Computer Networking
BCA V SEM

The Application Layer

Kailash Karki
Kailash.karki@deerwalk.edu.np

Unit 6: The Application Layer 5 Hrs.

6.1 Functions of Application layer

6.2 Application Layer Protocols: DNS, DHCP, WWW, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP

6.3 Concept of traffic analyzer: MRTG, PRTG, SNMP, Packet tracer, Wireshark.

Application Layer

- The application layer provides services to the user. Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages.
- The application layer acts as interface between the applications and the underlying network.

Functions:

- **Mail Services:** This application provides various e-mail services.
- **File transfer & Access:** It allows users to access files in a remote host, to retrieve files from remote computer for use etc.
- **Remote log-in:** A user can log into a remote computer and access the resources of that computer.
- **Accessing the World Wide Web:** Most common application today is the access of the World Wide Web.

Application Layer Protocols:

1. Domain Name System (DNS):

- The domain name system (DNS) is a naming database in which internet domain names are located and translated into internet protocol (IP) addresses.

- Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 110.44.120.45 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

- Although it's possible to enter an IP address into a web browser into order to get to a website, it's a lot easier to enter its domain name instead. However, computers, servers and other devices are unable to make heads or tails of domain names they strictly rely on binary identifiers. The DNS's job, then, is to take domain names and translate them into the IP addresses that allow machines to communicate with one another. Every domain name has at least one IP address associated with it.

- DNS Port No: 53

Country Domain:

- Country domain uses two character country abbreviations.
- For example**,** for Nepal the country domain is “np”, India is .in, UK is .uk etc.

Generic Domain:

•It defines the registered hosts according to their generic behavior. It uses three-character labels, and these labels describe the organization type.

•For Example, .com for commercial organizations, .edu for educational institutions, .gov for government organizations, .org for non profit organization.

Inverse Domain:

Inverse domain is used to map an address to a name.

•**For example,** a client send a request to the server for performing a particular task, server finds a list of authorized client. The list contains only IP addresses of the client.

•The server sends a query to the DNS server to map an address to a name to determine if the client is on the authorized list

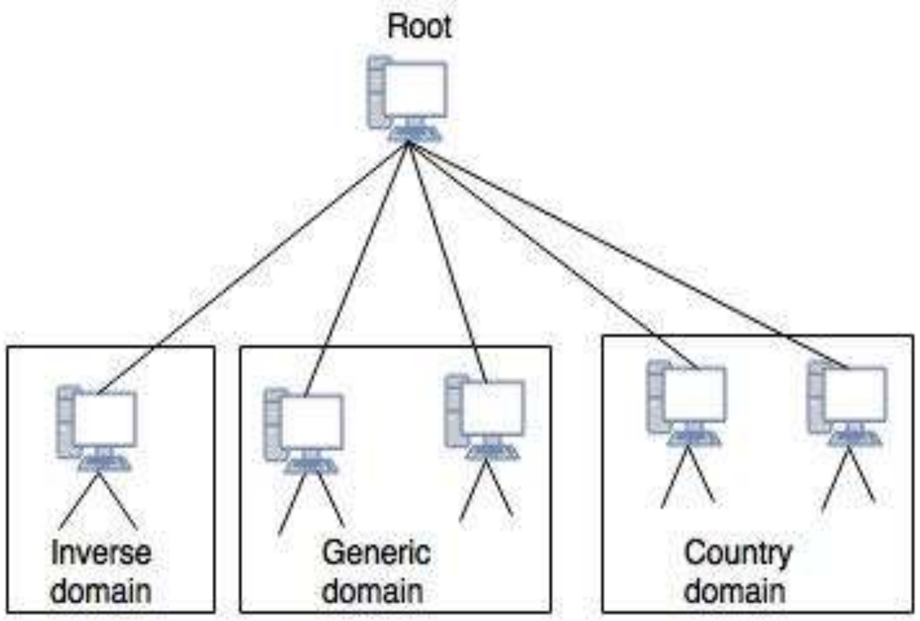
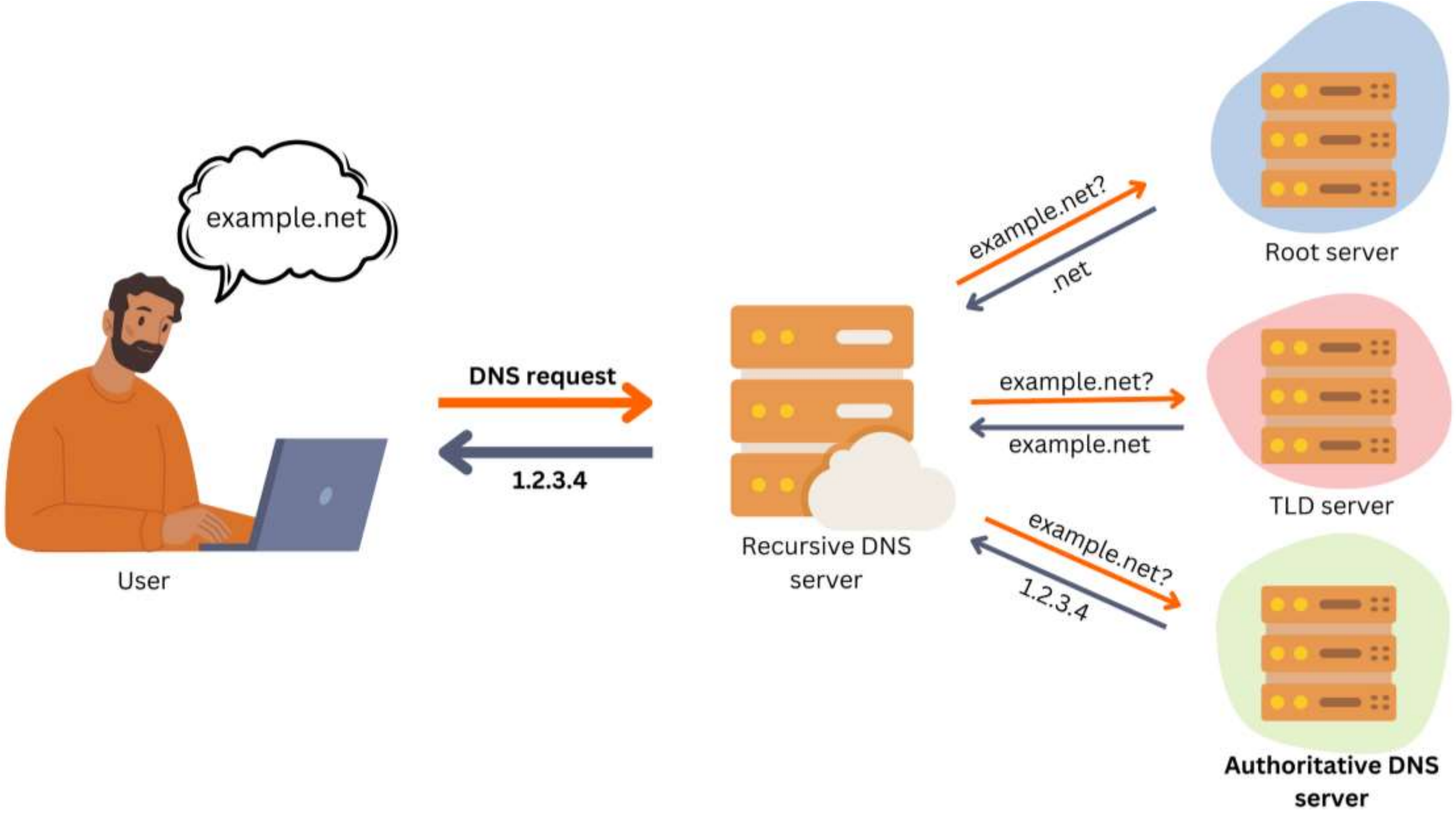


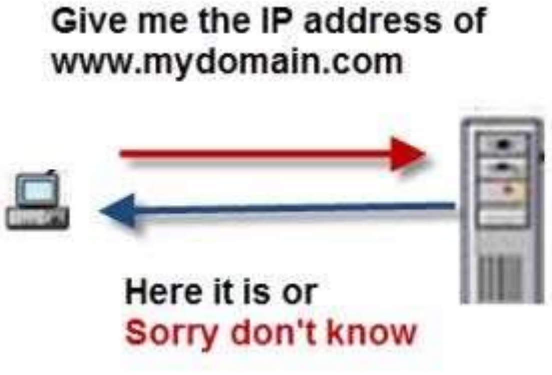
Fig. : DNS in the Internet

The basic process of a DNS resolution follows these steps:

1. The user enters a web address or domain name into a browser.
2. The browser sends a message, called a recursive DNS query, to the network to find out which IP or network address the domain corresponds to.
3. The query goes to a recursive DNS server, which is also called a recursive resolver, and is usually managed by the internet service provider (ISP). If the recursive resolver has the address, it will return the address to the user, and the webpage will load.
4. If the recursive DNS server does not have an answer, it will query a series of other servers in the following order: DNS root name servers, top-level domain (TLD) name servers and authoritative name servers.
5. The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address. It sends this information to the recursive DNS server, and the webpage the user is looking for loads. DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.
6. The recursive server stores, or caches, the A record for the domain name, which contains the IP address. The next time it receives a request for that domain name, it can respond directly to the user instead of querying other servers.
7. If the query reaches the authoritative server and it cannot find the information, it returns an error message.

DNS Resolution Process:

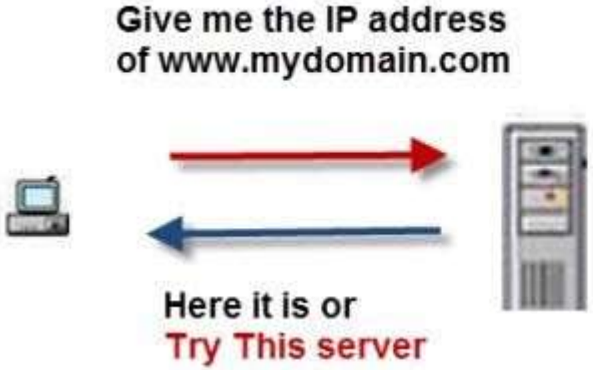




Give me the IP address of www.mydomain.com

Here it is or
Sorry don't know

Recursive Query



Give me the IP address of www.mydomain.com

Here it is or
Try This server

Non Recursive Query

2. Dynamic Host Configuration Protocol (DHCP)

- It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts.
- DHCP automates and centrally manages the assignment of IP address easing the work of network administrator. In addition to the IP address, the DHCP also assigns the subnet masks, default gateway and domain name server(DNS) address and other configuration to the host and by doing so, it makes the task of network administrator easier.

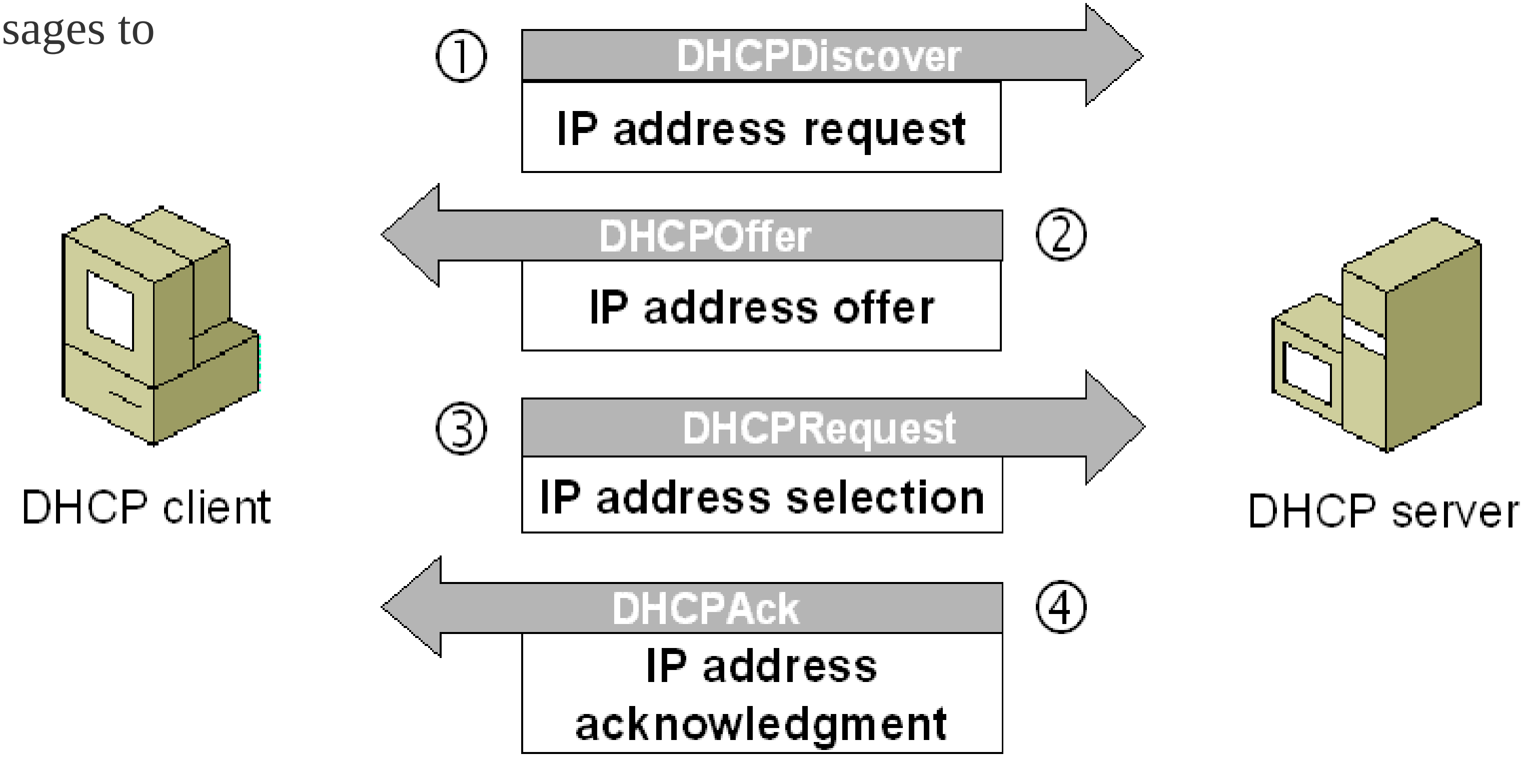
How do DHCP works?

DHCP Discover: The DHCP client broadcast messages to discover the DHCP servers.

DHCP Offer: When the DHCP server receives the DHCP Discover message then it suggests or offers an IP address(form IP address pool) to the client by sending a DHCP offer message to the client.

DHCP Request: In response to the offer, the client sends a DHCP Request requesting the offered address from one of the DHCP servers.

DHCP Acknowledgment: The server then sends Acknowledgment to the client confirming the DHCP lease to the client.



3. Hypertext Transfer Protocol (HTTP):

- HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files -- such as text, images, sound, video and other multimedia files -- over the web. HTTP is the foundation of data communication for the World Wide Web.
- The latest version of HTTP is HTTP/3, which was published in 2022. It is an alternative to its predecessor, HTTP 1.1 and HTTP/2
- HTTP is a client and server-side standard for request and response (TCP). The client is the end user, the server is the website. Typically, a request is made by the HTTP client to establish a TCP connection to the server's designated port (the default is port 80). The HTTP server listens on that port for requests sent by the client. Upon receipt of the request, the server sends a status line (to the client), such as "HTTP / 1.1 200 OK," and (response) a message body that may be a requested file, an error message, or some other information.
- A web browser is an HTTP client that sends requests to servers. When the browser user enters file requests by either "opening" a web file by typing in a URL or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in the destination server receives the request and sends back the requested file or files associated with the request.

4. Hypertext transfer protocol secure (HTTPS):

- Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.
- HTTPS is the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user HTTP page requests as well as the pages that are returned by the web server.
- Port No: 443

Refer:

HTTP: https://www.youtube.com/watch?v=a-sBfyiXysI

HTTPS: https://www.youtube.com/watch?v=j9QmMEWmcfo&t=11s

Each HTTP request contains encoded data, with information such as:

- **The specific version of HTTP followed:** HTTP/1,HTTP/1.1,HTTP/2 and HTTP/3 are the versions of HTTP.
- **A URL:** This points to the resource on the web.
- **An HTTP method**. This indicates the specific action the request expects to receive from the server in its response. The two most common HTTP methods are: GET and POST. GET is used to request data from a specified resource. POST is used to send data to a server to create/update a resource.
- **HTTP request headers:** This includes data such as what type of browser is being used and what data the request is seeking from the server. It can also include cookies, which show information previously sent from the server handling the request.
- **An HTTP body:** This is optional information the server needs from the request, such as user forms -- username/password logins, short responses and file uploads -- that are being submitted to the website.

HTTP responses typically include the following data:

- **HTTP status code**, which indicates the status of the request to the client device. Responses may indicate success, an informational response, a redirect, or errors on the server or client side.
- **HTTP response headers**, which send information about the server and requested resources.
- **An HTTP body (optional).** If a request is successful, this contains the requested data in the form of HTML code, which is translated into a web page by the client browser.

HTTP Status Codes

Level 200 (Success)

200 : OK

201 : Created

203 : Non-Authoritative Information

204 : No Content

Level 400

400 : Bad Request

401 : Unauthorized

403 : Forbidden

404 : Not Found

409 : Conflict

Level 500

500 : Internal Server Error

503 : Service Unavailable

501 : Not Implemented

504 : Gateway Timeout

599 : Network timeout

502 : Bad Gateway

5. FTP (File Transfer Protocol):

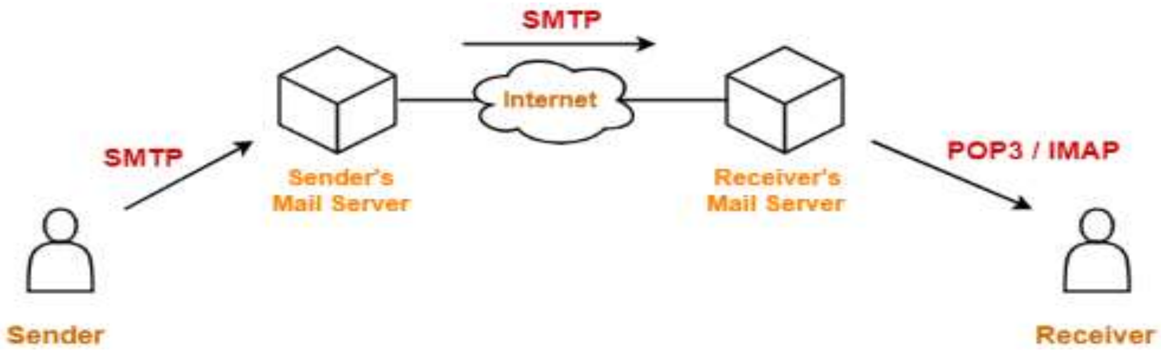
- The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.
- FTP services generally run on both ports 20 and 21.
- Port 20 is used to transmit data flow between the client and server, while port 21 is used to transmit control flow .
- Some FTP Client Software for windows: FileZilla, WinScp, CoreFTP etc.

6. TELNET:

- Telnet stands for the TELetype NETwork. It is a type of protocol that enables one computer to connect to local computer.
- It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

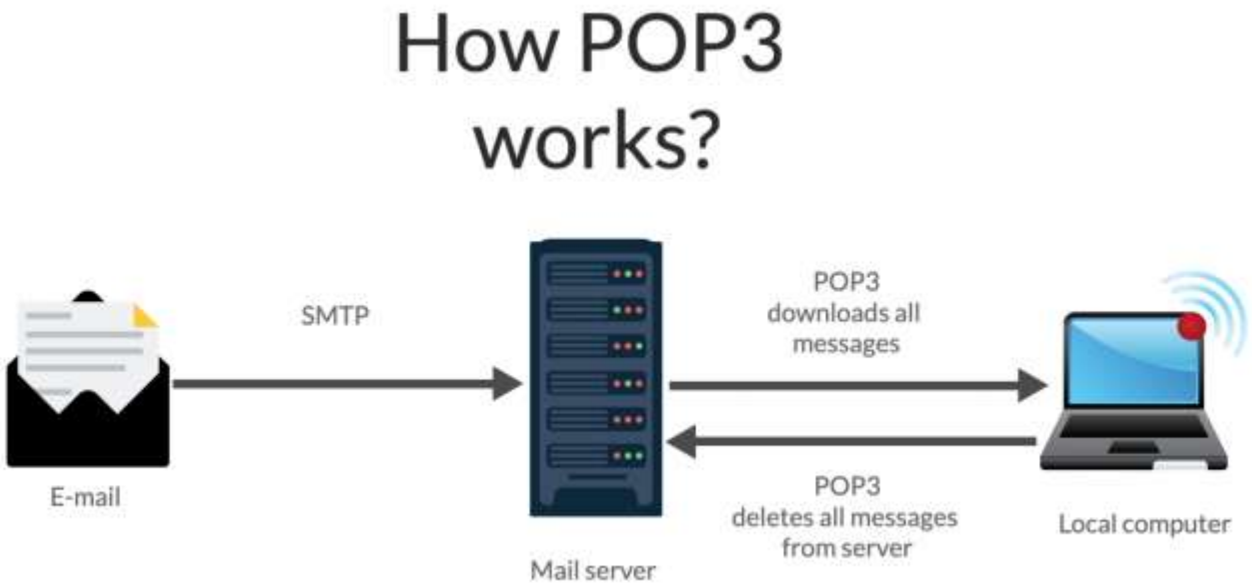
7. Simple Mail Transfer Protocol (SMTP) :

- SMTP stands for Simple Mail Transfer Protocol, and it is responsible for sending email messages. This protocol is used by email clients and mail servers to exchange emails between computers.
- It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.
- SMTP spells out and directs how your email moves from your computer’s MTA to an MTA on another computer, and even several computers. Using that “store and forward” feature mentioned before, the message can move in steps from your computer to its destination. At each step, Simple Mail Transfer Protocol is doing its job.



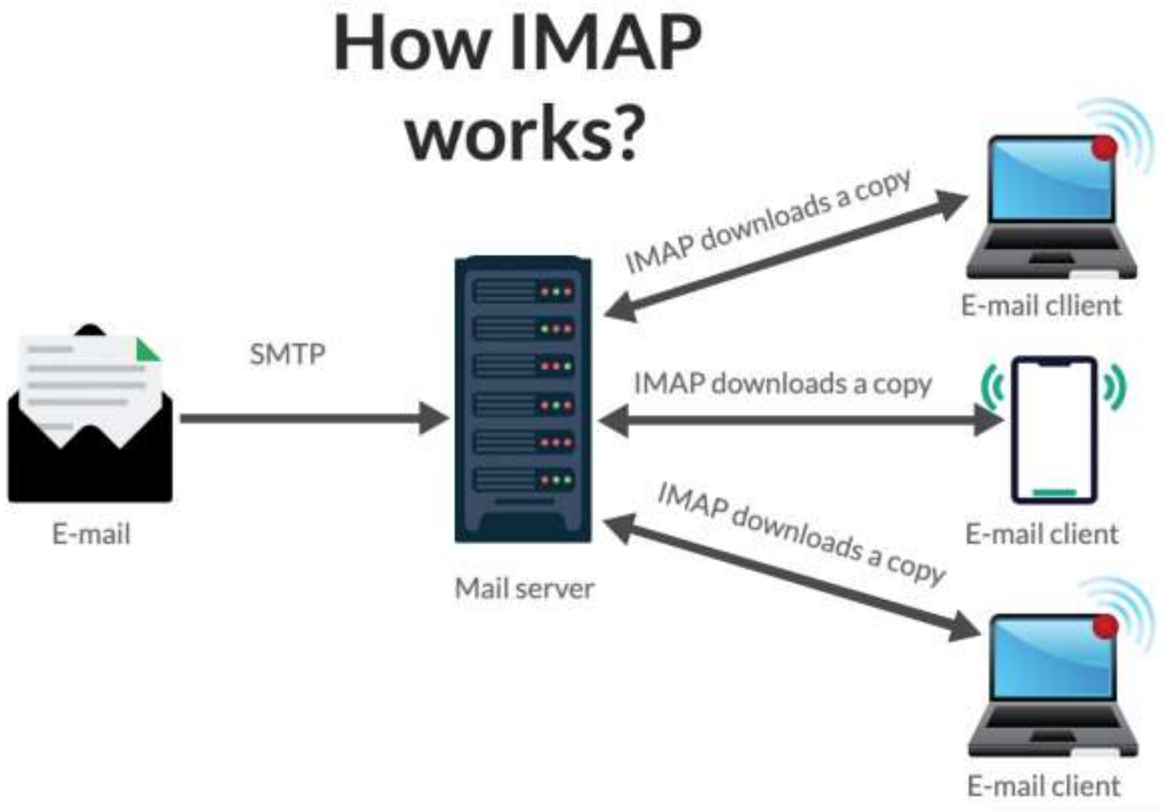
8. Post Office Protocol (POP3):

- The POP3 abbreviation stands for Post Office Protocol version 3, which provides access to an inbox stored in an email server. It executes the download and delete operations for messages. Thus, when a POP3 client connects to the mail server, it retrieves all messages from the mailbox. Then it stores them on your local computer and deletes them from the remote server.


How POP3 works?
E-mail
SMTP
Mail server
POP3 downloads all messages
POP3 deletes all messages from server
Local computer

9. Internet Message Access Protocol (IMAP):

- The Internet Message Access Protocol (IMAP) allows you to access and manage your email messages on the email server. This protocol permits you to manipulate folders, permanently delete and efficiently search through messages. It also gives you the option to set or remove email flags, or fetch email attributes selectively. By default, all messages remain on the server until the user specifically deletes them.

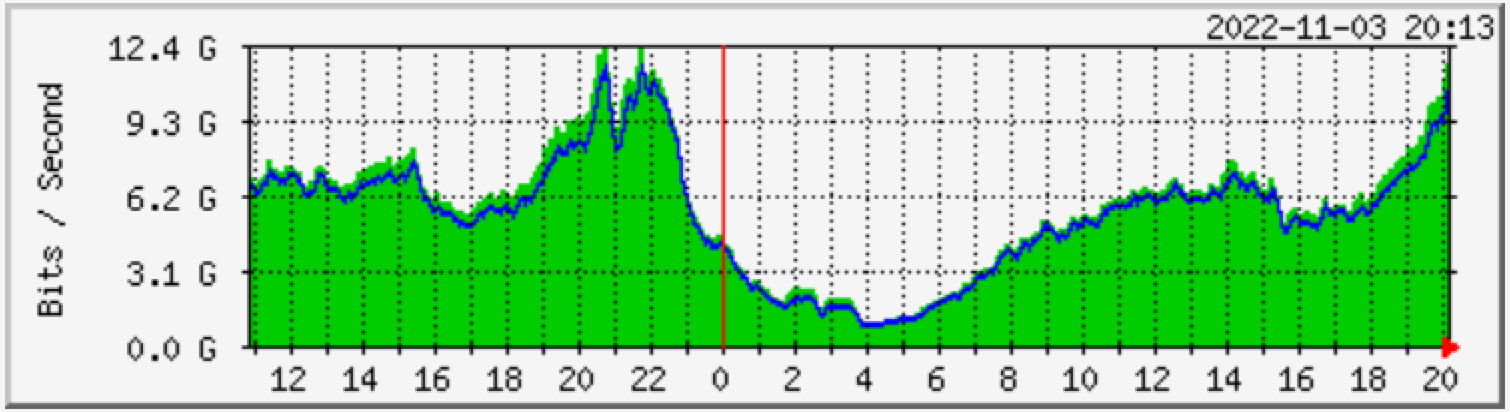


Concept of Traffic Analyzer

MRTG:

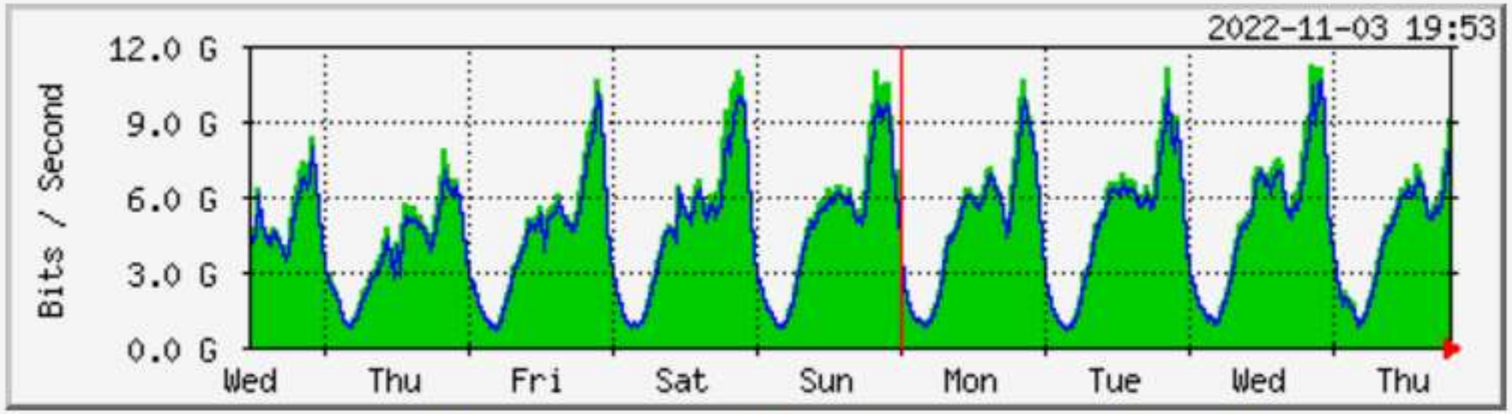
- You have a router, you want to know what it does all day long? Then MRTG is for you. It will monitor SNMP network devices and draw pretty pictures showing how much traffic has passed through each interface.
- Routers are only the beginning. MRTG is being used to graph all sorts of network devices as well as everything else from weather data to vending machines.
- MRTG, which stands for *Multi Router Traffic Grapher* is a software tool that helps your monitor and traffic on your network ports and links.
- MRTG generates HTML pages containing PNG images which provide an almost live visual representation of this traffic.
- It supports SNMP to collecting data to visually graph points and charts within the interface via their routines and algorithms.

Day Graph



	Max	Average	Current
In	12.987 Gbits	5.753 Gbits	12.783 Gbits
Out	11.980 Gbits	5.334 Gbits	11.803 Gbits

Week Graph



	Max	Average	Current
In	12.987 Gbits	4.891 Gbits	12.783 Gbits
Out	11.980 Gbits	4.523 Gbits	11.803 Gbits

PRTG (Paessler Router Traffic Graphic):

- PRTG is a unified monitoring tool that can monitor almost any object that has an IP address. It consists of the PRTG core server and one or more probes:
- The PRTG core server is responsible for configuration, data management, PRTG web server, and more.
- Probes collect data and monitor processes on devices via sensors.
- Sensors are the building blocks of PRTG. A sensor can tell you about one or more aspects of a device:

✓ Uptime

✓ Load

✓ Bandwidth usage

✓ Loading times

✓ Hardware status

✓ Temperature

✓ Quality

✓ Resource consumption

✓ User counts

✓ Log events

✓ Database requests

Simple Network Management Protocol (SNMP):

- SNMP stands for Simple Network Management Protocol. It is a framework used for managing devices on the internet. It provides a set of operations for monitoring and managing the internet.

- SNMP components
  There are 3 components of SNMP:

1. SNMP Manager
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. SNMP agent
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. Management Information Base
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

Packet Tracer:

- Packet Tracer is a simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.
- Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.
- The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts.
- Major Features:

✓Visualizing Networks

✓Real-time and simulation mode

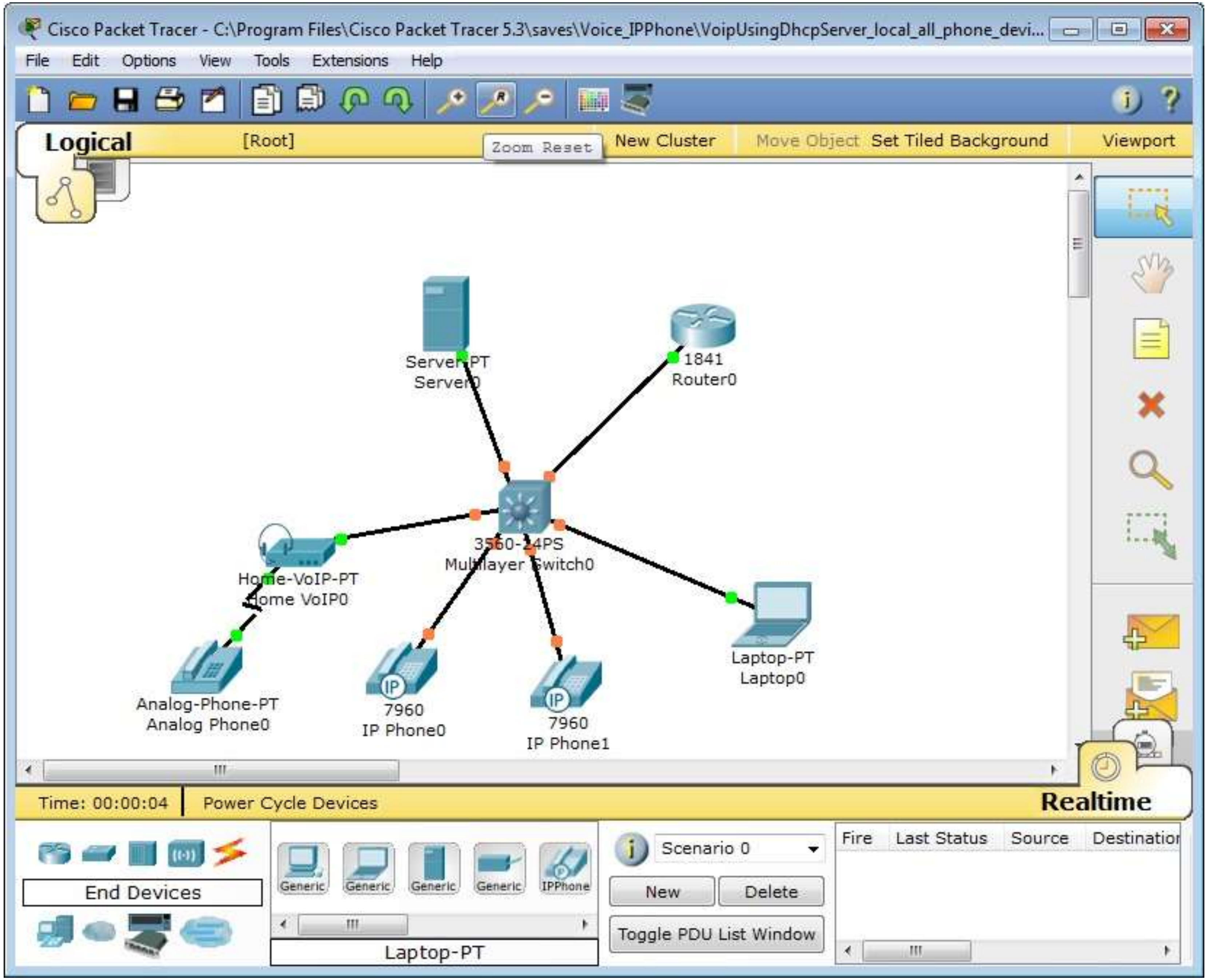
✓Compatible on various platforms

✓Support to all languages

✓Most networking protocols are supported

✓Environment is interactive

✓Can be used on unlimited devices


Cisco Packet Tracer - C:\Program Files\Cisco Packet Tracer 5.3\saves\Voice_IPPhone\VoipUsingDhcpServer_local_all_phone_devi...
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
Zoom Reset
New Cluster
Move Object
Set Tiled Background
Viewport
Server-PT
Server0
1841
Router0
3560-24PS
Multilayer Switch0
Home-VoIP-PT
Home VoIP0
Analog-Phone-PT
Analog Phone0
7960
IP Phone0
7960
IP Phone1
Laptop-PT
Laptop0
Time: 00:00:04
Power Cycle Devices
Realtime
End Devices
Generic
Generic
Generic
Generic
IPPhone
Laptop-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

Wireshark:

- Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical network.
- Wireshark does three things:

1. Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

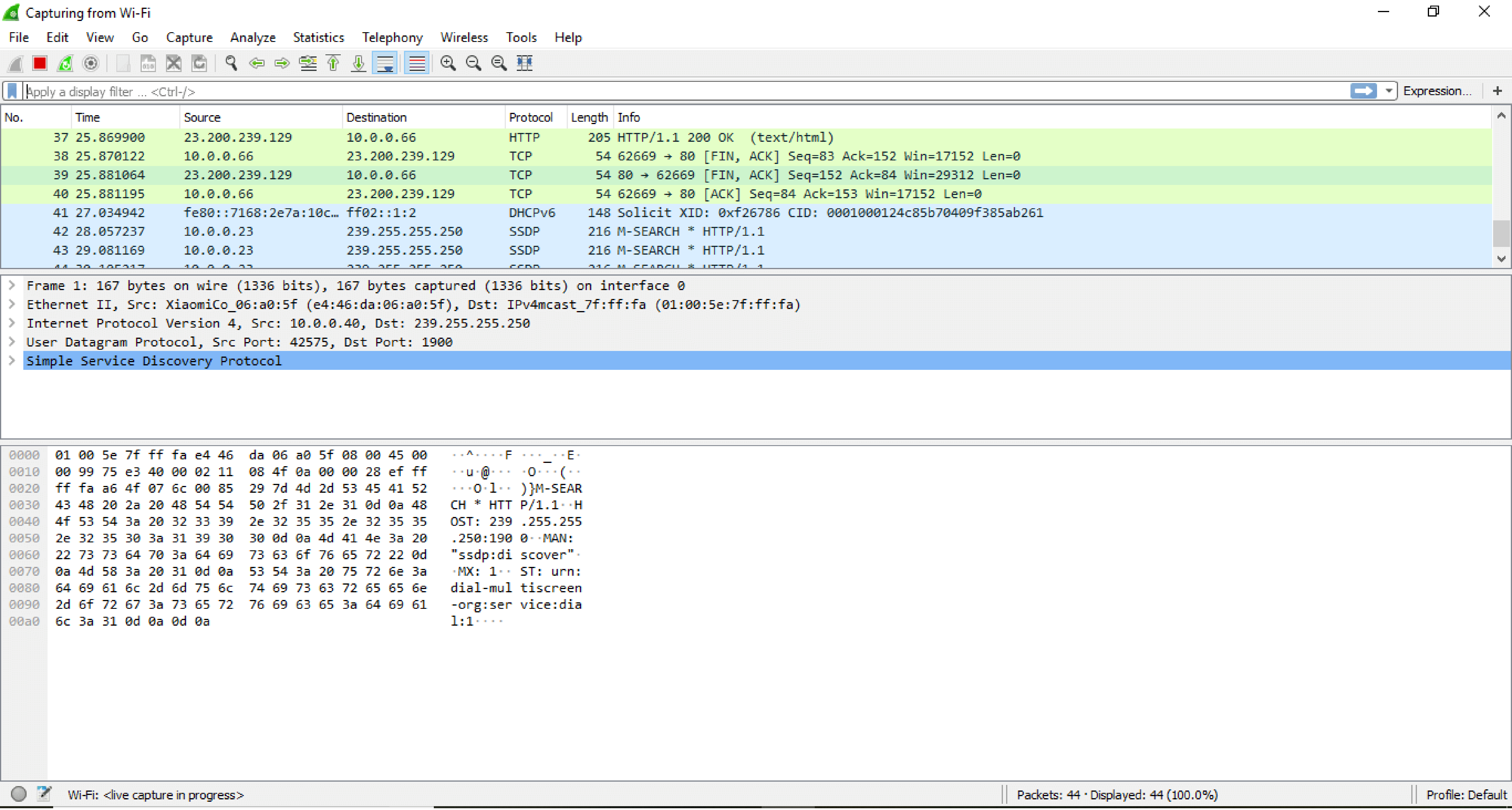
2. Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

3. Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

- Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

Uses of Wireshark:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.



```
No.   Time       Source              Destination      Protocol Length Info
   37 25.869900  23.200.239.129      10.0.0.66        HTTP      205 HTTP/1.1 200 OK  (text/html)
   38 25.870122  10.0.0.66           23.200.239.129   TCP        54 62669 → 80 [FIN, ACK] Seq=83 Ack=152 Win=17152 Len=0
   39 25.881064  23.200.239.129      10.0.0.66        TCP        54 80 → 62669 [FIN, ACK] Seq=152 Ack=84 Win=29312 Len=0
   40 25.881195  10.0.0.66           23.200.239.129   TCP        54 62669 → 80 [ACK] Seq=84 Ack=153 Win=17152 Len=0
   41 27.034942  fe80::7168:2e7a:10c… ff02::1:2       DHCPv6    148 Solicit XID: 0xf26786 CID: 0001000124c85b70409f385ab261
   42 28.057237  10.0.0.23           239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
   43 29.081169  10.0.0.23           239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 0
> Ethernet II, Src: XiaomiCo_06:a0:5f (e4:46:da:06:a0:5f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.0.0.40, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 42575, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa e4 46  da 06 a0 5f 08 00 45 00   ··^····F ···_··E·
0010  00 99 75 e3 40 00 02 11  08 4f 0a 00 00 28 ef ff   ··u·@··· ·O···(··
0020  ff fa a6 4f 07 6c 00 85  29 7d 4d 2d 53 45 41 52   ···O·l·· )}M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 0d 0a                               l:1····
```

Wi-Fi: <live capture in progress>   Packets: 44 · Displayed: 44 (100.0%)   Profile: Default