Chapter-6
Application Layer

Introduction

- Application layer is the Layer 4(topmost layer) of the TCP/IP reference model, in which network-aware, user-controlled software is implemented—for example, e-mail, file transfer utilities, and terminal access.
- Some of protocols that run at the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), DNS, SMTP, POP, telnet, and similar protocols that can be implemented as utilities the user can interface with.

Principle of application layer protocol

- An application layer protocol defines how an application's processes, running on different end systems, pass messages to each other.
- In particular, an application layer protocol defines:
  i. The types of message exchanged. Example: request message and response message.
  ii. The syntax of the various message types. i.e. the field in the message and how the fields are represented.
  iii. The semantics of the fields. i.e. the meaning of the information in the fields.
  iv. Rules for determining when and how a process/application sends message and response to a message.
- Example: The application layer protocol of email application define how message are passed between servers, how the content of certain part of mail message (header) are to be interpreted etc.

1. World Wide Web and HTTP (Hypertext transfer protocol)

- The Hypertext Transfer Protocol (HTTP), the Web's application-layer protocol which is implemented in both client program (web browser) and server program (web server).
- The client program and server programs, executing on different end systems, talk to each other by exchanging HTTP messages.
- HTTP defines how Web clients (i.e., browsers) request Web pages from servers (i.e., Web servers) and how servers transfer Web pages to clients.
- HTTP defines the structure of these messages and how the client and server exchange the messages.

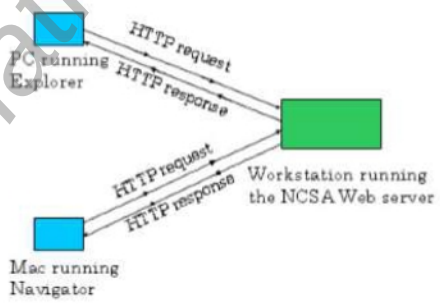


Figure 2.2-1: HTTP request-response behavior

- When a user requests a Web page (e.g., clicks on a hyperlink), the browser sends HTTP request messages for the objects (Jpeg image, audio file) in the page to the server. The server receives the requests and responds with HTTP response messages that contain the objects.
- For this HTTP client first initiate a TCP connection a TCP with the server. Once the connection is established, the browser and the server processes access TCP through their **socket** interfaces.
- The client sends HTTP request messages into its socket interface and receives HTTP response messages from its **socket** interface.
- Similarly, the HTTP server receives request messages from its socket interface and sends response messages into the socket interface.
- HTTP is also called **as stateless protocol** because HTTP server maintain no information about client.
- 80 is the default port for HTTP.

HTTP connection

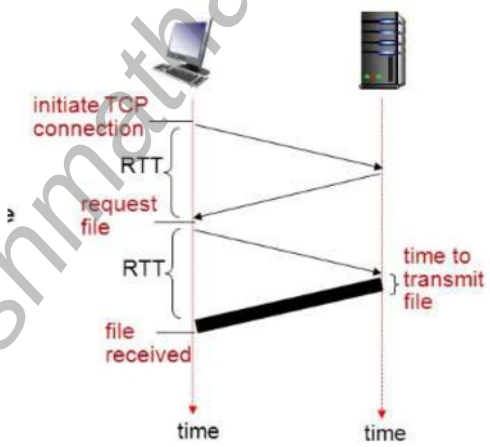
- There are two types of HTTP connection
    1. Persistent connection
    2. Non persistent connection

1. Non persistent connection

- The HTTP connection in which at most one object is sent over a TCP connection is called non persistent HTTP connection.
- Suppose a web page consists of some text and reference to 10 JPEG image. Then the steps of transferring this webpage from server to client using non persistent HTTP connection are
    i. HTTP client initiate TCP connection to HTTP server at port 80.
    ii. HTTP server waits for TCP connection at port 80 and accept it if any connection available.
    iii. HTTP client sends HTTP request message containing URL into TCP connection socket.
    iv. HTTP server receives request message then form response message containing requested object and sends message back to the socket.
    v. HTTP server **close** the connection.
    vi. HTTP client receive response message and get required web page. But while parsing, if finds 10 addition referenced JPEG image and text image.
    vii. So entire above steps are repeated for each of 10 JPEGE image object.
- Since, TCP connection is closed after the server sends each object, the connection does not persist for other object hence called as non-persistent connection.

Drawback

- Non persistent connection has mainly two drawback
    i. Overhead to server for establishing and maintaining connection for each requested object.
    ii. Require two RTT (Round Trip Time: time to move packet from client to server then back to client) per object. First RTT for establishing connection and second RTT for requesting and receiving object.



Response Time= 2 RTT + transmit time

2. Persistent connection

- In case of persistent connection, the server leave connection open after sending response so that subsequent HTTP message between same client and server are sent over same connection.
- So here, a client can send request as soon as it encounters additional referenced object.
- Hence it requires only one RTT for initiating TCP connection for all the referenced object.
- It is further categorized as
    i. Persistent connection with pipelining
        - Here the client can issue a request as soon as it encounters reference.

ii. Persistent connection without pipelining

- Here the client issues a new request only when the previous response has been received.

FTP (File transfer protocol)

- FTP (File Transfer Protocol) is a protocol for transferring a file from one host to another host. Figure 2.3-1: FTP moves files between local and remote file systems.

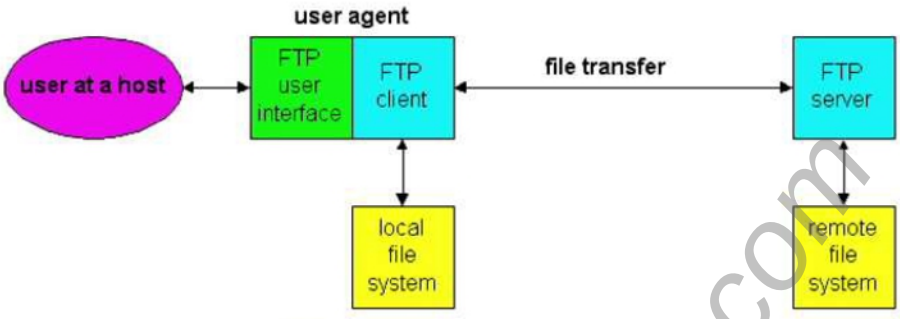


Figure 2.3-1: FTP moves files between local and remote file systems.

- An FTP client is an application that can issue FTP commands to an FTP server, while an FTP server is a service or daemon running on a server that responds to FTP commands from a client.
- For any user to access the remote computer, the user first provides the hostname of the remote host, which causes the FTP client process in the local host to establish a TCP connection with the FTP server process in the remote host. The user then provides the user identification and password, which get sent over the TCP connection as part of FTP commands. Once the server has authorized the user, the user copies one or more files stored in the local file system into the remote file system (or vice versa).

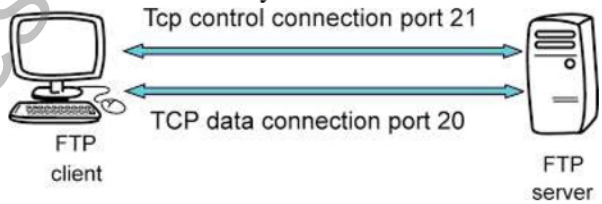
  Some FTP commands
  - **Get "filename"** FTP command is used to get file from server to client.
  - **Put "filename"** FTP command is used to write new file into server from client.
  - **Delete "filename"** FTP command is used to delete a file.

Similarity Between FTP and HTTP

- Both are file transfer protocol
- Both run on top of TCP i.e. transport layer protocol which is connection oriented and reliable data transfer protocol.

Difference between FTP and HTTP

3. HTTP uses a single TCP connection but FTP uses two parallel TCP connection (control connection and data connection) to transfer a file. Control connection is used for sending control information like username, password, command to get and put file etc. The data connection is used to actually send the file.



4. HTTP use 80 as port number but FTP uses 20 and 21 as port number.
5. FTP server maintain state about user but HTTP is stateless i.e. it doesn't have to keep track of users.\

SFTP

- SFTP stands for SSH file transfer protocol.
- IT is a secure file transfer protocol that runs over the SSH (Secure shell protocol).
- It supports the full security and authentication functionality of SSH.
- SFTP has almost replaced FTP as it provides all the functionalities of FTP with more security and reliablility.
- SFTP also protects against password sniffing and man in the middle attack.

- It provides integrity of data using encryption and cryptographic hash functions, and authenticate both server and the user.

DNS

- IP address are tough for human to remember and impossible to guess. Domain Name System are usually used to translate a hostname or Domain name into an IP address.
- The DNS is a way that the internet domain names are translated into internet protocol (IP) address.
- DNS automatically converts the host name(pu.edu.np) we type in our web browser address bar to the IP address 202.2.106.77 of webserver hosting the site.
- DNS is an application layer protocol.

Working principle

- DNS implement a distributed database to store the hostname and address information for all public host on the internet as hierarchy of many named servers.
- When a client like web browser issues a request involving the internet hostname, a piece of software called DNS resolver first contact a DNS server to determine IP address.
- If the server doesn't contain the needed mapping, it will forward the request to next higher level in the hierarchy.
- After several forwarding, the IP address for the given host eventually arrive at the resolver, that in turn complete the request over internet protocol(IP) address.

Note:

Dos Command: nslookup

```
C:\Users\Bheeshma>nslookup google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:803::200e
          216.58.221.46
```

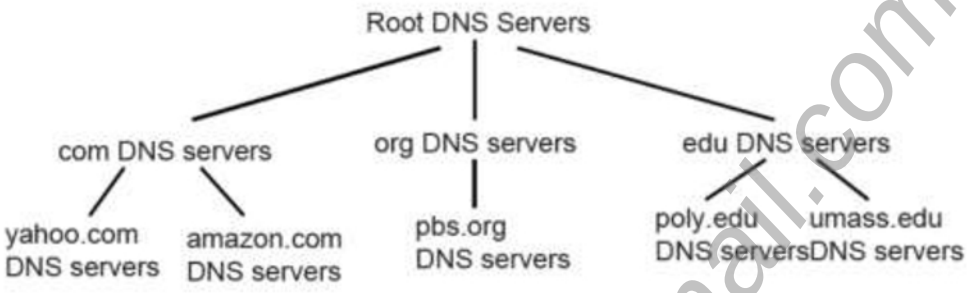
```
C:\Users\Bheeshma>nslookup www.facebook.com
Server:  dsldevice.lan
Address:  192.168.1.254

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f10c:283:face:b00c:0:25de
          157.240.25.35
Aliases:  www.facebook.com
```

Here the first two line indicates the server name and ip address of DNS server which the request was directed.

Services provided by DNS

1. Translation of hostname to IP address
   - People prefer mnemonics than IP address.
   - DNS translates the hostname to IP address.
2. Host aliasing
   - A host with a complicated host name can have one or more alias name.
   - For example, a hostname such as relay1.west-coast.enterprise.com could have, say, two aliases such as enterprise.com and www.enterprise.com.
3. Mail server aliasing
   - It can be used to provides simple mnemonics email address instead of using more complicated email address.
   - Example: canonical host name = relay1.west-coast.hotmail.com
     Alias= bob@hotmail.com.
4. Load distribution
   - DNS is also being used to perform load distribution among replicated servers, such as replicated Web servers.
   - Busy sites, such as cnn.com, are replicated over multiple servers, with each server running on a different end system, and having a different IP address.
   - For replicated Web servers, a set of IP addresses is thus associated with one canonical hostname.
   - The DNS database contains this set of IP addresses.
   - When clients make a DNS query for a name mapped to a set of addresses, the server responds with the entire set of IP addresses, but rotates the ordering of the addresses within each reply.

A distributed Hierarchical database



- DNS implement distributed database to store the host name and the address information for all public host on the internet as a hierarchy of many name servers.
- A single server doesn't provide mapping for all host in the internet.
- There are three classes of DNS server named as
  1. Root DNS server
  2. Top level DNS server
  3. Authoritative DNS server

- **Root DNS server**

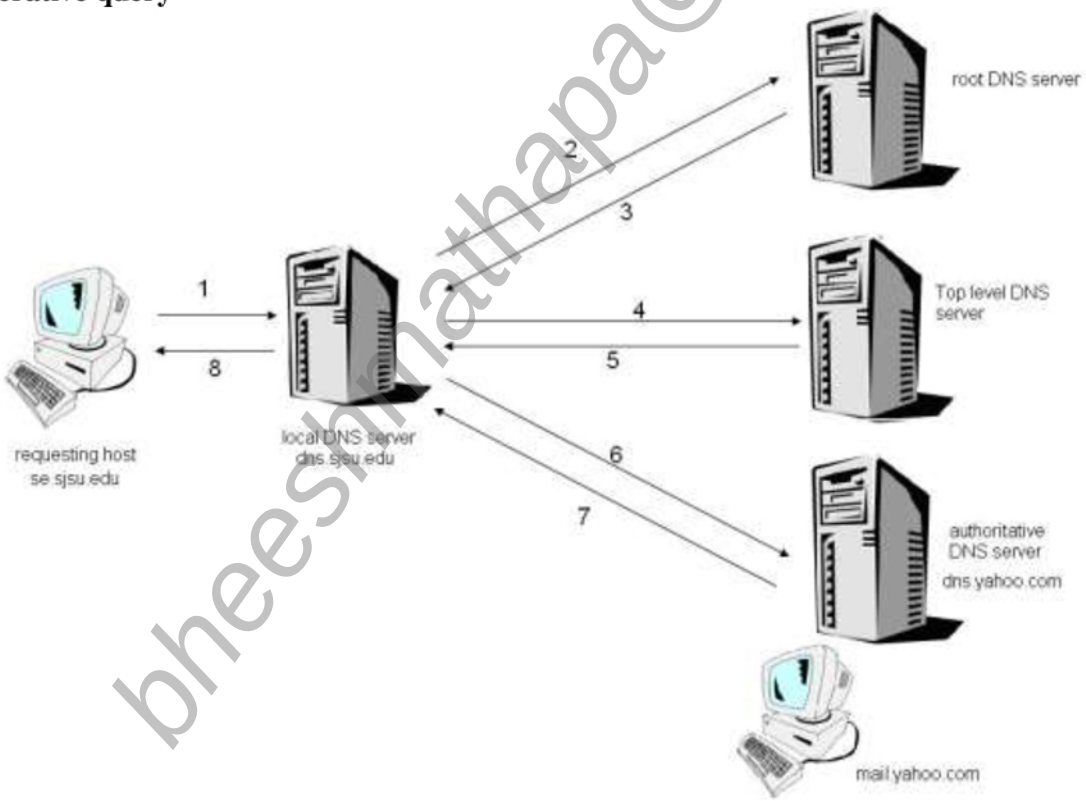
Client wants IP for www.amazon.com; 1st approx:

- client queries a root server to find com DNS server
- client queries com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

- **Top-level domain (TLD) servers:**
  - responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.
  - Network Solutions maintains servers for com TLD
  - Educause for edu TLD
- **Authoritative DNS servers:**
  - organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web, mail).
  - can be maintained by organization or service provider

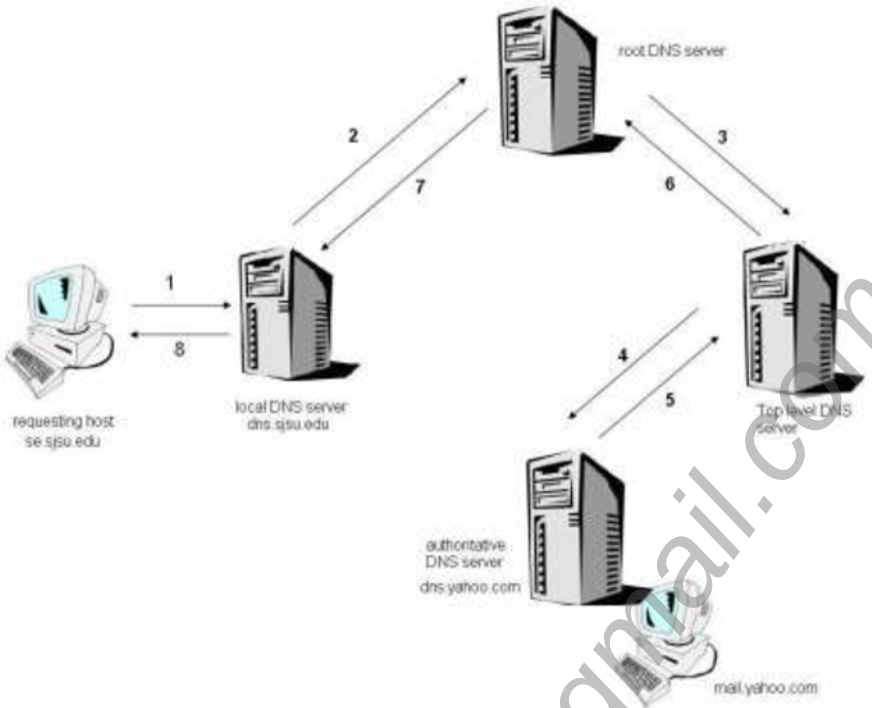
DNS Queries for Name Resolution

i. Iterative query



- Suppose a DNS client want to determine IP address for www.amazon.com
- First client queries one of the root server.
- The root server returns the IP address for TLD server for top level domain .com
- The client then contacts one of these TLD server, which returns the IP address for authoritative server for amazon.com
- Finally, the client contacts one of the authoritative server for amazon.com which returns the ip address for the host name www.amazon.com.

ii. Recursive Query



Explain yourself……..

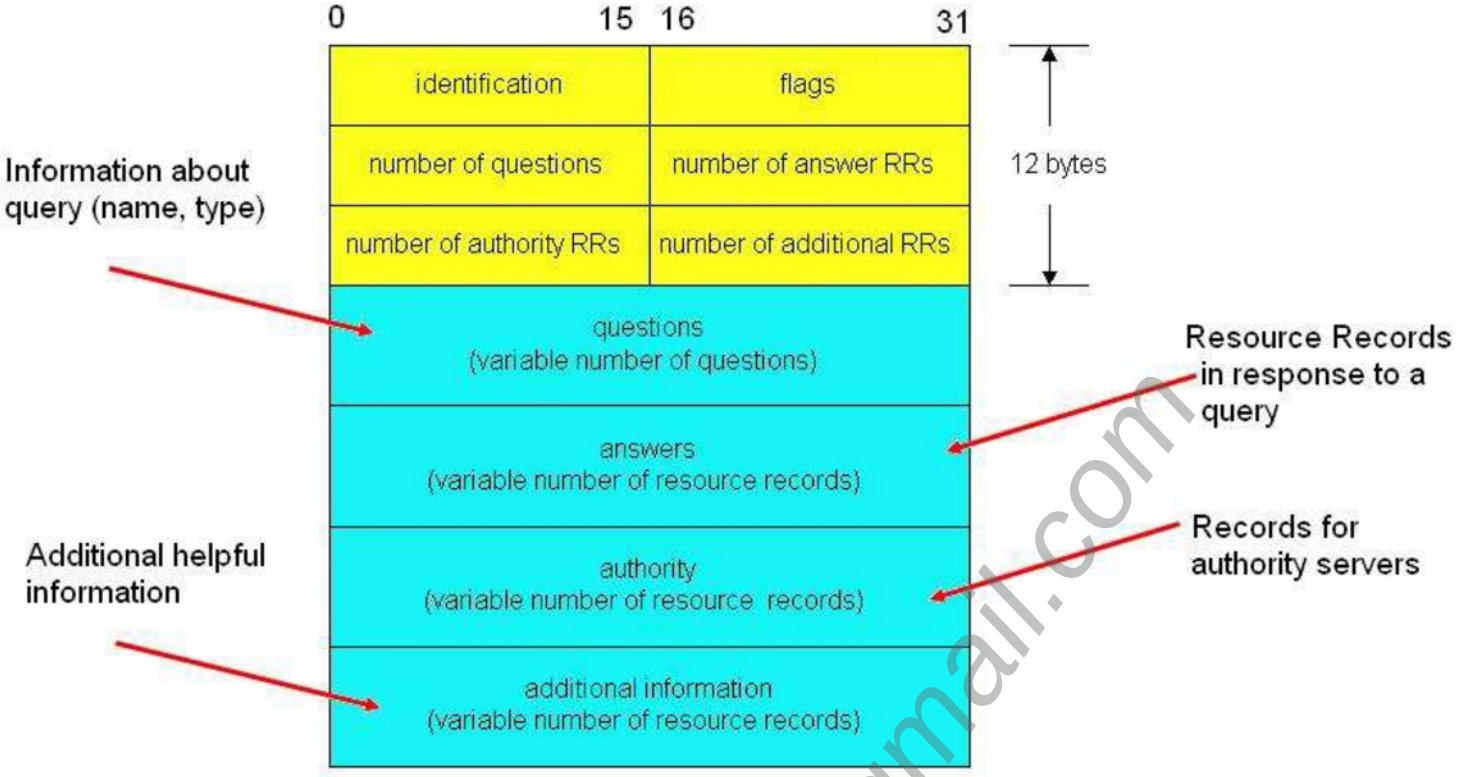
DNS record

- The DNS server includes resource record that provide hostname to IP address mapping.
- A resource record has four fields: **(Name, Value, Type, TTL)**
- TTL is the time to live the resource record.
- Name and Value depends on type
- If type=A i.e. **Authoritative**, then name is host name and value is IP address for hostname. Example:
  (relay1.bar.foo.com, 192.168.1.5, A) is a type of A Record

- If Type=NS i.e. **Name Server**, then Name is a domain (such as foo.com) and Value is the hostname of a server that knows how to obtain the IP addresses for hosts in the domain. This record is used to route DNS queries further along in the query chain. Example
  (www.foo.com, relay1.bar.foo.com, NS) is a Type NS record.
- If Type=CNAME i.e. **Cannonical Name**, then Value is a canonical hostname for the alias hostname Name. Example
  (foo.com, www.foo.com, CNAME) is a CNAME record.
- If Type=MX i.e. **Mail Exchange**, then Value is a hostname of a mail server that has an alias hostname Name. Example,
  (gmail.com. mail.google.com, MX) is an MX record.
  MX records allow the hostnames of mail servers to have simple aliases an MX record is used to tell the world which mail servers accept incoming mail for your domain and where emails sent to your domain should be routed to

DNS Message

These are the only two kinds of DNS messages. Both request and reply messages have the same format as shown in figure below.



- **The first 12 bytes is the header section, which has a number of fields.**
- **The first field is a 16-bit number that identifies the query.** This identifier is copied into the reply message to a query, allowing the client to match received replies with sent queries.
- There are a number of flags in the flag field (16 bit) each of which stores 1 and 0. For example, **A one-bit query reques/reply flag indicates whether the message is a request (0) or a reply (1). A one-bit authoritative flag is set in a reply message when a name server is an authoritative server for a queried name.** A one-bit recursion-desired flag is set when a client (host or name server) desires that the name server to perform recursion when it doesn't have the record. A one-bit recursion available field is set in a reply if the name server supports recursion.
- **In the header, there are also four "number of" fields.** These fields indicate the number of occurrences of the four types of "data" sections that follow the header.
- **The question section contains information about the query that is being made. This section includes**
  - **i. A name field that contains the name that is being queried,**
  - **ii. A type field that indicates the type of question being asked about the name (e.g., a host address associated with a name - type "A", or the mail server for a name - type "MX").**
- **In a reply from a name server, the answer section contains the resource records i.e. DNS record for the name that was originally queried.** Recall that in each resource record there is the Type (e.g., A, NS, CSNAME and MX), the Value and the TTL. A reply can return multiple RRs in the answer, since a hostname can have multiple IP addresses (e.g., for replicated Web servers, as discussed earlier in this section).
- **The authority section contains records of other authoritative servers.**
- **The additional section contains other "helpful" records. For example, the answer field in a reply to an MX query will contain the hostname of a mail server associated with the alias name Name e.g. gmail.com. The additional section will contain a Type A record providing the IP address for the canonical hostname of the mail server i.e. mail.google.gmail.com**.

Concept of Mail Server and Protocols

SMTP (Simple Mail Transfer Protocol)

- SMTP transfers messages from senders' mail servers to the recipients' mail servers.
- SMTP supports:
  - Sending a message to one or more recipients.
  - Sending message that includes texts, voice, video or graphics.
  - Sending message to users on the network outside the Internet.
- SMTP supports sending of email only It cannot pull messages from a remote server on demand. Other protocols, such as the Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP) are specifically designed for retrieving messages and managing mail boxes.
- However, SMTP has a feature to initiate mail queue processing on a remote server so that the requesting system may receive any messages destined for it.
- SMTP has two sides: **a client side which executes on the sender's mail server**, and **server side which executes on the recipient's mail server**. **Both the client and server sides of SMTP run on every mail server. When a mail server sends mail (to other mail servers), it acts as an SMTP server. When a mail server receives mail (from other mail servers) it acts as an SMTP client.**
- To illustrate the basic operation of SMTP, let's walk through a common scenario. Suppose Alice wants to send Bob a simple ASCII message:

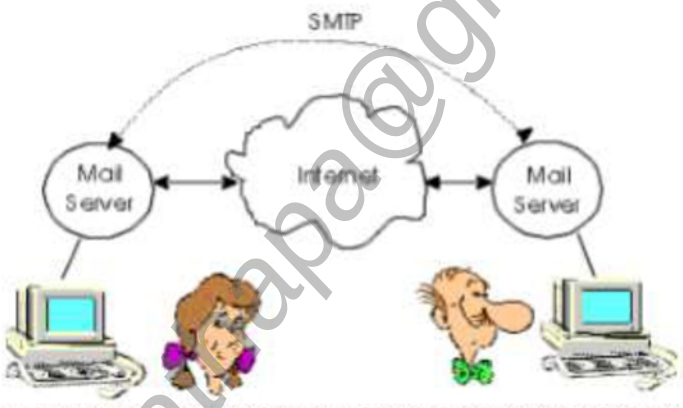


Figure 2.4-2: Alice's mail server transfers Alice's message to Bob's mail server.

- Alice invokes her user agent for email, provides Bob's email address (e.g., bob@someschool.edu), composes a message and instructs the user agent to send the message.
- Alice's user agent sends the message to her mail server, where it is placed in a message queue.
- The client side of SMTP i.e. SMTP client, running on Alice's mail server, sees the message in the message queue.
- It opens a TCP connection to a SMTP server, running on Bob's mail server.
- After some initial SMTP handshaking, the SMTP client sends Alice's message into the TCP connection.
- At Bob's mail server host, the server side of SMTP i.e. SMTP server receives the message.
- Bob's mail server then places the message in Bob's mailbox.
- Bob invokes his user agent to read the message at his convenience using POP or IMAP protocol.

POP3 (Post Office Protocol version 3)

- An Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts.
- SMTP provides the underlying transport mechanism for sending e-mail messages over the Internet, but it does not provide any facility for storing messages and retrieving them. SMTP hosts must be continuously connected to one another, but most users do not have a dedicated connection to the Internet.
- **Post Office Protocol version 3 (POP3) provides mechanisms for storing messages sent to each user and received by SMTP in a receptacle called a mailbox.**
- A POP3 server stores messages for each user until the user connects to download and read them using a POP3 client such as Microsoft Outlook 98, Microsoft Outlook Express, or Microsoft Mail and News.

- POP3 begins when the user agent (the client) opens a TCP connection to the the mail server (the server) on port 110. With the TCP connection established, POP3 progresses through three phases: authorization, transaction and update. During the first phase, authorization, the user agent sends a user name and a password to authenticate the user downloading the mail. During the second phase, transaction, the user agent retrieves messages. During the transaction phase, the user agent can also mark messages for deletion, remove deletion marks, and obtain mail statistics. The third phase, update, occurs after the client has issued the quit command ending the POP3 session; at this time, the mail server deletes the messages that were marked for deletion.

IMAP (Internet Mail Access Protocol)

- An Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts. Internet Mail Access Protocol version provides functions similar to Post Office Protocol version 3 (POP3), with additional features.
- The main problem with pop3 is
  After downloading the messages to the local machine using POP3, we can create mail folders and move the downloaded messages into the folders. We also can then delete messages, move messages across folders, and search for messages (say by sender name or subject). But this paradigm -- folders and messages in the local machine -- poses a problem for the nomadic user, who would prefer to maintain a folder hierarchy on a remote server that can be accessed by from any computer. This is not possible with POP3.
- IMAP4 includes a number of features that are not supported by POP3. Specifically, IMAP4 allows users to
  - Access multiple folders, including public folders
  - Create hierarchies of folders for storing messages
  - Leave messages on the server after reading them so that they can access the messages again from another location
  - Search a mailbox for a specific message to download
  - Flag messages as read
  - Selectively download portions of messages or attachments only
  - Review the headers of messages before downloading them
- To retrieve a message from an IMAP4 server, an IMAP4 client first establishes a Transmission Control Protocol (TCP) session using TCP port 143. . The IMAP server is always in one of four states.
- In the non-authenticated state, which starts when the connection starts, the user must supply a user name and password before most commands will be permitted.
- In the authenticated state, the user must select a folder before sending commands that affect messages.
- In the selected state, the user can issue commands that affect messages (retrieve, move, delete, retrieve a part in a multipart message, etc.).
- Finally, the logout state is when the session is being terminated.

Introduction to network management

- A network consists of *many* complex, interacting pieces of hardware and software - from the links, bridges, routers, hosts and other devices that comprise the physical components of the network to the many protocols that control and coordinate these devices.
- When hundreds or thousands of such components are cobbled together by an organization to form a network, it is not surprising that components will occasionally malfunction, that network elements will be misconfigured, that network resources will be over utilized, or that network components will simply "break" (e.g., a cable will be cut, a can of soda will be spilled on top of router).
- The network administrator, whose job it is to keep the network "up and running," must be able to respond to (and better yet, avoid) such mishaps.
- With potentially thousands of network components spread out over a wide area, the network administrator in a network operations centre (NOC) clearly needs **tools** to help monitor, manage, and control the network.

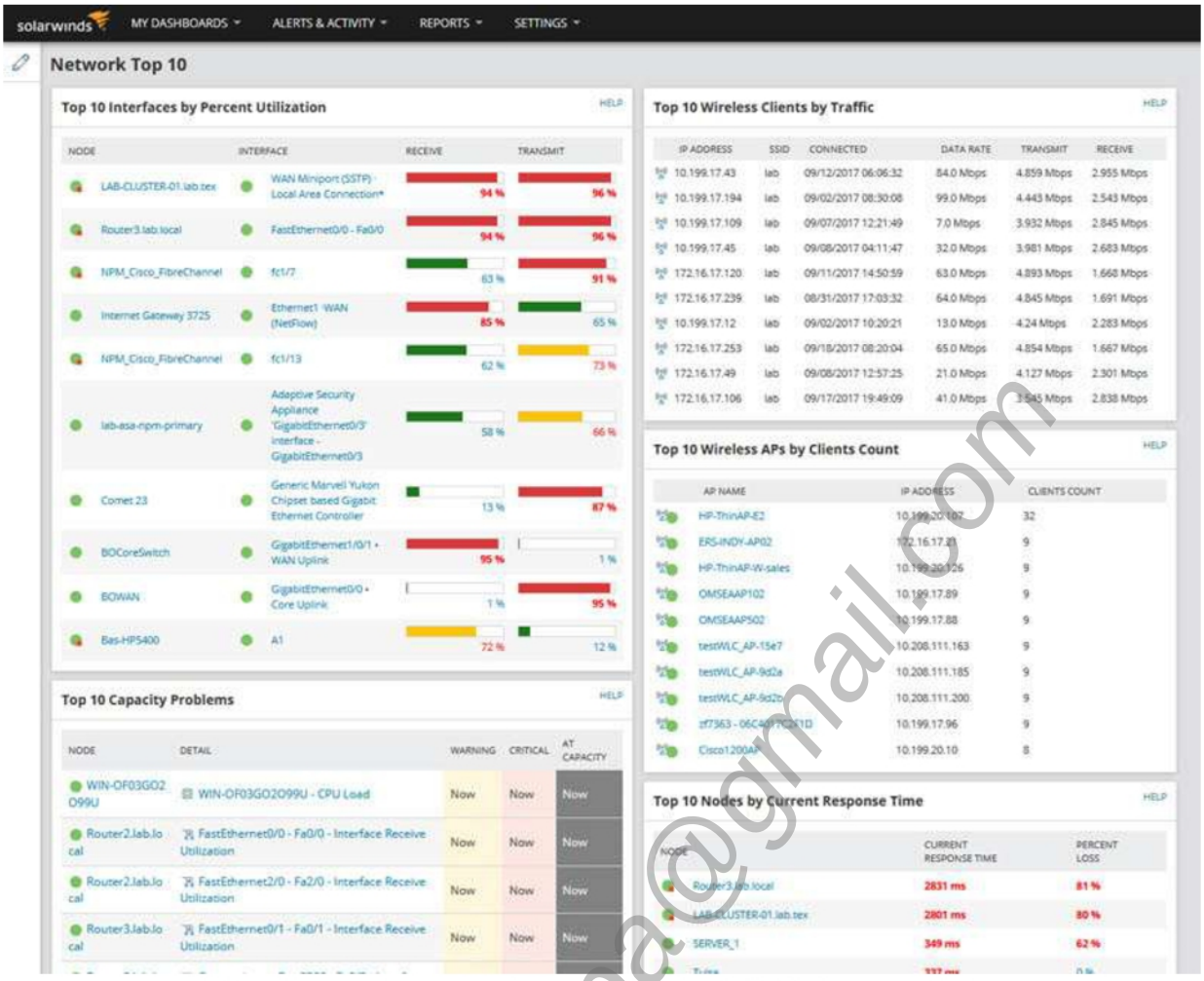


Fig: Network Analysis provided by NMS(Solar winds)

- ***"Network management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, poll, configure, analyse, evaluate and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."***

Advantage of proper Network Management

1. **Optimizing network availability and performance**

   Network availability can be thought of as how it easy it for one point of the IP infrastructure to reach another. With networks becoming more widely dispersed and supporting more operations than ever before, achieving optimal availability—and fulfilling SLA requirements—requires a top-flight solution.

   Network management software can proactively and automatically gather data about the network, giving administrators information about problems before someone else reports the issue via SMS or email. Performance can be analyzed in real time through functionalities that look at packet drops and throughout.

2. **Lowering expenses by improving asset utilization**

   The number of IP-enabled endpoints is rising. Cisco has predicted that mobile and wireless devices will generate more traffic than wired ones by 2016 and account for 55 percent of all activity by 2017. In this context, it is important for administrators to know what's connecting to their networks and whether their infrastructure is equipped to handle major fluctuations, if only to keep costs under control as conditions evolve.

3. **Effective change management**

   Often it is useful to have records of past network configurations in case something needs to be reverted. Network management software enables efficient change management so that users can establish solid baselines for performance.

4. **Achieving service level agreements and documenting performance with reports**

   With the advent of Service Level Agreements (SLA) - contracts that define specific performance metrics and acceptable levels of network provider performance with respect to these metrics These SLAs include service availability (outage), latency, throughput and outage notification requirements. Clearly, if performance criteria are to be part of a service agreement between a network provider and its users, then measuring and managing performance will be of great importance to the network administrator.

5. **Intrusion detection**

   A network administrator may want to be notified when network traffic arrives from, or is destined to, a suspicious source (e.g., host or port number). Similarly, a network administrator may want to detect (and in many cases filter) the existence of certain types of traffic that are known to be characteristic of certain attacks.

The infrastructure for network management

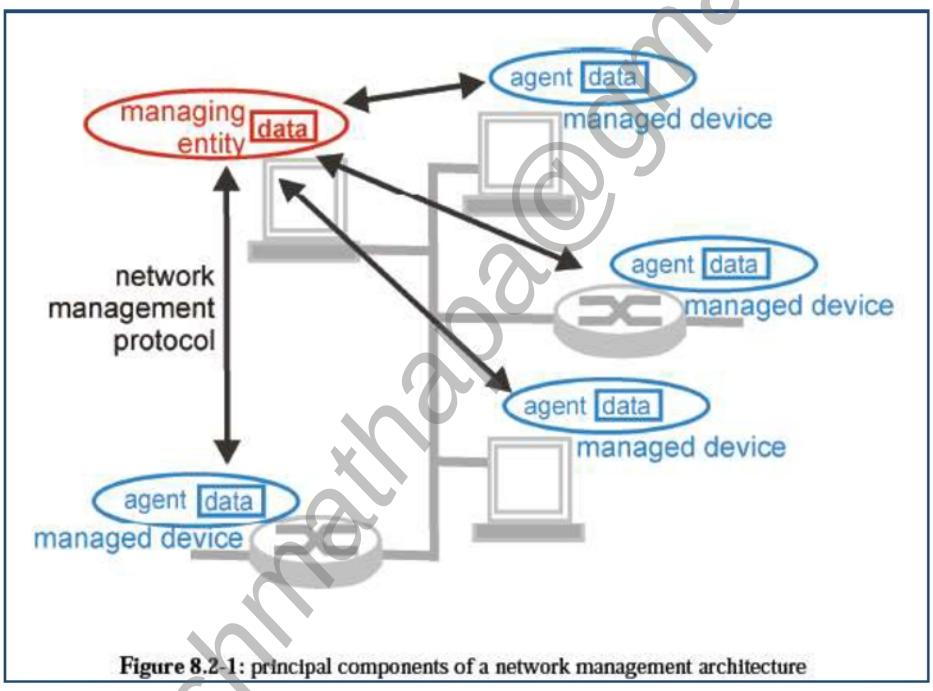


Figure 8.2-1: principal components of a network management architecture

- **The managing entity** is an application, typically with a human-in-the-loop, running in a centralized network management station in the network operations center (NOC). It controls the collection, processing, analysis, and/or display of network management information.

- **A Managed Device** is a piece of network equipment that resides on a managed network. It might be host, router, bridge, hub or printer. Managed Device contains several Managed Objects. These managed objects are the actual pieces of hardware within the managed device (e.g., a network interface card), and the sets of configuration parameters for the pieces of hardware and software (e.g., an intradomain routing protocol such as RIP). Managed Object have Piece of information associated with them that are collected into management information base(MIB). Finally, a network management agent resides in each managed device. An agent is a process running in the managed device that communicates with the managing entity, taking local actions on the managed device under the command and control of the managing entity.

- The third part of network management architecture is **Network management protocol.** Network Management Protocol runs between Managing Entity and Managed Device allowing the managing entity to query the status of managed devices and indirectly effect actions in these devices via its agents. Agents can use the network management protocol (**Example: SNMP**) to inform the managing entity of exceptional events

SNMP

- Simple Network Management Protocol us an application layer protocol for exchanging management information between network devices.
- It is one of the widely accepted protocols to manage and monitor network elements.
- Most of the network elements like router, hubs, switches, etc. come with the bundle of SNMP agent. These agents has to be enabled and configured to communicate with the **network management system**.
- SNMP consists of following components.
  1. SNMP manager i.e. managing entity
  2. Managed Device
  3. SNMP agent
  4. Management information base

Assignment:

1. **Differentiate between HTTP and HTTPs**
2. **Write short notes on**
   - **i. Proxy server**
   - **ii. Firewall and its type**

Proxy Server

- A computer that can act on the behalf of other computers to request content from the Internet or an intranet.
- **Proxy Server is placed between a user's machine and the Internet.**
- It can act as a **firewall to provide protection and as a cache area** to speed up Web page display.
- A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
- Proxy servers have two main purposes:
  1. Improve Performance: Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users.
  2. Filter Requests: Proxy servers can also be used to filter requests.

Types of Proxy Server

1. **Forward Proxy**
   - In this client requests its internal network server to forward the internet.
   - So this proxy can be used by client to bypass firewall restrictions in order to visit blocked websites.
   - There are many paid proxy services that has numerous proxy system around the world so that they can change your IP address every time you visit a new web page and make it harder for website administrator to detect.

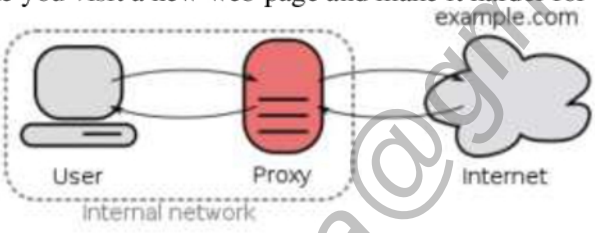


Fig:A forward proxy taking requests from an internal network and forwarding them to the Internet

2. **Open proxy**
   - An open proxy is a forward proxy server that is accessible by any Internet user.
   - Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet

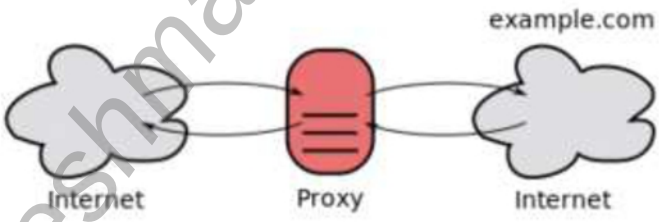


Fig: An open proxy forwarding requests from and to anywhere on the Internet.

3. **Reverse Proxy**
   - In this proxy, the requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original server.
   - It is generally used by network administrator to achieve load balancing and high availability.
   - The reverse proxy server take request from internet then forward to one of the web server however the user is unaware about proxy server and its operation.

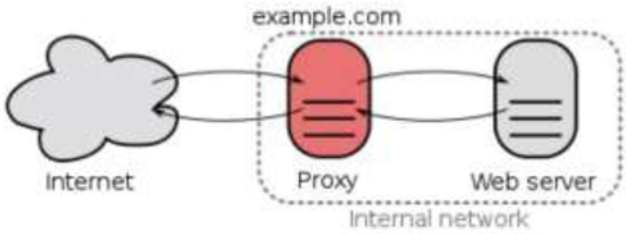
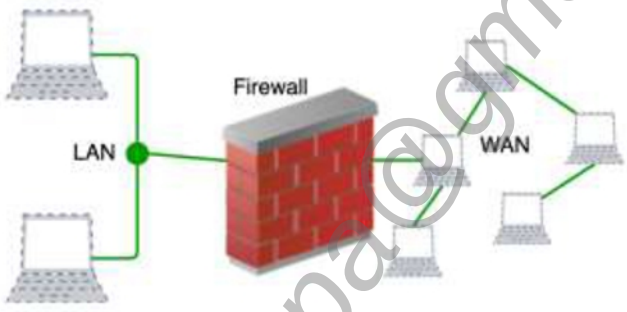


Fig: A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.

Firewall

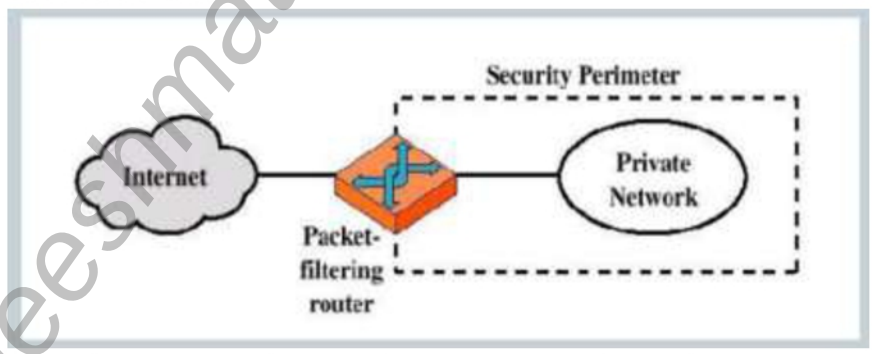
- A Firewall is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.
- It is any system or device that allows safe network traffic to pass while restricting or denying unsafe traffic.
- Firewalls are usually dedicated machines running at the gateway point between your local network and the outside world, and are used to **control** who has access to your private corporate network from the outside—for example, over the Internet.



- Some firewall also blocks traffic and services that are not desired.

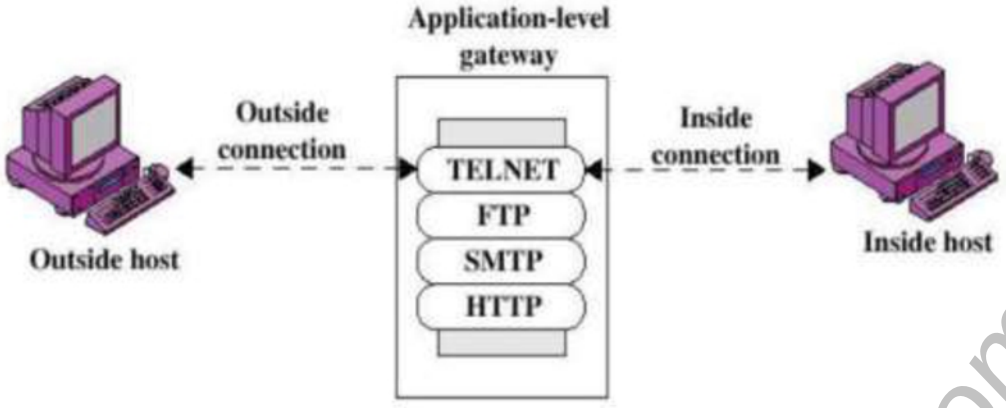
Types of firewall

1. **Packet Filter/ Packet Level Firewall**



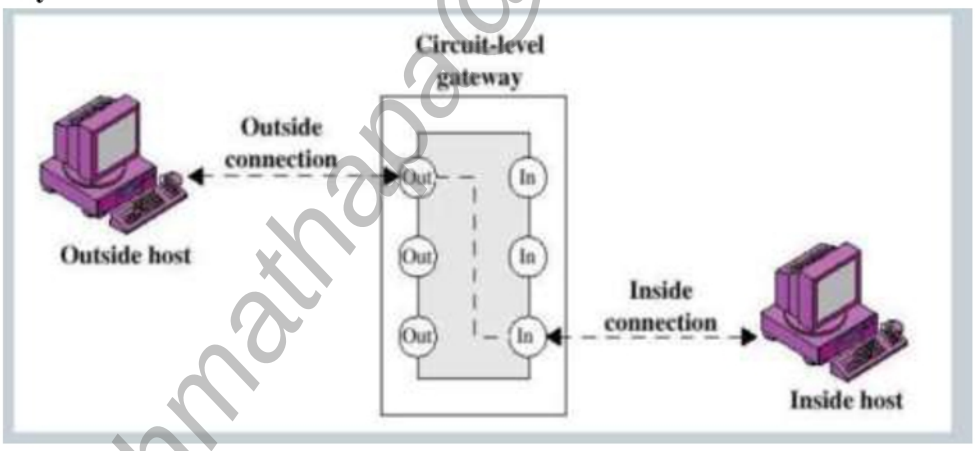
- It is one of the most basic traffic control mechanism among firewall technologies.
- Packet filter applies a set of rules to each incoming IP packet and then forwards or discards the packet
- It filters packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- It implements two default policies (discard or forward)
- Packet Filtering mechanisms work in the network layer of the OSI model.

2. Application level Firewall / Proxy Server



- Application level firewall are also called proxy server
- It acts as a relay of application-level traffic like FTP, SMPT etc.
- A proxy server sits between the client and destination working as middleman between two communicating parties.
- It requires the client to establish session with the proxy itself, which in turns creates a second session between itself and the destination.
- For example: A client requiring to request some HTTP information from web first need to create session with the proxy server then the proxy server authenticates whether the client request is valid or not, if the client request is valid, the proxy server creates a second session between the web server and itself.

3. Circuit level gateway



- Another type of firewall is a circuit-level gateway, which is usually a component of a proxy server.
- With a circuit-level firewall, connections with the private network are hidden from the remote user.
- The remote user connects with the firewall, and the firewall forms a separate connection with the network resource being accessed **after changing** the IP address of the packets being transmitted in either direction through the firewall.
- This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet). This way, the packets are tagged with only the Public IP address (Firewall level) and the internal private
- The circuit level gateway firewalls work at the session layer of the OSI model.

4. Stateful Packet Filter

- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in the session flow table.
- This table contain source ip address, destionation ip address, port number and TCP protocol information.

- Before traffic can travel back through the firewall, stateful inspections of the packets are cross-checked to the session flow tables for an existing connection slot.
- If match is mound, the packets are forwarded otherwise the packets are dropped or rejected.