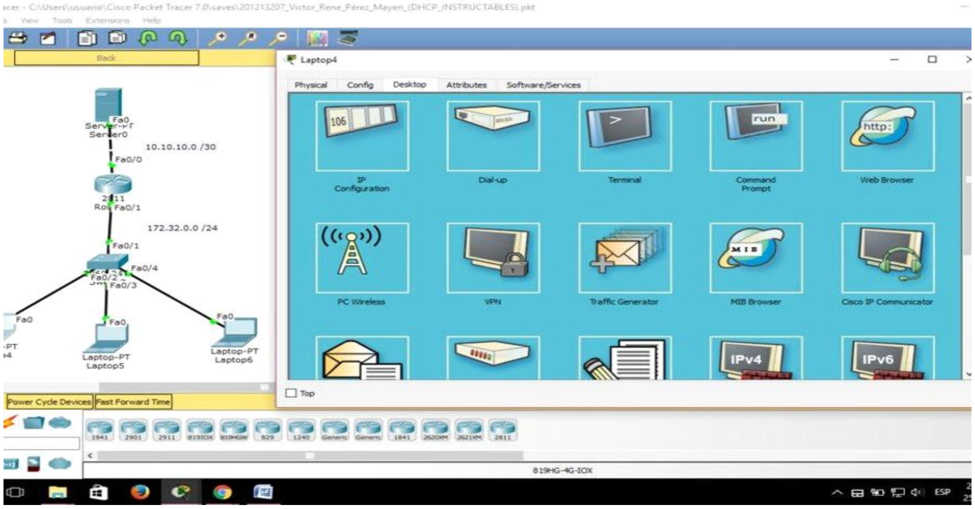
Int Fa0/1

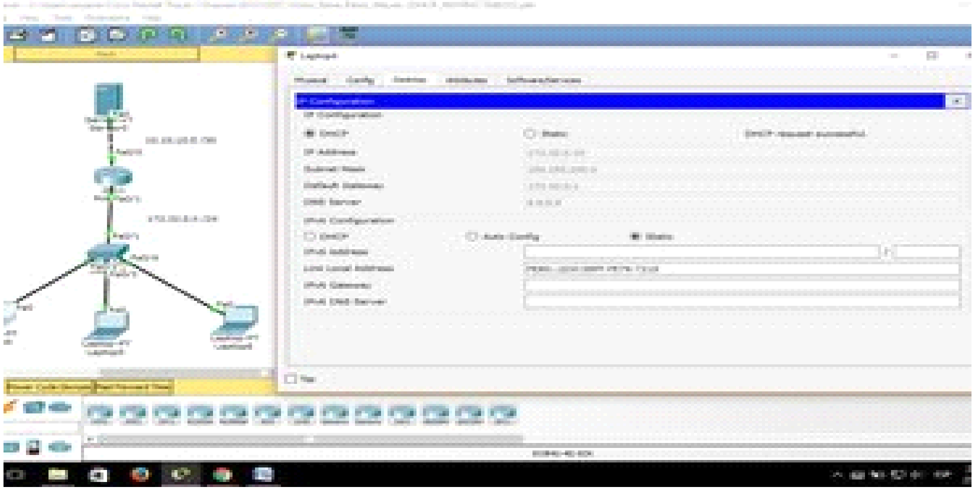
Ip helper-address 10.10.10.2

Do write memory

Step 14: Finally on a laptop select the option of Desktop and Ip Configuration, then select the DHCP option to receive the IP address automatically.
It should be remembered that if you do not give the address automatically you can implement the recommendations in Step 5.

Step 14:





Laptop4

IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address [illegible]

Subnet Mask 255.255.255.0

Default Gateway [illegible]

DNS Server 8.8.8.8

IPv6 Configuration

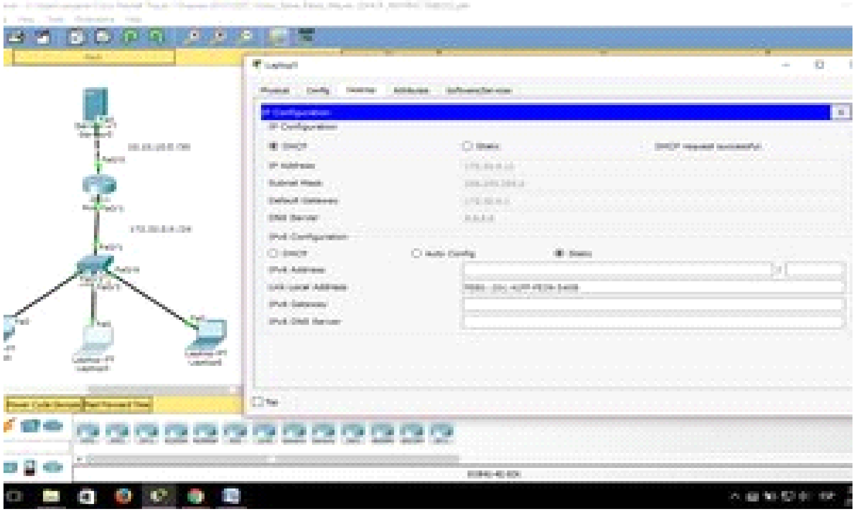
○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address [illegible]

IPv6 Gateway

IPv6 DNS Server



Laptop5

IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address [illegible]

Subnet Mask 255.255.255.0

Default Gateway [illegible]

DNS Server [illegible]

IPv6 Configuration

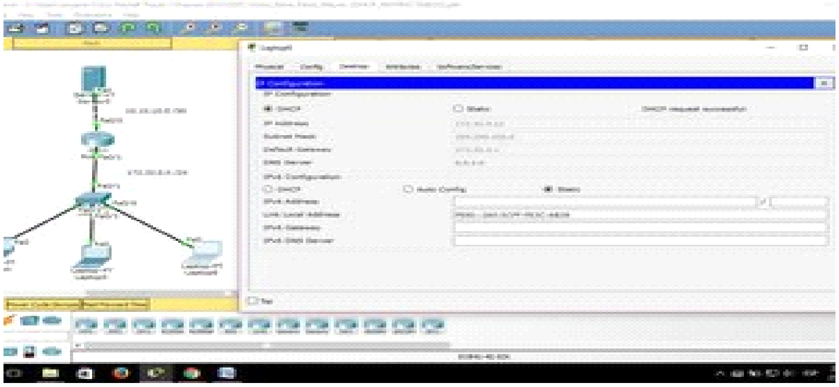
○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address [illegible]

IPv6 Gateway

IPv6 DNS Server



- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Network Interface Card	Manufacturer: Cisco
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
3.	Switch (min. 8 ports)	8 ports
4.	Any other Resource	

- **Result/Conclusion**

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

………………

- **Practical Related Questions**
- Which task does DHCP perform?
- What is DHCP?
- List some benefits of using DHCP.
- What is DHCP spoofing?
- Can DHCP support remote access?

(Space for Answer)

…………………………………………………………………………………………………

……

…………………………………………………………………………………………………

…………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

…………………………………………………………………

………………………………………………………………………………………………
……

- **References/ Suggestions for further Reading**

  https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

………………………………………………..

………………………………………………..

…………………………………………..........

Marks Obtained			Dated Signature of Teacher
Process Related(35)	**Product Related (15)**	**Total(50)**	

………………………………………………..

Practical No.09: Configure Domain Name Server (DNS) using relevant software

- **Practical Significance**
  - Student should be able to configure Domain Name Server
- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**
  - Ability to configure Domain Name Server
- **Relevant Course Outcomes**

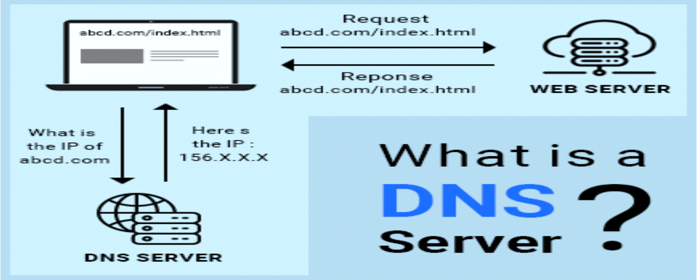
  Implement DNS
- **Practical Outcomes (POs)**

  Understand configuration of DNS
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Proposition 1.

DNS or Domain Name System is what lets you (and other internet users) connect to websites. The primary intent of DNS is to convert Internet domain names and hostnames such as those in URLs from a Web browser - into IP addresses

- **Diagrams / Experimental set-up /Work Situation**



- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		

- **Procedure**

This step-by-step guide describes how to configure Domain Name System (DNS) for Internet access in the Windows Server2003 products. DNS is the core name resolution tool that is used on the Internet. DNS handles resolution between host names and Internet addresses.

How to Start with a Stand-Alone Server Running Windows Server 2003

The stand-alone server running Windows Server 2003 becomes a DNS server for your network. In the first step, you assign this server a static Internet Protocol (IP) address. DNS servers must not use dynamically assigned IP addresses because a dynamic change of address could cause clients to lose contact with the DNS server.

Step 1: Configure TCP/IP

- Click Start, point to Control Panel, point to Network Connections, and then click Local Area Connection.
- Click Properties.
- Click Internet Protocol (TCP/IP), and then click Properties.
- Click the General tab.
- Click **Use the following IP address**, and then type the IP address, subnet mask, and default gateway address in the appropriate boxes.

- Click Advanced, and then click the DNS tab.
- Click **Append primary and connection specific DNS suffixes**.
- Click to select the **Append parent suffixes of the primary DNS suffix** check box.
- Click to select the **Register this connection's addresses in DNS** check box.

  Note that DNS servers running Windows Server 2003 must point to themselves for DNS. If this server needs to resolve names from its Internet service provider (ISP), you must configure a forwarder. Forwarders are discussed in the How to Configure Forwarders section later in this article.
- Click OK three times.

  NOTE: If you receive a warning from the DNS Caching Resolver service, click OK to dismiss the warning. The caching resolver is trying to contact the DNS server, but you have not finished configuring the server.

Step 2: Install Microsoft DNS Server

- Click Start, point to Control Panel, and then click **Add or Remove Programs**.
- Click **Add or Remove Windows Components**.
- In the Components list, click Networking Services (but do not select or clear the check box), and then click Details.
- Click to select the **Domain Name System (DNS)** check box, and then click OK.
- Click Next.
- When you are prompted, insert the Windows Server 2003 CD-ROM into the computer's CD-ROM or DVD-ROM drive.
- On the **Completing the Windows Components Wizard** page, click Finish when Setup is complete.
- Click Close to close the **Add or Remove Programs**window.

Step 3: Configure the DNS Server

To configure DNS by using the DNS snap-in in Microsoft Management Console (MMC), follow these steps:

Click Start, point to Programs, point to Administrative Tools, and then click DNS.

- Right-click Forward lookup zones, and then click New Zone
- When the New Zone Wizard starts, click Next.

  You are prompted for a zone type. The zone types include:

  - Primary zone: Creates a copy of a zone that can be updated directly on this server. This zone information is stored in a .dns text file.

  - Secondary zone: A standard secondary zone copies all of the information from its master DNS server. A master DNS server can be an Active Directory, primary, or secondary zone that is configured for zone transfers. Note that you cannot modify the zone data on a secondary DNS server. All of its data is copied from its master DNS server.
  - Stub zone: A Stub zone contains only those resource records that are necessary to identify the authoritative DNS servers for that zone. Those resource records include Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records.

  There is also an option to the store zone in Active Directory. This option is only available if the DNS server is a Domain controller.

- The new forward lookup zone must be a primary or an Active Directory-integrated zone so that it can accept dynamic updates. Click Primary, and then click Next.
- The new zone contains the locator records for this Active Directory-based domain. The name of the zone must be the same as the name of the Active Directory-based domain, or be a logical DNS container for that name. For example, if the Active Directory-based domain is named "support.microsoft.com", valid zone names are "support.microsoft.com" only.

  Accept the default name for the new zone file. Click Next.

  NOTE: Experienced DNS administrators may want to create a reverse lookup zone, and are encouraged to explore this branch of the wizard. A DNS server can resolve two basic requests: a forward lookup and a reverse lookup. A forward lookup is more common. A forward lookup resolves a host name to an IP address with an "A" or Host Resource record. A reverse lookup resolves an IP address to a host name with a PTR or Pointer Resource record. If you have your reverse DNS zones configured, you can automatically create associated reverse records when you create your original forward record.

How to Remove the Root DNS Zone

A DNS server running Windows Server 2003 follows specific steps in its name-resolution process. A DNS server first queries its cache, it checks its zone records, it sends requests to forwarders, and then it tries resolution by using root servers.

By default, a Microsoft DNS server connects to the Internet to process DNS requests more with root hints. When you use the Dcpromo tool to promote a server to a domain controller, the domain controller requires DNS. If you install DNS during the promotion process, a root zone is created. This root zone indicates to your DNS server that it is a root Internet server. Therefore, your DNS server does not use forwarders or root hints in the name-resolution process.

Click Start, point to Administrative Tools, and then click DNS.

- Expand **ServerName**, where **ServerName** is the name of the server, click Properties and then expand Forward Lookup Zones.

- Right-click the "." zone, and then click Delete.

How to Configure Forwarders

Windows Server 2003 can take advantage of DNS forwarders. This feature forwards DNS requests to external servers. If a DNS server cannot find a resource record in its zones, it can send the request to another DNS server for additional attempts at resolution. A common scenario might be to configure forwarders to your ISP's DNS servers.
Click Start, point to Administrative Tools, and then click DNS.

- Right-click **ServerName**, where **ServerName** is the name of the server, and then click the Forwarderstab.
- Click a DNS domain in the DNS domain list. Or, click New, type the name of the DNS domain for which you want to forward queries in the DNS domain box, and then click OK.
- In the **Selected domain's forwarder IP address** box, type the IP address of the first DNS server to which you want to forward, and then click Add.
- Repeat step 4 to add the DNS servers to which you want to forward.
- Click OK.

How to Configure Root Hints

Windows can use root hints. The Root Hints resource records can be stored in either Active Directory or in a text file (%SystemRoot%\System32\DNS\Cache.dns). Windows uses the standard Internic root server. Also, when a server running Windows Server 2003 queries a root server, it updates itself with the most recent list of root servers.
Click Start, point to Administrative Tools, and then click DNS.

- Right-click **ServerName**, where **ServerName** is the name of the server, and then click Properties.
- Click the Root Hints tab. The DNS server's root servers are listed in the **Name servers** list.

  If the Root Hints tab is unavailable, your server is still configured as a root server. See the How to Remove the Root DNS Zone section earlier in this article. You may have to use custom root hints that are different from the default. However, a configuration that points to the same server for root hints is always incorrect. Do not modify your root hints. If your root hints are incorrect and have to be replaced, click the following article number to view the article in the Microsoft Knowledge Base:

  Setting up the Domain Name System for Active Directory

How to Configure DNS Behind a Firewall

Proxy and Network Address Translation (NAT) devices can restrict access to ports. DNS uses UDP port 53 and TCP port 53. The DNS Service Management console also uses RCP.

RCP uses port 135. These are potential issues that may occur when you configure DNS and firewalls.

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Network Interface Card	Manufacturer: Cisco
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
3.	Switch (min. 8 ports)	8 ports
4.	Any other Resource	

- **Result/Conclusion**

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

………………

- **Practical Related Questions**
  - What is DNS?
  - How DNS works?
- **Exercise**
  - Configure DNS server

(Space for Answer)

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

....
....
....

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

....
....
....
....
....
....
....

- **References/ Suggestions for further Reading**

  https://cloudacademy.com/blog/how-dns-works/

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**

2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

………………………………………………..

………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

………………………………………….........

……………………………………………….

Practical No.10: a)Configure File Transfer Protocol (FTP) using relevant software

- **Practical Significance**

Know the use of FTP

Create FTP Environment

- **Relevant Programs Outcomes (POs)**

- **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**
  - Create FTP Environment using simulator
- **Relevant Course Outcomes**

  Configure FTP Network
- **Practical Outcomes (POs)**

  FTP environment
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Users can upload, download, rename, or delete files on an FTP server using an FTP client. This kind of program establishes the TCP connection to the port of a server; this allows **data exchange** to be controlled with the help of commands. Many internet browsers have an integrated client, but dedicated FTP programs for Windows, macOS, and other operating systems make transferring data with FTP a more manageable task.

- **How file transfer works with the file transfer protocol**

In order to reach an FTP server, a connection through an FTP client first needs to be established. This FTP client creates a TCP connection to the control port of the server (normally port 21) and is then able to send commands that the server subsequently answers. Following this, the data is transferred through another port. At this point, it’s important to differentiate between two **different types of transfer modes**. In active mode, the client, which uses port 1023, signals its IP address through port 21 during connection buildup. This process informs the server which port the client can be reached on. In passive mode, the server does not receive an IP address from the client (due to a firewall, for example) and offers the client a port through which a connection can be established.

Those using web-hosting solutions with FTP accounts profit from the quick and easy data transmission between the device and the web server. FTP software further assists these solutions by providing a sleek **user interface** that browser-based clients lack. FTP programs let the user sort and manage files into the existing directory structure with speed and ease. Administrators control the access rights of users who are able to simultaneously access the FTP server.

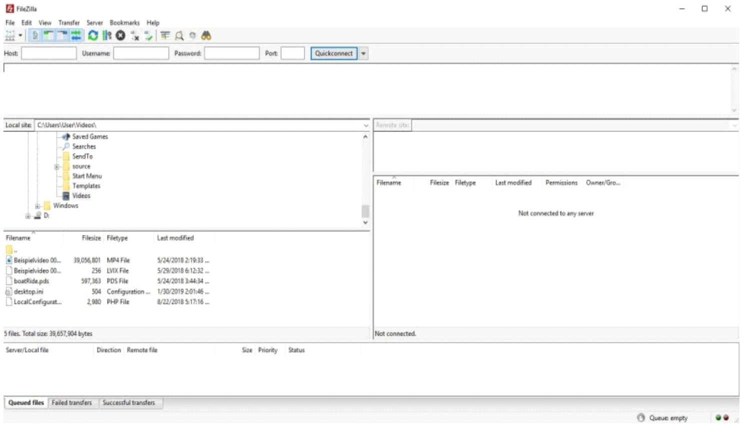
There are many FTP programs currently available on the market. Their use as well as many of their functions can also vary quite strongly from one another. Some are free, while others are fee based. Their operating systems differ as well: Windows,macOS, or Linux are all available. We've laid out five programs for you.

	Release year	**Developer**	**Platform**	**Price**
Cyberduck	2002	Iterate	Windows, macOS	free
FileZilla	2001	Tim Kosse	Windows, macOS, Linux	free
FireFTP	2004	Mime Čuvalo	Mutli-platform	free
Fresh FTP	2005	FreshWebmaster.com	Windows	free
SmartFTP	2001	SmartSoft Ltd.	Windows	from 39,99 $ / yrsyear
WinSCP	2000	Martin Přikryl	Windows	free
WISE-FTP	1998	AceBIT	Windows	40 $ approx

FileZilla

It is not without reason that FileZilla is the most popular FTP application on the market. The open source software is free of charge and available for Windows 7 and beyond, Linux, and macOS. As soon as a connection is established, data is then ready to be easily exchanged between client and server via a drag-and-drop feature. FileZilla also supports large data transfers (over 4 GB) and is also able to resume terminated file transfers. Users can set up upload and download speeds themselves and the server manager function allows the used FTP server, including access information, to be saved. With FileZilla, users have the option of encrypting the FTP via SSL/TLS or SSH. FileZilla at a glance:

- compatible with Windows, Linux, and macOS
- supports SSL and SSH encryption
- configurable transfer speeds
- enables connection to FTP proxy servers
- Keepalive system for network connection maintenance



Local site: C:\Users\User\Videos\

Filename	Filesize	Filetype	Last modified
..			
Beispielvideo 00...	39,056,801	MP4 File	5/24/2018 2:19:33 ...
Beispielvideo 00...	256	LVIX File	5/29/2018 6:12:32 ...
boatRide.pds	597,363	PDS File	5/24/2018 3:44:34 ...
desktop.ini	504	Configuration ...	1/30/2019 2:01:46 ...
LocalConfigurat...	2,980	PHP File	8/22/2018 5:17:16 ...

5 files. Total size: 39,657,904 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...

Not connected to any server

Not connected.

Server/Local file	Direction	Remote file	Size	Priority	Status

Queue: empty

You can use the server manager in FileZilla to store the address and access data of FTP servers.

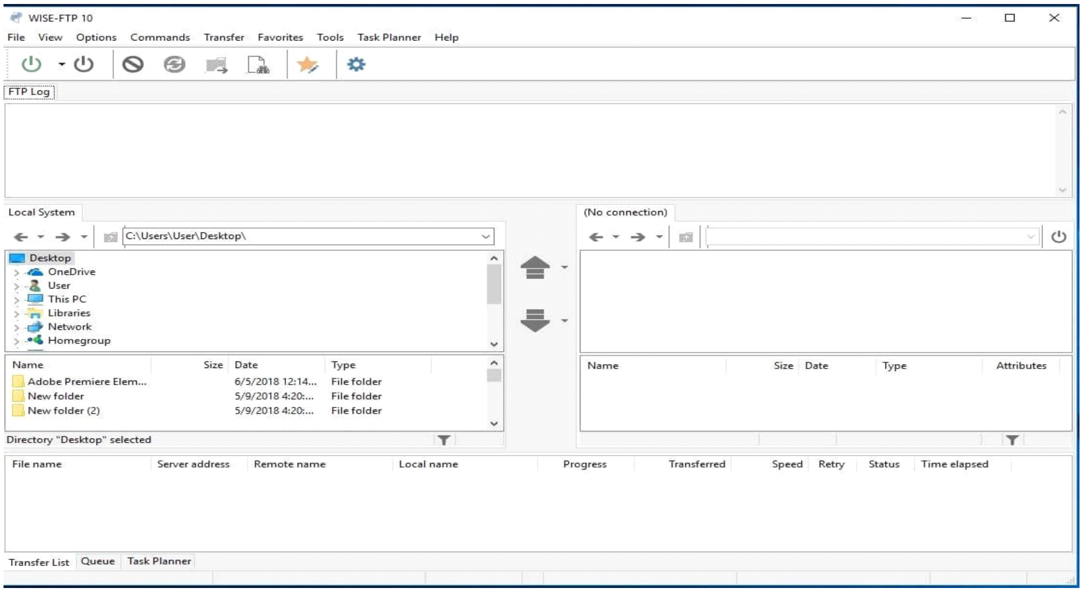
WISE-FTP

WISE-FTP is a paid FTP program for Windows operating systems (XP or higher), which can be tested free of charge for 30 days before purchase without any restrictions. The software supports all common protocols like **FTP, SFTP, FTPS or FTPES** and thus allows the connection to any FTP server. Thanks to the integrated task planner, the upload and download of files can be **completely automated with WISE-FTP**: Users only have to define the target server and when and how often a certain task should be executed. Both authentication and file transfer are subject to maximum security thanks to the SFTP or FTPS protocol. In addition, the data can be encrypted via Rijndael, BlowFish or TripleDES. The features of the FTP client at a glance:

- Compatible with Windows
- Data encryption possible (Rijndael, BlowFish, TripleDES)
- Integrated task planner
- Powerful FTP synchronization
- User-defined, storable key combinations
- Adjustable upload and download speed

WISE-FTP presents the directory overview of the local system and that of the FTP server to which a connection has been established directly next to each other.

- **Diagrams / Experimental set-up /Work Situation**



C:\Users\User\Desktop\

Name	Size	Date	Type
Adobe Premiere Elem...		6/5/2018 12:14...	File folder
New folder		5/9/2018 4:20:...	File folder
New folder (2)		5/9/2018 4:20:...	File folder

Directory "Desktop" selected

- **Resources Required**

Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		

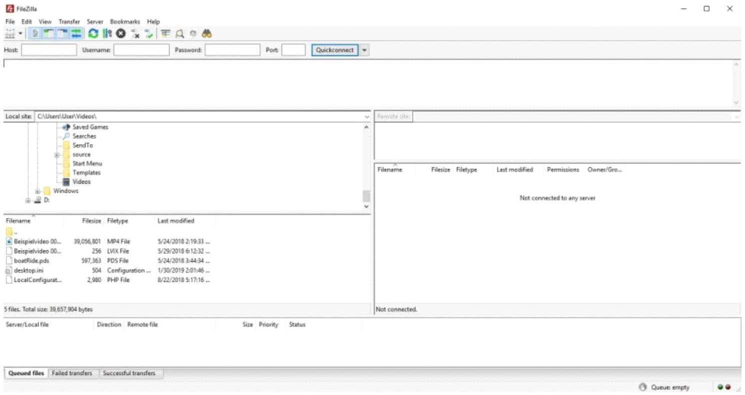
4.	Crossover Cable			

- **Procedure**

FileZilla

It is not without reason that FileZilla is the most popular FTP application on the market. The open source software is free of charge and available for Windows 7 and beyond, Linux, and macOS. As soon as a connection is established, data is then ready to be easily exchanged between client and server via a drag-and-drop feature. FileZilla also supports large data transfers (over 4 GB) and is also able to resume terminated file transfers. Users can set up upload and download speeds themselves and the server manager function allows the used FTP server, including access information, to be saved. With FileZilla, users have the option of encrypting the FTP via SSL/TLS or SSH. FileZilla at a glance:

- compatible with Windows, Linux, and macOS
- supports SSL and SSH encryption
- configurable transfer speeds
- enables connection to FTP proxy servers
- Keepalive system for network connection maintenanc



Filename	Filesize	Filetype	Last modified
..			
Beispielvideo 00...	39,056,801	MP4 File	5/24/2018 2:19:33 ...
Beispielvideo 00...	256	LVIX File	5/29/2018 6:12:32 ...
boatRide.pds	597,363	PDS File	5/24/2018 3:44:34 ...
desktop.ini	504	Configuration ...	1/30/2019 2:01:46 ...
LocalConfigurat...	2,980	PHP File	8/22/2018 5:17:16 ...

5 files. Total size: 39,657,904 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...

Not connected to any server

Not connected.

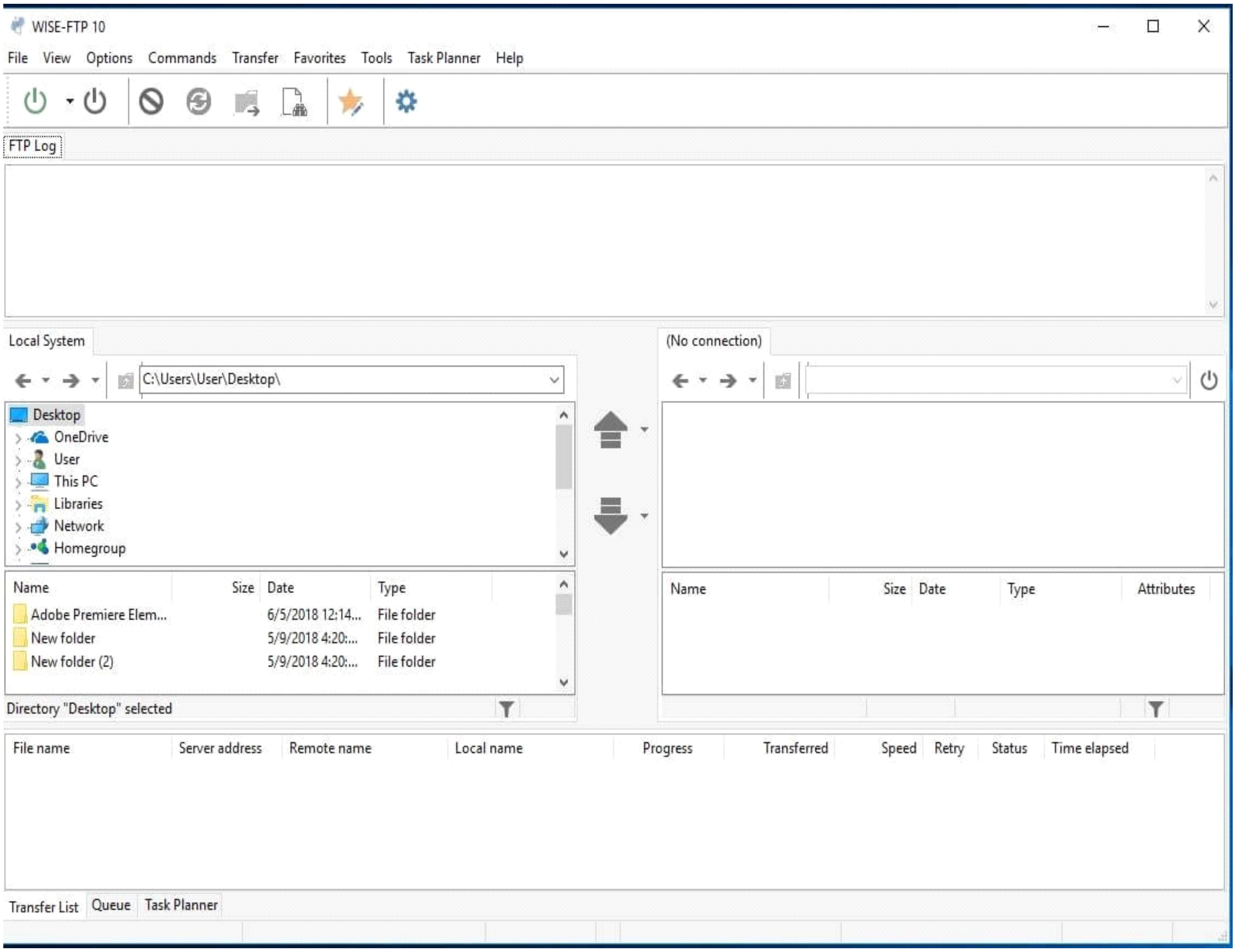
Server/Local file	Direction	Remote file	Size	Priority	Status

You can use the server manager in FileZilla to store the address and access data of FTP servers.

WISE-FTP

WISE-FTP is a paid FTP program for Windows operating systems (XP or higher), which can be tested free of charge for 30 days before purchase without any restrictions. The software supports all common protocols like **FTP, SFTP, FTPS or FTPES** and thus allows the connection to any FTP server. Thanks to the integrated task planner, the upload and download of files can be **completely automated with WISE-FTP**: Users only have to define the target server and when and how often a certain task should be executed. Both authentication and file transfer are subject to maximum security thanks to the SFTP or FTPS protocol. In addition, the data can be encrypted via Rijndael, BlowFish or Triple DES. The features of the FTP client at a glance:

- Compatible with Windows
- Data encryption possible (Rijndael, BlowFish, TripleDES)
- Integrated task planner
- Powerful FTP synchronization
- User-defined, storable key combinations
- Adjustable upload and download speed



C:\Users\User\Desktop\

Name	Size	Date	Type
Adobe Premiere Elem...		6/5/2018 12:14...	File folder
New folder		5/9/2018 4:20:...	File folder
New folder (2)		5/9/2018 4:20:...	File folder

Directory "Desktop" selected

Name	Size	Date	Type	Attributes

File name	Server address	Remote name	Local name	Progress	Transferred	Speed	Retry	Status	Time elapsed

WISE-FTP presents the directory overview of the local system and that of the FTP server to which a connection has been established directly next to each other.

b) Configure Hyper Text Transfer Protocol (HTTP) using relevant software

- **Practical Significance**

  Know the use of HTTP

  Create HTTP Environment

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
  - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
  - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
  - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**
  - Create HTTP Environment using simulator
- **Relevant Course Outcomes**

  Configure HTTP Network

- **Practical Outcomes (POs)**

  HTTP environment

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices

Minimum Theoretical Background

Note

These instructions assume that you are setting up an Oracle Linux 6 system as an Apache HTTP server.

To set up an HTTP server:

- Install the Apache HTTP server package.

  ```
  # yum install httpd
  ```

- Create the directory where you will copy the full Oracle Linux Release 6 Media Pack DVD image, for example /var/www/html/OSimage/OL6.6:

  ```
  # mkdir -p /var/www/html/OSimage/OL6.6
  ```

  Note

  If SELinux is enabled in enforcing mode on your system, create the directory under the /var/www/html directory hierarchy so that the httpd_sys_content_t file type is set automatically on all the files in the repository.

- Edit the HTTP server configuration file, /etc/httpd/conf/httpd.conf, as follows:
  - Specify the resolvable domain name of the server in the argument to ServerName.

    ```
    ServerName server_addr:80
    ```

    If the server does not have a resolvable domain name, enter its IP address instead. For example, the following entry would be appropriate for an HTTP server with the IP address 192.168.1.100.

    ```
    ServerName 192.168.1.100:80
    ```

  - If the directory to which you will copy the DVD image in not under /var/www/html, change the default setting of DocumentRoot.

    In this example, the DVD image will be copied to /var/www/html/OSimage/OL6.6 so the setting of DocumentRoot can remain unchanged.

    ```
    DocumentRoot "/var/www/html"
    ```

  - Verify that the <Directory> setting points to the same setting as DocumentRoot.
  - #
  - # This should be changed to whatever you set DocumentRoot to.
  - #

    ```
    <Directory "/var/www/html">
    ```

  - If you want to be able to browse the directory hierarchy, verify that the Options directive specifies the Indexes option, for example:

```
Options Indexes FollowSymLinks
```

Note

The Indexes option is not required for installation.

- Save your changes to the file.

- Start the Apache HTTP server, and configure it to start after a reboot.
-
```
# service httpd start
# chkconfig httpd on
```

- If you have enabled a firewall on your system, configure it to allow incoming HTTP connection requests on TCP port 80.

  For example, the following command configures iptables to allow incoming HTTP connection requests and saves the change to the firewall configuration:

```
# iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
# service iptables save
```

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resource	

- **Result/Conclusion**

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………

- **Practical Related Questions**
  - What is FTP?
  - Draw a diagram for FTP
  - Which Port numbers are used for FTP?

- What is the use of HTTP

- **Exercise**

1.Configure FTP and HTTP

(Space for Answer)

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

- **References/ Suggestions for further Reading**

https://www.cloudwards.net/what-is-ftp/

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**

Total(50 Marks)	**100%**

- **List of Students/Team Members**

……………………………………………..

……………………………………………..

…………………………………….........

…………………………………….........

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.11: a) Use telnet to login a remote machine

- **Practical Significance**

  Student should be able to study how to login remote machine using Telnet

- **Relevant Programs Outcomes (POs)**
  - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
  - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.

- **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**

  To understand telnet basics.

  To study Telnet connections.

- **Relevant Course Outcomes**

  Configure various application layer protocols.

- **Practical Outcomes (POs)**

  Understand basic of Telnet.

  Understand networking commands.

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

  Proposition 1.

Telnet

Telnet is a network protocol that allows a user to communicate with a remote device. It is a virtual terminal protocol used mostly by network administrators to remotely access and manage devices. Administrator can access the device by *telnetting* to the IP address or hostname of a remote device.

To use telnet, you must have a software (Telnet client) installed. On a remote device, a Telnet server must be installed and running. Telnet uses the TCP port 23 by default.

One of the greatest disadvantages of this protocol is that all data, including usernames and passwords, is sent in clear text, which is a potential security risk. This is the main reason why Telnet is rarely used today and is being replaced by a much secure protocol called SSH. Here you can find information about setting up Telnet access on your Cisco device.

Opening a TELNET Session

Run the Client-TELNET utility to connect to a remote host. Client-TELNET supports as many as 10 connected sessions at any one time. However, of these ten sessions, only one can be a TN3270 session. To open a TELNET session (see Example 12-1):

1 At the DCL prompt, enter: `$ TELNET`

2 Use the OPEN command to open a remote TELNET session in one of the following ways:

a To use standard authentication, at the TELNET> prompt, enter either:

```
TELNET>OPEN host
TELNET>OPEN host /AUTH=NULL
```

—*host* is the name of the host to which you want to connect. /AUTH=NULL explicitly specifies to use standard authentication.

b To use Kerberos version 4 authentication, enter at the `TELNET>` prompt:

TELNET> **OPEN *host* /AUTH=KERBV4 /REALM=*realm***

—*host* is the name of the host to which you want to connect.

–`/AUTH=KERBV4` specifies the use of Kerberos version 4 authentication.

–`/REALM=realm` specifies the name of the Kerberos Server realm.

You must first get a ticket-granting ticket (TGT) from the Kerberos Server. (See Chapter 4, *Kerberos User Commands.*)

You can specify the Kerberos realm using the /REALM qualifier. If you omit the qualifier, the contents of the TCPWARE:KRB.REALMS file determines the Kerberos realm.

To open a connection, TELNET first tries to use Kerberos version 4 authentication if requested, then reverts to standard authentication if Kerberos version 4 authentication fails.

3 Respond to the login prompts, if any, of the remote host, including any PASSCODE.

4 Open another session if desired:

a Return to the local TELNET prompt by entering the escape sequence displayed when opening the connection (usually **`Ctrl/\`**). The previous session remains open.

b Use the OPEN command to open the next session. Repeat steps 2 and 3.

Alternative method. You can also open a remote TELNET connection as follows:

```
$ TELNET host
```

See the OPEN, CLOSE, and EXIT commands in the *Command Reference*.

Example 12-1 **Opening Multiple TELNET Sessions**

```
(IRIS) $ TELNET
TELNET>OPEN BART
%TCPWARE_TELNET-I-TRYING, trying bart.nene.com,telnet(192.168.1.92,23)...
%TCPWARE_TELNET-I-ESCAPE, escape (attention) character is "^\"
```

(login procedure to BART)

```
(BART) $ Ctrl/\

TELNET> OPEN MARGE                    [BART remains open]
%TCPWARE_TELNET-I-TRYING, trying marge.nene.com,telnet
(192.168.1.91,23)...
%TCPWARE_TELNET-I-ESCAPE, escape character is "^\"
```

(login procedure to MARGE)

```
(MARGE) $ Ctrl/\

TELNET>OPEN HOMER                           [BART and MARGE remain open]
%TCPWARE_TELNET-I-TRYING, trying homer.nene.com,telnet
(192.168.1.90,23)...
%TCPWARE_TELNET-I-ESCAPE, escape character is "^\"
```

(login procedure to HOMER)

```
(HOMER) $ Ctrl/\
TELNET> OPEN LISA        [BART, MARGE, and HOMER remain open]
%TCPWARE_TELNET-I-TRYING, trying lisa.nene.com,telnet
(192.168.1.89,23)...
%TCPWARE_TELNET-I-ESCAPE, escape character is "^\"
```

(login procedure to LISA)

```
(LISA) $ Ctrl/\

TELNET> OPEN /AUTH=KERBV4 /REALM=SIMPSONS.COM MAGGIE
%TELNET-I-TRYING, trying maggie.yours.com,telnet (192.168.99.1,23)...
%TELNET-I-ESCCHR, escape (attention) character is "^\"
(MAGGIE) $
```

Note! TCPware provides secure TELNET-OpenVMS logins through its Token Authentication feature, if installed and enabled. For more information, see Chapter 14, *Token Authentication: Protecting Logins*.

Opening a TN3270 Session

Client-TELNET supports TN3270 mode for local OpenVMS terminals. The remote IBM host must support a TELNET server.

You can only connect one TN3270 session at any one time. Client-TELNET returns an error message if you try to open more than one TN3270 session.

To open a TELNET session in TN3270 mode (see Example 12-2):

1 At the DCL prompt, enter: `$` **`TELNET`**

2 Use the OPEN command at the TELNET> prompt: `TELNET>`***`OPEN host`*** *`[`***`/TN3270`***`]`*

TELNET servers that cannot automatically negotiate this mode require the /TN3270 qualifier.

3 Enter the TN3270 escape sequence **`Ctrl/C`** instead of **`Ctrl/\`**.

4 If you want to print a screen in TN3270 mode, add the /PRINT qualifier as follows:

TELNET>**OPEN *host* /TN3270 /PRINT=(FILE=*filename* | QUEUE=*qname*)**

SeeTN3270 Screen Printing and Dumping.

5 Only one TN3270 session can be open at any given time. If you try to open more than one TN3270 session, Client-TELNET returns an error message.

Table 12-1 lists the IBM terminal models and screen sizes Client-TELNET supports. To use the emulated model, your terminal must support the minimum size (number of rows and columns) indicated. DECwindows, DECterm, and virtual workstation (VWS) windows resize accordingly.

Table 12-1 **Supported IBM Models**

Emulated Model	**Minimum Size (rows x columns)**
IBM 3278-2	24 x 80
IBM 3278-3	32 x 80
IBM 3278-4	43 x 80
IBM 3278-5	27 x 132

Some Client-TELNET commands have specific meaning for TN3270 mode.

See *TN3270 Keyboard Mapping*.

Alternative method. You can also open a remote TELNET TN3270 connection by entering the following command:

```
$ TELNET host /TN3270
```

See the OPEN, CLOSE, and EXIT commands in the *Command Reference*.

Example 12-2 **Opening a TN3270 Session**

```
$ TELNET
TELNET>OPEN LOCIS.LOC.GOV
<Library of Congress menus displayed>
Ctrl/C

TELNET>CLOSE
TELNET>OPEN LOCIS.LOC.GOV /TN3270 /PRINT(=QUEUE=ENG_PRINTER_ASCII)
Ctrl/C

TELNET>OPEN BLUE.ADP.WISC.EDU /TN3270
%TCPWARE-TELNET-E-CONLOST, connection to remote host lost
%TCPWARE-TELNET-E-MAXTN3270, only one TN3270 session may be open at any
one time
%TCPWARE-TELNET-I-CURRSESSION, current session is not 1, LOCIS.LOC.GOV
TELNET>
```

Closing a Session

A TELNET session remains open until you log out of that session at the system prompt or use the CLOSE, EXIT, QUIT, or BYE commands or enter **Ctrl/Z** at the TELNET> prompt.

To close a TELNET session, use one of the following commands at the TELNET> prompt (see Example 12-3):

- TELNET>**CLOSE** closes the current session, as in the following chart:

If you open a TELNET session using...	And...	Then CLOSE closes the current session and...
Telnet>**OPEN *host***	It is the only session	Keeps you in TELNET
	There are other sessions	Keeps you in TELNET with the other sessions open
$ **TELNET *host***	It is the only session	Exits TELNET
	There are other sessions	Keeps you in TELNET with the other sessions open

  If you close the current session, and there are other connected sessions, Client-TELNET resets the current session to the "next" session.

- TELNET>**CLOSE *session-number***
  closes only the specified session, as indicated by the SHOW STATUS command.
- TELNET> **EXIT** exits TELNET
- TELNET>**QUIT** exits TELNET
- TELNET>**BYE** exits TELNET
- TELNET>**Ctrl/Z** interrupts TELNET

See the OPEN, CLOSE, EXIT, and SHOW STATUS commands in the *Command Reference*.

Example 12-3 **Closing TELNET Sessions**

```
(IRIS) $ TELNET
TELNET>OPEN BART
%TCPWARE_TELNET-I-TRYING, trying bart.nene.com,telnet(192.168.1.92,23)...
%TCPWARE_TELNET-I-ESCAPE, escape character is "^\"
```

(login procedure to BART)

```
(BART) $ Ctrl/\
TELNET> OPEN MARGE     [BART remains open]
```

```
%TCPWARE_TELNET-I-TRYING,trying marge.nene.com,telnet(192.168.1.91,23)...
%TCPWARE_TELNET-I-ESCAPE, escape character is "^\"
```

(login procedure to MARGE)

```
(MARGE) $ Ctrl/\
TELNET>SHOW STATUS
Client-TELNET V6.0-0 Copyright (c) Process Software
Connected sessions:
     1. bart.nene.com,telnet (192.168.1.92,23).
 --> 2.  marge.nene.com, telnet (192.168.1.91,23).
"^\" is the escape (attention) character

TELNET> CLOSE 2
%TCPWARE_TELNET-I-CONNCLOSED, closing session 2, marge.nene.com
TELNET>CLOSE 1
%TCPWARE_TELNET-S-CONNCLOSED, closing session 1,bart.nene.com
TELNET>EXIT
(IRIS) $
```

Issuing Local Commands

You can issue commands to the Client-TELNET utility during a remote session by returning to the TELNET prompt. You can then enter one or more TELNET commands.

TELNET OpenVMS features multiline recall of up to 20 command lines using the standard OpenVMS line recall and editing keys.

You return to the remote session by entering the RESUME command.

To issue a local TELNET command while connected to a remote host and then resume the session on the host (see Example 12-4):

1. Enter the escape (attention) character to return to the TELNET prompt: for example: **`Ctrl/\`**
2. Issue a TELNET command. For example, you may want to:
   - Issue the SHOW STATUS command. The SHOW STATUS command displays a list of open connections. The arrow (-->) identifies the current session.

   Change the escape (attention) character using the SET ESCAPE command.
3. Return to the remote host by entering: `TELNET>`**`RESUME`**

   This command resumes to the current remote host. Pressing **`Return`** or entering the OPEN command also resumes to the current remote host.

   To resume to a different session, enter: `TELNET>`**`RESUME`** ***`session-number`***

   – *session-number* is the number of the session which you want to resume. The session-number refers to a particular connection, as displayed by the SHOW STATUS command.

   You can switch between local TELNET command mode and the remote host as often as you like.

See the RESUME, SET ESCAPE, and SHOW STATUS commands in the *Command Reference*.

Example 12-4 **Issuing TELNET Commands and Resuming a Session**

```
(BART) $ Ctrl/\

TELNET>SHOW STATUS
Client-TELNET V6.0-0 Copyright (c) Process Software
Connected sessions:
          1. BART.nene.com,  telnet  (192.168.1.92,23).
                 2. HOMER.nene.com, telnet  (192.168.1.90,23).
                 3. MARGE.nene.com, telnet  (192.168.1.91,23).
          -->    4. LISA.nene.com,  telnet  (192.168.1.89,23).

"^\" is the escape (attention) character.
```

```
TELNET>SET ESCAPE "^A"
escape (attention) character is "^A"

TELNET>RESUME
(BART) $

(BART) $ Ctrl/\

TELNET>RESUME 2
%TCPWARE_TELNET-I-RESUME, resuming session 2, HOMER.illiad.com
(HOMER) $
```

Practical No.11: b)Connect remote machine using Secure Shell(SSH)

- **Practical Significance**

Student should be able to study how to connect remote machine using Secure Shell(SSH)

- **Relevant Programs Outcomes (POs)**
    - **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
    - **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
    - **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
    - **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
    - **Communication:** Communicate effectively in oral and written form.
- **Competency and Practical skills**

To understand SSH basics

To study SSH connections

- **Relevant Course Outcomes**

Configure various application layer protocols.

- **Practical Outcomes (POs)**

  Understand basic of Application layer.

  Understand networking basics of SSH.

- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

Proposition 1: Introduction

- Accessing machines remotely became a necessity a long time ago and we can barely imagine how it would be if we couldn't control computers from remote locations. There are many ways to establish a connection with a remote machine depending on the operating system you are running. The two most used protocols are:
- Secure Shell (SSH) for Linux-based machines
- Remote Desktop Protocol (RDP) for Windows-based machines
- The two protocols use the client and server applications to establish a remote connection. These tools allow you to gain access and remotely manage other computers, transfer files, and do virtually anything you can do while physically sitting in front of the machine.

Proposition 2: Prerequisites

Before you can **establish a secure remote desktop protocol** with a remote machine, there are a few basic requirements to meet:

- The remote computer must be turned on at all times and have a network connection.
- The client and server applications need to be installed and enabled.
- You need the IP address or the name of the remote machine you want to connect to.
- You need to have the necessary permissions to access the remote computer.
- Firewall settings need to allow the remote connection.

Secure Socket Shell, is a protocol which allows you to connect securely to a remote computer or a server by using a text-based interface.

When a secure SSH connection is established, a shell session will be started, and you will be able to manipulate the server by typing commands within the client on your local computer.

System and network administrators use this protocol the most, as well as anyone who needs to manage a computer remotely in a highly secure manner.

VIII. Procedure:

How Does SSH Work?

In order to establish an SSH connection, you need two components: a client and the corresponding server-side component. An SSH client is an application you install on the computer which you will use to connect to another computer or a server. The client uses the provided remote host information to initiate the connection and if the credentials are verified, establishes the encrypted connection.On the server's side, there is a component called an SSH daemon that is constantly listening to a specific TCP/IP port for possible client connection requests. Once a client initiates a connection, the SSH daemon will respond with the software and the protocol versions it supports and the two will exchange their identification data. If the provided credentials are correct, SSH creates a new session for the appropriate environment.

The default SSH protocol version for SSH server and SSH client communication is version 2.

How to Enable an SSH Connection

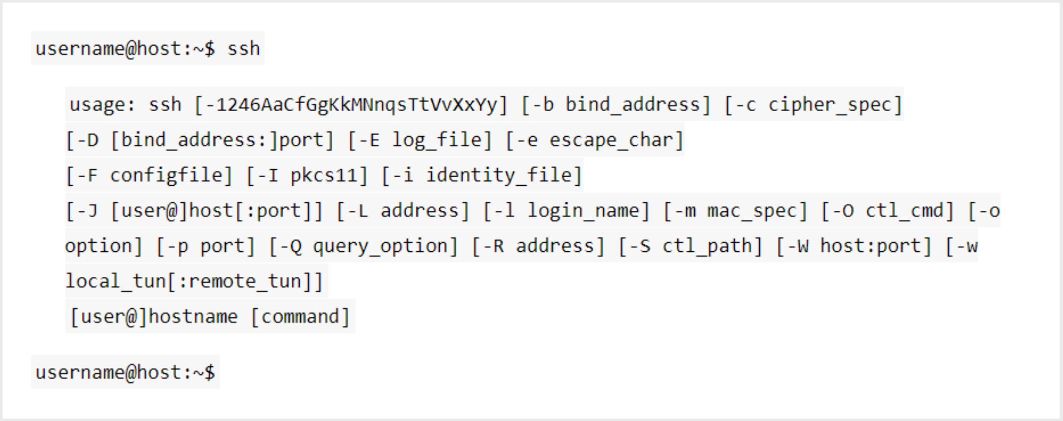
Since creating an SSH connection requires both a client and a server component, you need to make sure they are installed on the local and the remote machine, respectively. An open source SSH tool—widely used for Linux distributions— is OpenSSH. Installing OpenSSH is relatively easy. It requires access to the terminal on the server and the computer that you use for connecting. Note that Ubuntu does not have SSH server installed by default.

How to Install an OpenSSH Client

Before you proceed with installing an SSH client, make sure it is not already installed. Many Linux distributions already have an SSH client. For Windows machines, you can install PuTTY or any other client of your choice to gain access to a server.

To check if the client is available on your Linux-based system, you will need to:

- Load an SSH terminal. You can either search for "terminal" or press CTRL + ALT + T on your keyboard.
- Type in ssh and press Enter in the terminal.
- If the client is installed, you will receive a response that looks like this:



```
username@host:~$ ssh

  usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
 [-D [bind_address:]port] [-E log_file] [-e escape_char]
 [-F configfile] [-I pkcs11] [-i identity_file]
 [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o
 option] [-p port] [-Q query_option] [-R address] [-S ctl_path] [-W host:port] [-w
 local_tun[:remote_tun]]
  [user@]hostname [command]

username@host:~$
```

This means that you are ready to remotely connect to a physical or virtual machine. Otherwise, you will have to install the OpenSSH client:

- Run the following command to install the OpenSSH client on your computer: sudo apt-get install openssh-client
- Type in your superuser password when asked.
- Hit Enter to complete the installation.

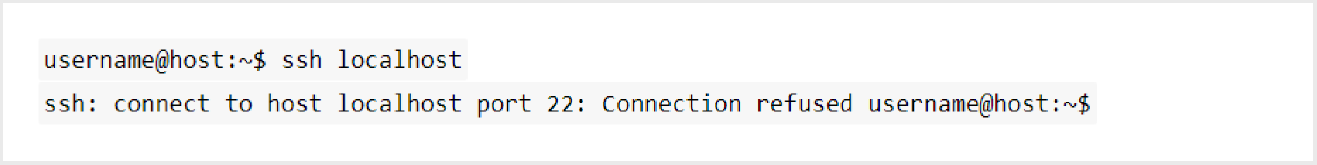
You are now able to SSH into any machine with the server-side application on it, provided that you have the necessary privileges to gain access, as well as the hostname or IP address.

How to Install an OpenSSH Server

In order to accept SSH connections, a machine needs to have the server-side part of the SSH software toolkit.

If you first want to check if OpenSSH server is available on the Ubuntu system of the remote computer that needs to accept SSH connections, you can try to connect to the local host:

- Open the terminal on the server machine. You can either search for “terminal” or press **CTRL + ALT + T** on your keyboard.
- Type in ***ssh localhost*** and hit enter.
- For the systems **without** the SSH server installed the response will look similar to this:



```
username@host:~$ ssh localhost
ssh: connect to host localhost port 22: Connection refused username@host:~$
```

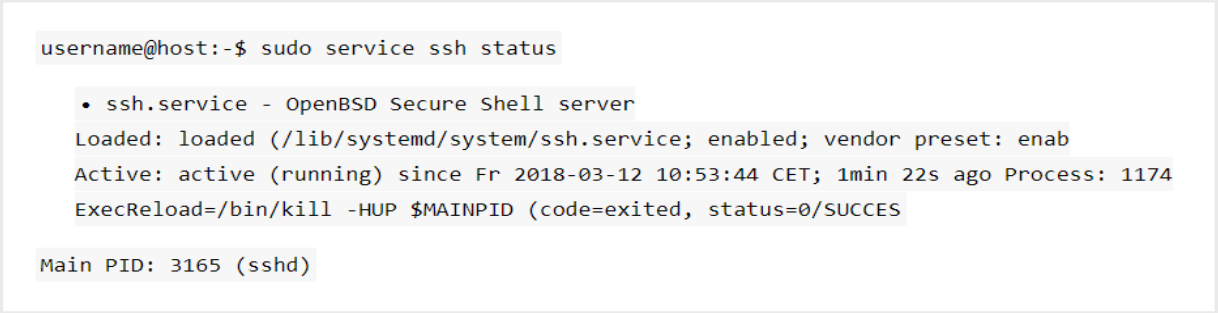
If the above is the case, you will need to install the OpenSSH server. Leave the terminal open and:

- Run the following command to install the SSH server: sudo apt-get install openssh-server ii.
- Type in your superuser password when asked.
- Enter Y to allow the installation to continue after the disk space prompt.

The required support files will be installed, and then you can check if the SSH server is running on the machine by typing this command:

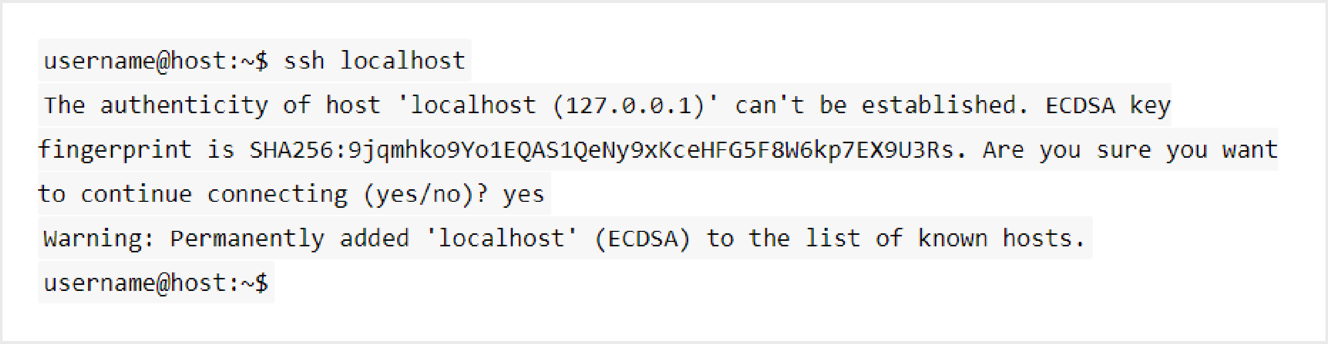
sudo service ssh status

The response in the terminal should look similar to this if the SSH service is now running properly:



```
username@host:-$ sudo service ssh status

   • ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Fr 2018-03-12 10:53:44 CET; 1min 22s ago Process: 1174
   ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCES

Main PID: 3165 (sshd)
```

Another way to test if the OpenSSH server is installed properly and will accept connections is to try running the ssh localhost command again in your terminal prompt. The response will look similar to this screen when you run the command for the first time:



```
username@host:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established. ECDSA key
fingerprint is SHA256:9jqmhko9Yo1EQAS1QeNy9xKceHFG5F8W6kp7EX9U3Rs. Are you sure you want
to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
username@host:~$
```

Enter **yes** or **y** to continue.

Congratulations! You have set up your server to accept SSH connection requests from a different computer using an SSH client.

TIP

You can now edit the SSH daemon configuration file, for example, you can change the default port for SSH connections. In the terminal prompt, run this command:
sudo nano /etc/ssh/sshd_config and the configuration file will open in the editor of your choice. In this case, we used nano.
If you need to install nano, run this command: sudo apt-get install nano
Please note that you need to restart SSH service every time you make any changes to the sshd_config file by running this command: sudo service ssh restart

IX. How to Connect via SSH

Now that you have the OpenSSH client and server installed on every machine you need, you can establish a secure remote connection with your servers. To do so:

- Open the SSH terminal on your machine and run the following command: ssh your_username@host_ip_address If the username on your local machine matches the one on the server you are trying to connect to, you can just type ssh host_ip_address and hit enter.
- Type in your password and hit Enter. Note that you will not get any feedback on the screen while typing. If you are pasting your password, make sure it is stored safely and not in a text file.
- When you are connecting to a server for the very first time, it will ask you if you want to continue connecting. Just type yes and hit Enter. This message appears only this time since the remote server is not identified on your local machine.
- An ECDSA key fingerprint is now added and you are connected to the remote server.

If the computer you are trying to remotely connect to is on the same network, then it is best to use the private IP address instead of the public IP address. Otherwise, you will have to use the public IP address only. Additionally, make sure that you know the correct TCP port OpenSSH is listening to for connection requests and that the port forwarding settings are correct. The default port is 22 if nobody changed configuration in the sshd_config file. You may also just append the port number after the host IP address.

Here is the example of a connection request using the OpenSSH client. We will specify the port number as well:

```
username@machine:~$ ssh phoenixnap@185.52.53.222 -p7654 phoenixnap@185.52.53.222’s
password:
The authenticity of host '185.52.53.222 (185.52.53.222)' can't be established. ECDSA key
fingerprint is SHA256:9lyrpzo5Yo1EQAS2QeHy9xKceHFH8F8W6kp7EX2O3Ps. Are you sure you want
to continue connecting (yes/no)? yes
Warning: Permanently added ' 185.52.53.222' (ECDSA) to the list of known hosts.
username@host:~$
```

You are now able to manage and control a remote machine using your terminal. If you have trouble connecting to a remote server, make sure that:

- The IP address of the remote machine is correct.
- The port SSH daemon is listening to is not blocked by a firewall or forwarded incorrectly.
- Your username and password are correct.
- The SSH software is installed properly.

SSH Further Steps

Now that you are able to establish a connection to your server using SSH, we highly recommend a few further steps to improve SSH security. When you leave the setup with the default values, it is more likely to be hacked and your server can easily become a target of scripted attacks.

Some of the suggestions for hardening SSH by editing the sshd configuration file include:

Change the default TCP port where SSH daemon is listening. Change it from 22 to something much higher, for example 24596. Make sure you do not use a port number that is easy to guess, such as 222, 2222 or 22222.

Use SSH key pairs for authentication. They are both safer and also allow logging in without the need to use your password (which is faster and more convenient).

Disable password-based logins on your server. If your password gets cracked, this will eliminate the possibility of using it to log into your servers. Before you disable the option to log in using passwords, it is important to make sure that authentication using key pairs is working properly.

Disable root access to your server and use a regular account with the su - command to switch to a root user.

You can also use TCP wrappers to restrict access to certain IP addresses or hostnames. Configure which host can connect using TCP wrappers by editing
the /etc/hosts.allow and etc/hosts.deny files.
Note that allowed hosts supersede the denied hosts. For example, to allow SSH access to a single host you will first deny all hosts by adding these two lines in the etc/hosts.deny:

```
sshd : ALL
ALL : ALL
```

Then, in the etc/hosts.allow add a line with the allowed hosts for the SSH service. That can be a single IP address, an IP range, or a hostname: sshd : 10.10.0.5, LOCAL.

Make sure to keep your log in information secure at all times and to apply security at multiple layers. Use different methods to limit SSH access to your servers, or use services that will block anyone who tries to use brute force to gain access to your servers. Fail2ban is one example of such service.

- **Diagrams / Experimental set-up /Work Situation**

- **Resources Required**

Sr.No	**Name of Resource**	**Specification**	**Quantity**	**Remarks/Use**
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Switch (min. 8 ports)	8 ports		
3.				

- **Procedure**

How Does SSH Work?

In order to establish an SSH connection, you need two components: a client and the corresponding server-side component. An SSH client is an application you install on the computer which you will use to connect to another computer or a server. The client uses the provided remote host information to initiate the connection and if the credentials are verified, establishes the encrypted connection.On the server's side, there is a component called an SSH daemon that is constantly listening to a specific TCP/IP port for possible client connection requests. Once a client initiates a connection, the SSH daemon will respond with the software and the protocol versions it supports and the two will exchange their identification data. If the provided credentials are correct, SSH creates a new session for the appropriate environment.

The default SSH protocol version for SSH server and SSH client communication is version 2.

How to Enable an SSH Connection

Since creating an SSH connection requires both a client and a server component, you need to make sure they are installed on the local and the remote machine, respectively. An open source SSH tool—widely used for Linux distributions— is OpenSSH. Installing OpenSSH is relatively easy. It requires access to the terminal on the server and the computer that you use for connecting. Note that Ubuntu does not have SSH server installed by default.

How to Install an OpenSSH Client

Before you proceed with installing an SSH client, make sure it is not already installed. Many Linux distributions already have an SSH client. For Windows machines, you can install PuTTY or any other client of your choice to gain access to a server.

To check if the client is available on your Linux-based system, you will need to:

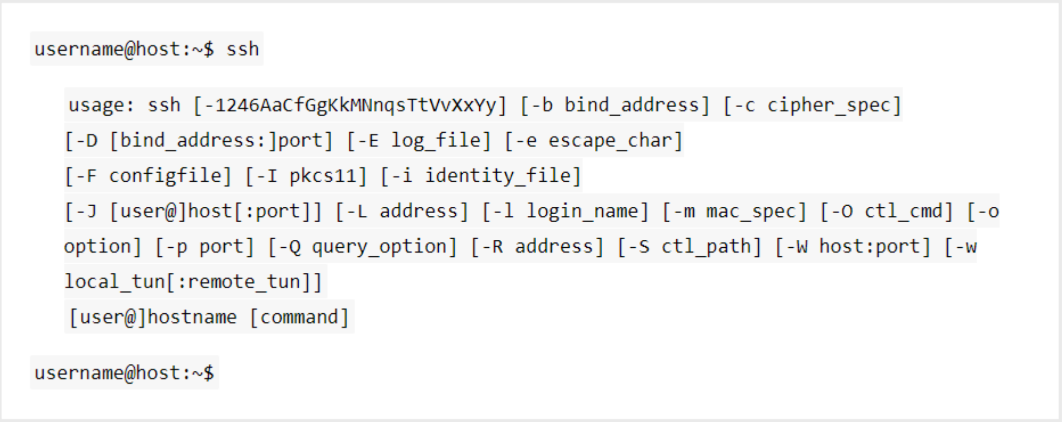
- Load an SSH terminal. You can either search for “terminal” or press CTRL + ALT + T on your keyboard.
- Type in ssh and press Enter in the terminal.
- If the client is installed, you will receive a response that looks like this:

This means that you are ready to remotely connect to a physical or virtual machine. Otherwise, you will have to install the OpenSSH client:

- Run the following command to install the OpenSSH client on your computer: sudo apt-get install openssh-client
- Type in your superuser password when asked.
- Hit Enter to complete the installation.

You are now able to SSH into any machine with the server-side application on it, provided that you have the necessary privileges to gain access, as well as the hostname or IP address.

-



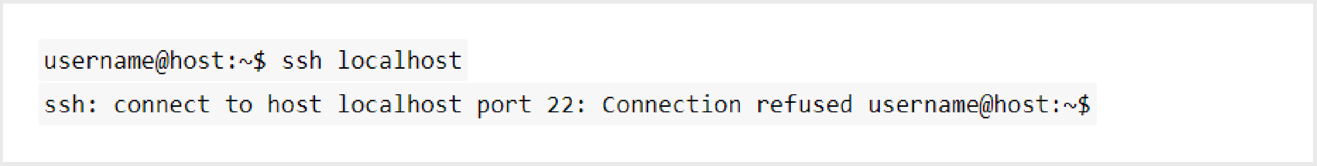
```
username@host:~$ ssh

  usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
 [-D [bind_address:]port] [-E log_file] [-e escape_char]
 [-F configfile] [-I pkcs11] [-i identity_file]
 [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o
 option] [-p port] [-Q query_option] [-R address] [-S ctl_path] [-W host:port] [-w
 local_tun[:remote_tun]]
  [user@]hostname [command]

username@host:~$
```

How to Install an OpenSSH Server

In order to accept SSH connections, a machine needs to have the server-side part of the SSH software toolkit.

If you first want to check if OpenSSH server is available on the Ubuntu system of the remote computer that needs to accept SSH connections, you can try to connect to the local host:

- Open the terminal on the server machine. You can either search for “terminal” or press **CTRL + ALT + T** on your keyboard.
- Type in ***ssh localhost*** and hit enter.
- For the systems **without** the SSH server installed the response will look similar to this:

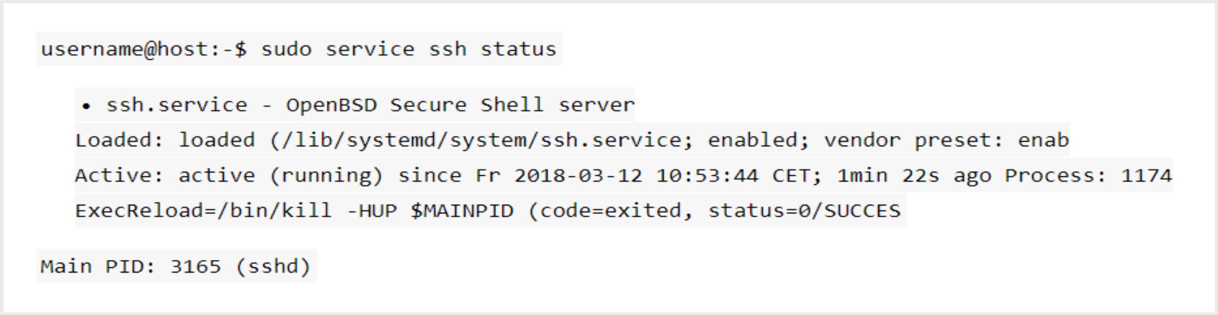


```
username@host:~$ ssh localhost
ssh: connect to host localhost port 22: Connection refused username@host:~$
```

If the above is the case, you will need to install the OpenSSH server. Leave the terminal open and:

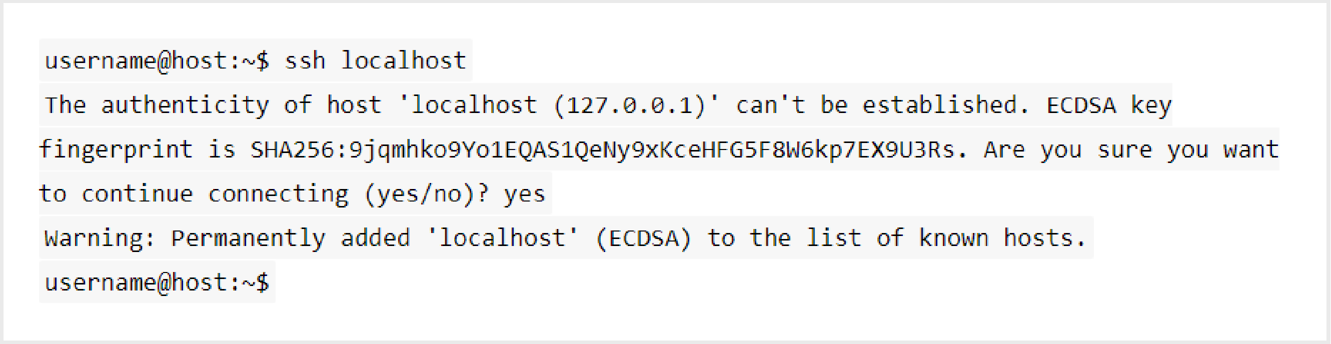
- Run the following command to install the SSH server: sudo apt-get install openssh-server ii.
- Type in your superuser password when asked.
- Enter Y to allow the installation to continue after the disk space prompt.

The required support files will be installed, and then you can check if the SSH server is running on the machine by typing this command:
sudo service ssh status
The response in the terminal should look similar to this if the SSH service is now running properly:



```
username@host:-$ sudo service ssh status

   • ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Fr 2018-03-12 10:53:44 CET; 1min 22s ago Process: 1174
   ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCES

Main PID: 3165 (sshd)
```

Another way to test if the OpenSSH server is installed properly and will accept connections is to try running the ssh localhost command again in your terminal prompt. The response will look similar to this screen when you run the command for the first time:



```
username@host:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established. ECDSA key
fingerprint is SHA256:9jqmhko9Yo1EQAS1QeNy9xKceHFG5F8W6kp7EX9U3Rs. Are you sure you want
to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
username@host:~$
```

Enter **yes** or **y** to continue.

Congratulations! You have set up your server to accept SSH connection requests from a different computer using an SSH client.

You can now edit the SSH daemon configuration file, for example, you can change the default port for SSH connections. In the terminal prompt, run this command:
sudo nano /etc/ssh/sshd_config and the configuration file will open in the editor of your choice. In this case, we used nano.
If you need to install nano, run this command: sudo apt-get install nano
Please note that you need to restart SSH service every time you make any changes to the sshd_config file by running this command: sudo service ssh restart

IX. How to Connect via SSH

Now that you have the OpenSSH client and server installed on every machine you need, you can establish a secure remote connection with your servers. To do so:

- Open the SSH terminal on your machine and run the following command: ssh your_username@host_ip_address If the username on your local machine matches the one on the server you are trying to connect to, you can just type ssh host_ip_address and hit enter.
- Type in your password and hit Enter. Note that you will not get any feedback on the screen while typing. If you are pasting your password, make sure it is stored safely and not in a text file.
- When you are connecting to a server for the very first time, it will ask you if you want to continue connecting. Just type yes and hit Enter. This message appears only this time since the remote server is not identified on your local machine.
- An ECDSA key fingerprint is now added and you are connected to the remote server.

If the computer you are trying to remotely connect to is on the same network, then it is best to use the private IP address instead of the public IP address. Otherwise, you will have to use the public IP address only. Additionally, make sure that you know the correct TCP port OpenSSH is listening to for connection requests and that the port forwarding settings are correct. The default port is 22 if nobody changed configuration in the sshd_config file. You may also just append the port number after the host IP address.

Here is the example of a connection request using the OpenSSH client. We will specify the port number as well:

```
username@machine:~$ ssh phoenixnap@185.52.53.222 –p7654 phoenixnap@185.52.53.222’s
password:
The authenticity of host '185.52.53.222 (185.52.53.222)' can't be established. ECDSA key
fingerprint is SHA256:9lyrpzo5Yo1EQAS2QeHy9xKceHFH8F8W6kp7EX2O3Ps. Are you sure you want
to continue connecting (yes/no)? yes
Warning: Permanently added ' 185.52.53.222' (ECDSA) to the list of known hosts.
username@host:~$
```

You are now able to manage and control a remote machine using your terminal. If you have trouble connecting to a remote server, make sure that:

- The IP address of the remote machine is correct.
- The port SSH daemon is listening to is not blocked by a firewall or forwarded incorrectly.
- Your username and password are correct.
- The SSH software is installed properly.

SSH Further Steps

Now that you are able to establish a connection to your server using SSH, we highly recommend a few further steps to improve SSH security. When you leave the setup with the default values, it is more likely to be hacked and your server can easily become a target of scripted attacks.

Some of the suggestions for hardening SSH by editing the sshd configuration file include:

Change the default TCP port where SSH daemon is listening. Change it from 22 to something much higher, for example 24596. Make sure you do not use a port number that is easy to guess, such as 222, 2222 or 22222.

Use SSH key pairs for authentication. They are both safer and also allow logging in without the need to use your password (which is faster and more convenient).

Disable password-based logins on your server. If your password gets cracked, this will eliminate the possibility of using it to log into your servers. Before you disable the option to log in using passwords, it is important to make sure that authentication using key pairs is working properly.

Disable root access to your server and use a regular account with the su - command to switch to a root user.

You can also use TCP wrappers to restrict access to certain IP addresses or hostnames. Configure which host can connect using TCP wrappers by editing
the /etc/hosts.allow and etc/hosts.deny files.
Note that allowed hosts supersede the denied hosts. For example, to allow SSH access to a single host you will first deny all hosts by adding these two lines in the etc/hosts.deny:

```
sshd : ALL
ALL : ALL
```

Then, in the etc/hosts.allow add a line with the allowed hosts for the SSH service. That can be a single IP address, an IP range, or a hostname: sshd : 10.10.0.5, LOCAL.

Make sure to keep your log in information secure at all times and to apply security at multiple layers. Use different methods to limit SSH access to your servers, or use services that will block anyone who tries to use brute force to gain access to your servers. Fail2ban is one example of such service.

- **Precaution**
  - Handle Computer System and peripherals with care
  - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Crossover Cable	
2.	Network Interface Card	Manufacturer: Cisco
3.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
4.	Switch (min. 8 ports)	8 ports
5.	Any other Resource	

- **Result/Conclusion**

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

………………

- **Practical Related Questions**
  - What is SSH Protocol?
  - What Is The Default Port & Configuration File Of Ssh Server?
  - What Is The Difference Between Ssh & Telnet?
  - How To Check Ssh Server's Version?
  - How To Allow Only Specific Users To Ssh Your Linux Server?
- **Exercise**
  - Configure SSH protocol.

(Space for Answer)

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

………

………

…………………………………

………

………

………

………

………

………

………

………

………

………

………

………

………

………

………

………………………………………………………………………………………

………

………

………

………………

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**

Total(50 Marks)	**100%**

- **List of Students/Team Members**

  ………………………………………………..

  ………………………………………………..

  …………………………………………..........

  ………………………………………………..

Marks Obtained			**Dated Signature of Teacher**
Process Related(35)	**Product Related (15)**	**Total(50)**	

Practical No.12: Configure SMTP, POP3 and IMAP using relevant software

- **Practical Significance**

  Student should be able to study servers like SMTP, POP and IMAP.

- **Relevant Programs Outcomes (POs)**

- **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- **Communication:** Communicate effectively in oral and written form.

- **Competency and Practical skills**
  - Ability to configure SMTP, POP3 and IMAP servers.
- **Relevant Course Outcomes**

  Implement Application Layer Protocols
- **Practical Outcomes (POs)**

  Understand configuration of SMTP, POP3 and IMAP servers.
- **Relevant Affective domain related Outcomes**
  - Follow safety practices
  - Follow ethical practices
- **Minimum Theoretical Background**

  Proposition 1.

POP: Post Office Protocol

A communications “protocol” is just the language computers use to talk between themselves. POP is the language used between a computer fetching email (usually your computer, running an email program) and the computer holding your email (usually that of your email service provider or ISP).

A “POP client” is a program fetching email. Thunderbird and Microsoft Office’s Outlook desktop program are two examples. A “POP server” is the server holding your email. POP allows the user to pick up the message and download it into his own inbox: it’s the incoming server. The “3” indicates that we’re all using version three of the POP protocol.

IMAP: Internet Message Access Protocol

IMAP is another protocol used by email programs to access your email.

IMAP is an alternative to POP3, and works in a fundamentally different way. Those differences make it a frequently-preferred alternative in today's always-connected world.

SMTP: Simple Mail Transfer Protocol

SMTP is the protocol used to send mail from one computer to another.

When you're using a desktop email program like Thunderbird, it's the protocol used when you hit "Send" to transfer your email message from your computer to that of your email provider. What most people don't realize is that it's also the protocol used behind the scenes to transfer your message from server to server as it makes its way to the server on which your recipient receives email.

Configuring an SMTP server generally requires the same three things you needed for POP3 or IMAP:

- The name of your email provider's server which will accept your outgoing email. It could be the same as your POP3 or IMAP server, or something different.
- The account ID you were assigned by your ISP. Most commonly it's your email address, but it doesn't have to be.
- Your password.

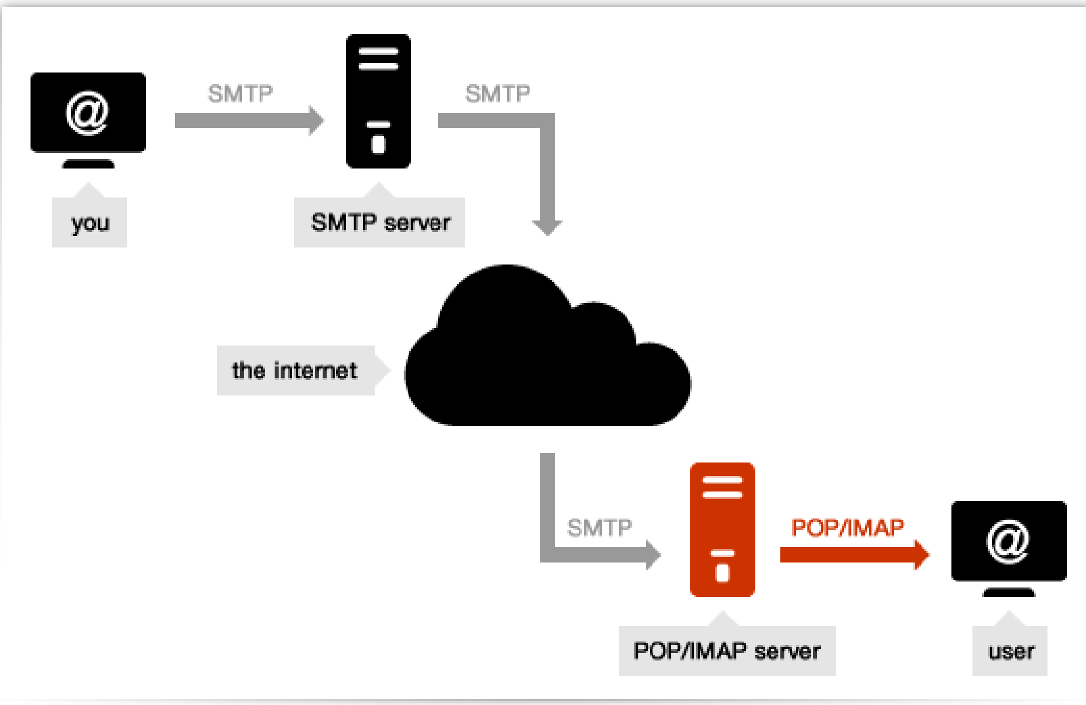
The normal journey of an email is more or less like the journey of a paper mail through different post offices: you send a message using a client (Apple Mail, Mozilla Thunderbird, etc.), it connects with a server via SMTP protocol and delivers the email: finally, the recipient's client uses POP3 or IMAP to retrieve it.
Below you find a list of the SMTP and POP/POP3 names for the most common email providers.

If you need to send a bulk email or an email campaign you should opt for a professional server like turboSMTP. Matter of fact, while "normal" SMTPs are based on widely shared IPs (affecting in a negative way your delivery rate), a dedicated outgoing service will rely only on controlled ones. Ensuring that all your messages reach their destination.

PROVIDER	URL	SMTP	POP / POP3
1&1	1and1.com	Smtp.1and1.com	Pop.1and1.com
Airmail	Airmail.net	Mail.airmail.net	Pop3.airmail.net
AOL	Aol.com	Smtp.aol.com	Pop.aol.com
AT&T	Att.net	Outbound.att.net	Inbound.att.net
Bluewin	Bluewin.ch	Smtpauths.bluewin.ch	Pop3.bluewin.ch
BT Connect	Btconnect.com	Mail.btconnect.tom	Pop3.btconnect.com
Comcast	Comcast.net	Smtp.comcast.net	Mail.comcast.net
Earthlink	Earthlink.net	Smtpauth.earthlink.net	Pop.earthlink.net
Gmail	Gmail.com	Smtp.gmail.com	Pop.gmail.com
Gmx	Gmx.net	Mail.gmx.net	Pop.gmx.net
HotPop	Hotpop.com	Mail.hotpop.com	Pop.hotpop.com
Libero	Libero.it	Mail.libero.it	Popmail.libero.it
Lycos	Lycos.com	Smtp.lycos.com	Pop.lycos.com
O2	o2.com	Smtp.o2.com	Mail.o2.com
Orange	Orange.net	Smtp.orange.net	Pop.orange.net
Outlook.com (former Hotmail)	Outlook.com	Smtp.live.com	Pop3.live.com
Tin	Tin.it	Mail.tin.it	Pop.tin.it / Box.tin.it
Tiscali	Tiscali.co.uk	Smtp.tiscali.co.uk	Pop.tiscali.co.uk
Verizon	Verizon.net	Outgoing.verizon.net	Incoming.verizon.net
Virgin	Virgin.net	Smtp.virgin.net	Pop.virgin.net
Wanadoo	Wanadoo.fr	Smtp.wanadoo.fr	Pop.wanadoo.fr

Yahoo	Yahoo.com	Mail.yahoo.com	Pop.yahoo.com

- **Diagrams / Experimental set-up /Work Situation**



- **Resources Required**

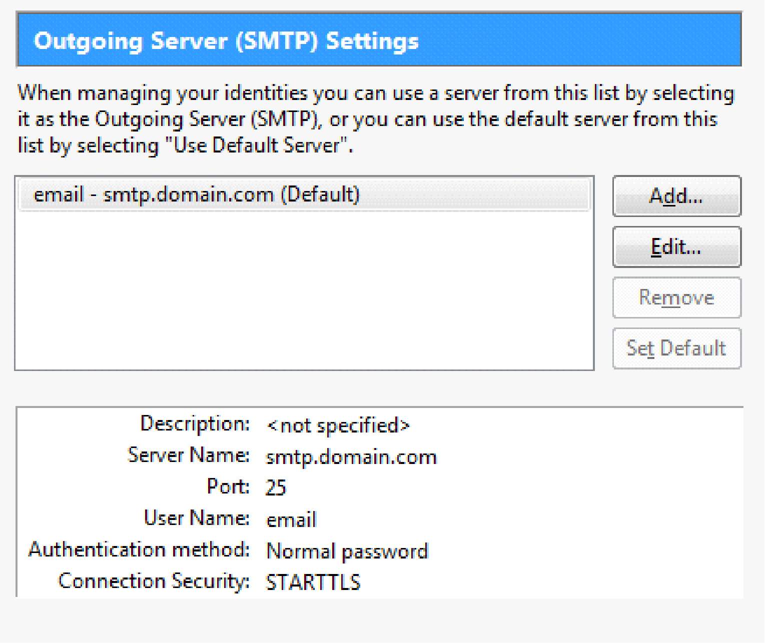
Sr.No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		
4.	Crossover Cable			

- **Procedure**

The standard procedure of SMTP configuration, in four steps:

1. Select the voice “Account Settings” in your mail client, generally in the “Tools” menu.

2. Choose the “Outgoing server (SMTP)” voice:



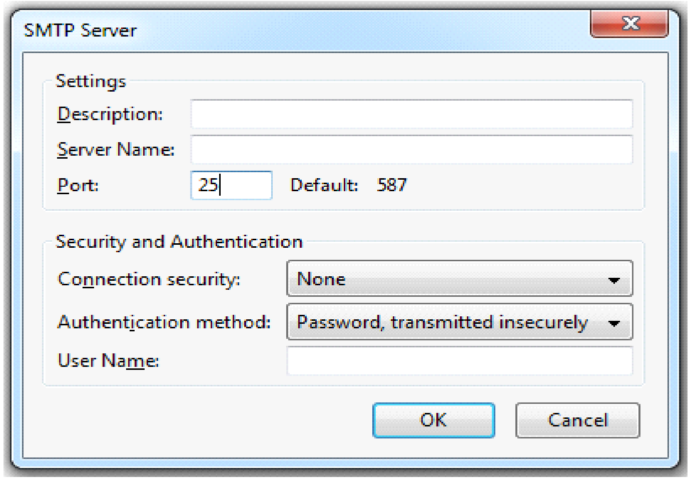
Outgoing Server (SMTP) Settings

When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".

email - smtp.domain.com (Default)

Description: <not specified>
Server Name: smtp.domain.com
Port: 25
User Name: email
Authentication method: Normal password
Connection Security: STARTTLS

3. Push the "Add…" button in order to set a new SMTP. A popup window will appear:



SMTP Server

Settings
Description:
Server Name:
Port: 25 Default: 587

Security and Authentication
Connection security: None
Authentication method: Password, transmitted insecurely
User Name:

- Now simply fill the voices as follows:
- **Description**: an informal name that you will decide to identify the server (best to use the email provider's, like Gmail or Yahoo).
- **Server Name**: the actual SMTP server's specification. You can find it either consulting the web page of your provider, or searching for it on our list of server POP and SMTP.
- **Port**: usually SMTP works with port 25, but as the screenshot shows it can work also with 587. For further information, check out our article about SMTP ports.

- **Connection security**: in itself, SMTP email transfer doesn't provide an encryption. So if you want to make your connection more secure, it's a good choice to use a STARTTLS or SSL/TLS extension, that employ a separate port for encrypted communication.
- **Authentication method**: there's a certain number of methods (passwords, CRAM-MD5, KERBEROS etc.).
- **User Name:** your email address.
- **Precaution**
    - Handle Computer System and peripherals with care
    - Follow Safety Practices
- **Resources Used**

Sr.No	Name of Resource	Specification
1.	Crossover Cable	
2.	Network Interface Card	Manufacturer: Cisco
3.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
4.	Switch (min. 8 ports)	8 ports
5.	Any other Resource	

- **Result/Conclusion**

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

………………

- **Practical Related Questions**
    - 1 .What is difference between IMAP and POP3?
    - 2. What is IMAP?
    - 3. Explain POP3 protocol.
    - 4. Explain SMTP in detail.
- **Exercise**
    - **Configure IMAP,POP3 and SMTP**

(Space for Answer)

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………

- **Assessment Scheme**

Performance indicator		**Weightage**
Process Related(35 Marks)		**75%**
1.	**Completion of given task**	**25%**
2.	**Correctness of given task**	**50%**
Product Related(15 Marks)		**25%**
3.	**Answer to sample Question**	**15%**
4.	**Submit Report in Time**	**10%**
Total(50 Marks)		**100%**

- **List of Students/Team Members**

…………………………………………………..

…………………………………………………..

……………………………………………..........

…………………………………………………..

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	