Computer Networks-2

Protocols

It is a set of rules . Protocols are followed by nodes/servers etc for communication purposes.

Various types of protocols are:

- http
- ftp
- pop3
- imap
- smtp
- VoIP
- nfc

Protocols

- **http**- it is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

Protocols

- **HTTP- (hypertext transfer protocol)-**

1. It is used for viewing web pages.

2.In standard HTTP, all information is sent in clear text.

3. It is vulnerable to hackers.

- **HTTPS-(Secure hypertext transfer protocol)**

1. HTTP with a security feature.

2. It encrypts the data that is being retrieved by HTTP.

3. It uses encryption algorithms to scramble the data that's being transferred.

4. In this all information is sent in encrypted text.

Protocols

- **ftp**- it transfers file from one host to another. Efficient for sending and receiving larger files.
  - Advantages-used for transfer files from one network in organization to another. Allow geographically dispersed group to co-operate on a project.
  - ftp also works as a client server process

- **FTP-(file transfer protocol)-**

1. It is used to transfer files over a network.

2.It is standard protocol that is used to transfer files between computers and servers over a network.

3. FTP is the language that computers use to transfer files over a TCP/IP network.

4. Sometimes FTP servers will require an account with a username and password.and sometimes we can just log in anonymously.

5. FTP common uses:

   a) transferring files between computers.

   b) gives the ability of website designers to upload files to their web servers.

6. It is not a secure protocol.

7. Data being transferred is not encrypted.

8. Data is sent in clear text.

9. Should only be used on a limited basis.

- **SFTP-(secure file transfer protocol)**

1. It adds a layer of security.

2. Data is encrypted using secure shell.

3. Authenticates the user and the server.

TFTP-(Trivial File Transfer Protocol)

1. It is very simple transfer protocol.
2. Not used to transfer files over the internet.
3. Mainly used for transferring files within a LAN.
4. It is **connectionless protocol**.
5. Uses UDP(User Datagram Protocol) instead of TCP.
6. It doesnot provide any security during data transfer.

Note:

1. FTP and SFTP are **connection oriented protocols.**
2. They both use TCP for file transfer.

Protocols

- **pop3(post office protocol 3)-** this protocol is used by email clients to retrieve email messages from mail servers over TCP/IP network.
  - pop3 deletes emails on the server after downloading then on our local email client.
  - pop3 supports only one mail server for each mailbox.
  - pop3 works on 2 ports:
    - port 110-default,non encrypted port, used for unsecured email communications
    - port 995 – encrypted port, used for secure email communications

port-in computer networking, a port is a communication endpoint. Physical as well as wireless connections are terminated at ports of hardware devices. At the software level, within an operating system, a port is a logical construct that identifies a specific process or type of network service. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number.

Protocols

Port number	assigned protocol
20	FTP data transfer
21	ftp command control
22	secure login
23	telnet –remote service login, unencrypted text messages
25	smtp –email routing
53	dns
80	http- used in www
110	pop3
119	network news transfer protocol(NNTP)
143	IMAP
194	Internet Relay chat (IRC)
443	HTTP secure (HTTPS) . HTTP over TLS/SSL

Protocols

- IMAP-(Internet Message Access Protocol)- It enable email clients to retrieve email messages from mail servers over a TCP/IP connection. IMAP is designed to retrieve messages from multiple mail servers and consolidate them all in the user's mailbox.
- E.g. a corporate client handling multiple corporate accounts through a local mailbox located on his system.
- All modern email clients and servers like Gmail, outlook and yahoo mail support IMAP or POP3 protocol.

- **POP3 and IMAP –both are used for receiving mails**

- **POP3-(post office protocol 3)**

1.It is used for retrieving email from an email server.

2.It is download the email to your device from a mail server and only download inbox's email.

3.In pop3 , the email is deleted on the mail server once it's downloaded to a device.

4.It does not sync folders.

5.In pop3,downloaded email is viewable without an internet connection.

6.POP3 saves storage space on the mail server.

- **Disadvantages:**

1.We need a backup plan for our email incase device crashes or is lost.

2.Device is more vulnerable to viruses since the emails are fully downloaded.

- ---

- **IMAP- (Internet Message Access Protocol)**

1.It allows you to view your email, that is on the server, from multiple devices.

2.It caches local copies of the email onto all of your devices.

3.It does sync folders.

4.All the email is stored on the server.

5.We are able to see all our email including sent items,drafts,deleted items and any custom folders.

6. All the emails and folders are synchronized.

- **Disadvantages:**

1. Email is not viewable without an internet connection.(because IMAP only caches local copies of the email on your device instead of downloading them.)

Advantages of IMAP over POP3

- Faster response time than POP3
- Multiple mail clients connected to a single mailbox simultaneously.
- Keep track of message state like read, deleted, starred, replied etc
- Search for messages on the server.

- IMAP works on 2 ports:
- port 143- default, non encrypted port, used for unsecured email communications.
- port 993-encrypted port used for secure email communications

Protocols

SMTP-(Simple Mail Transfer Protocol)-

- 1. It is used for sending email i.e. It is designed to send and distribute outgoing E-mail.
- 2. It is a set commands that authenticates and directs the transfer of email.
- 3. SMTP- we can say smtp is “sending mail to people”. It is similar to a mailman.
- 4.It uses TCP protocol. (TCP guarantees email delivery(assuming that the email address exists).

SMTP- works on 2 ports:

- port45 – default, non encrypted port, used for unsecured email communications
- Port465-encrypted port, used for secure email communications.

Protocols

- VoIP-(Voice over Internet Protocol). It is a set of protocols that provides telephone services over internet.
- Earlier internet had been used for exchanging messages. It is now possible to deliver voice communication over IP networks by converting voice data into packets.
- NFC(near field communication)- It is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them 4cm(1 ½ in) of each other.

How HTTP works- a basic idea

- http client's (web browser) request message (http request) is sent to an http server (web server) in the form of urls.
- http server fetches information as per the request & send response message to http client response message can be an error if requested url does not exist.
- http client receive –interpret –display the message.
- http is a stateless protocol, means current request does not know what has been done in the previous requests.

Working of an E-mail

- Compose email, send it from email client.
- Email client connect to smtp server(gmail) and hands over email in the required format.
- Outgoing smtp validates sender details and then process the message for sending and places in outgoing queue.
- Now smtp server retrieves recipient server i.e yahoo.com, information(<mail exchange> MX records),based on the domain details in the recipient address(abc123@yahoo.com)
  - MX records are necessary for delivering email to recipient address. MX record specifies the mail server responsible for accepting email messages on behalf of a domain name.

- Now smtp server retrieve address of smtp server of yahoo.com & connects with recipient email server and sends the email.
- Recipient server validates recipient account i.e. abc123 on the server yahoo.com and delivers the email.
- Now recipient can see the received email.

Secure Communication

- Secure communication is when two nodes/devices are communicating and do not want a third party to listen in .
- To ensure safety of the information being transmitted over the web, many internet security measures are employed.
- **Encryption-** data encryption translates data into another form, or code, so that only people with access to a secret key (called decryption key) or password can read it. Encrypted data is commonly referred to as cipher text.
- https-(Hyper Text Transfer Protocol Secure)- It is a protocol for securing the communication between two systems. E.g. the browser and the web server.
  - HTTPS established an encrypted link between the browser and the web server using the secure socket layer(SSL) or transport layer security (TLS) protocols. TLS is the new version of SSL.

(lock indicated that site is secure)

Secure Communication

SSL- It is the standard security technology for establishing an encrypted link between the two systems. The https is essentially http over SSL. SSL establishes an encrypted link using an SSL certificate which is known as digital certificate. **Uses port 443 by default.**

HOW SSL works:

- A browser or server attempts to connect to a website(i.e web server) secured with SSL. The browser /server requests that the web server identify itself.
- The web server sends the browser /server a copy of its SSL certificate.
- The browser /server checks to see whether or not it trusts the SSL certificate. If sp, it sends a message to the web server.
- The web server sends back a digitally signed acknowledgement to start an SSL encrypted session.
- Encrypted data is shared between the browser /server and the web server.

- ## SSL- (secure sockets layer)

1. This protocol is used to ensure security on the internet.

2. It uses public key encryption to secure data.

3. An SSL certificate is used to authenticate the identity of a website.

- ## TLS- (transport layer security)

1.It is the successor of SSL i.e new version of SSL.

2. It is the latest industry standard cryptographic protocol.

3.It authenticates the server, client, and encrypts the data.

Note:

1.A lot of websites are now using HTTPS by default, regardless if sensitive data is going to be exchanged or not.

2. Google is flagging websites as "not secure" if they are not SSL protected.

3. Google is penalizing websites that are not SSL protected.