Chapter 4

FTP

File Transfer Protocol(FTP) is an application layer protocol which moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.

What is control connection?
For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.
What is data connection?
For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20. FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.
FTP Session :
When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.
Data Structures : FTP allows three types of data structures :

1. File Structure – In file-structure there is no internal structure and the file is considered to be a continuous sequence of data bytes.
2. Record Structure – In record-structure the file is made up of sequential records.
3. Page Structure – In page-structure the file is made up of independent indexed pages.

TFTP - Trivial File Transfer Protocol (TFTP)

Trivial file transfer protocol (TFTP) is suited for those applications that do not require complex procedures of FTP and do not have enough resources (RAM, ROM) for this purpose.
Typical applications of TFTP include loading the image on diskless machine and upgrading the operating system in network devices such as routers.
The main features TFTP are :
1. TFTP is based on client/server principle.
2. It uses Well-known UDP port number 69 for TFTP server.
3. TFTP 1S unsecured protocol.
4. TFTP does not support authentication.
5 Every TFTP data unit has a sequence number.
6. Each data unit is individually acknowledged. After receiving the acknowledgement the next data unit is sent.
7. Error recovery is by retransmission after timeout.

S.NO	FTP	TFTP
1.	FTP stands for File Transfer Protocol.	TFTP stands for Trivial File Transfer Protocol.
2.	The software of FTP is larger than TFTP.	While software of TFTP is smaller than FTP.
3.	FTP works on two ports: 20 and 21.	While TFTP works on 69 Port number.

4.	FTP services are provided by TCP.	While TFTP services are provided by UDP.
5.	The complexity of FTP is higher than TFTP.	While the complexity of TFTP is less than FTP complexity.
6.	There are many commands or messages in FTP.	There are only 5 messages in TFTP.
7.	FTP need authentication for communication.	While TFTP does not need authentication for communication.

The Telnet Protocol

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

The Telnet protocol is designed to provide a bi-directional, eight-bit byte oriented communications facility to allow for a a standard method of interfacing terminal devices and processes.

Using Telnet to Test Open Ports

One of the biggest perks of Telnet is with a simple command you can test whether a port is open. Issuing the Telnet command telnet [domainname or ip] [port] will allow you to test connectivity to a remote host on the given port.

Issue the following command in the Command Prompt:

telnet [domain name or ip] [port]

Put the IP address or domain name of the server you're trying to connect to in place of [domain name or ip], and replace the second brackets with the port number on the remote machine, connection to which you want to test. For example, to verify connection to 192.168.0.10 on port 25, issue the command:

telnet 192.168.0.10 25

If the connection succeeds, a blank screen will show up, meaning that the computer port is open.

A failed connection will be accompanied by an error message. It can indicate either a closed port or the fact that the indicated remote server is not listening on the provided port.

Simple Mail Transfer Protocol (SMTP)

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.

POP3

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail, probably using POP3.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

The conventional port number for POP3 is 110.

IMAP

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

- Port 143 - this is the default IMAP non-encrypted port
- Port 993 - this is the port you need to use if you want to connect using IMAP securely

HTTP

TTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

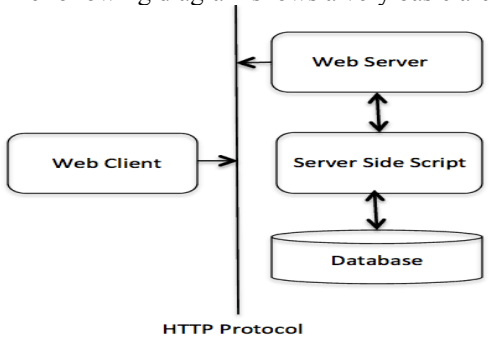
Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- HTTP is connectionless: The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.
- HTTP is media independent: It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- HTTP is stateless: As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

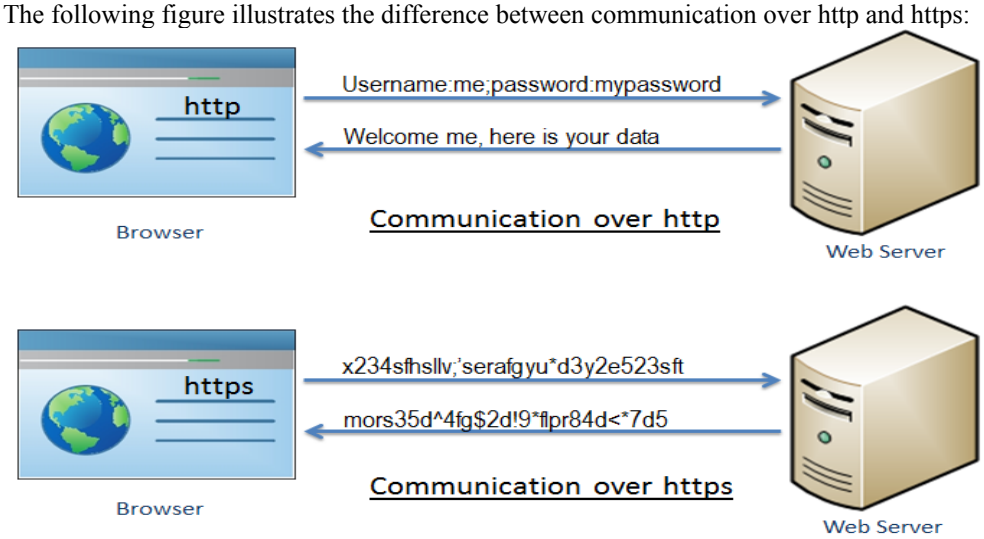
Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

HTTPS

HTTPS stands for Hyper Text Transfer Protocol Secure. It is a protocol for securing the communication between two systems e.g. the browser and the web server.

The following figure illustrates the difference between communication over http and https:



Communication over https and http

As you can see in the above figure, http transfers data between the browser and the web server in the hypertext format, whereas https transfers data in the encrypted format. Thus, https prevents hackers from reading and modifying the data during the transfer between the browser and the web server. Even if hackers manage to intercept the communication, they will not be able to use it because the message is encrypted.

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.

Advantage of https

- Secure Communication: https makes a secure connection by establishing an encrypted link between the browser and the server or any two systems.
- Data Integrity: https provides data integrity by encrypting the data and so, even if hackers manage to trap the data, they cannot read or modify it.
- Privacy and Security: https protects the privacy and security of website users by preventing hackers to passively listen to communication between the browser and the server.
- Faster Performance: https increases the speed of data transfer compared to http by encrypting and reducing the size of the data.
- SEO: Use of https increases SEO ranking. In Google Chrome, Google shows the Not Secure label in the browser if users' data is collected over http.
- Future: https represents the future of the web by making internet safe for users and website owners.

http vs https

http	https
Transfers data in hypertext (structured text) format	Transfers data in encrypted format
Uses port 80 by default	Uses port 443 by default
Not secure	Secured using SSL technology
Starts with http://	Starts with https://

Ping Command

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

```
ping 127.0.0.1
```

In the above example, we're pinging 127.0.0.1, also called the IPv4 localhost IP address or IPv4 loopback IP address, without options.

Using the ping command to ping 127.0.0.1 is an excellent way to test that Windows' network features are working properly

```
ping 192.168.2.1
```

Similar to the ping command examples above, this one is used to see if your computer can reach your router. The only difference here is that instead of using a ping command switch or pinging the localhost, we're checking the connection between the computer and the router (192.168.2.1 in this case).

ipconfig cmd

The ipconfig command is used to find out your current local IP address, default gateway, TCP/IP settings and more. With IPCONFIG you can not only find out your IP Address, find your default gateway and find your subnet mask, you can release and renew, resolve the DNS, troubleshoot internet connections and more. This is a very handy network tool for finding your local IP address as well as many other secrets.

```
ipconfig /all
```

To display all of your current IP information for all adapters. With ipconfig /all you can also find out your DNS Server and MAC Address. This will show your ethernet adapters full TCPIP configuration for all adapters on your Windows computer. You can find out your own IP Address as well as your default gateway.

NTP

NTP stands for Network Time Protocol, and it is an Internet protocol used to synchronize the clocks of computers to some time reference. NTP is an Internet standard protocol originally developed by Professor David L. Mills at the University of Delaware.

Why should Time be synchronized?

Time usually just advances. If you have communicating programs running on different computers, time still should even advance if you switch from one computer to another. Obviously if one system is ahead of the others, the others are behind that particular one. From the perspective of an external observer, switching between these systems would cause time to jump forward and back, a non-desirable effect.

As a consequence, isolated networks may run their own wrong time, but as soon as you connect to the Internet, effects will be visible. Just imagine some EMail message arrived five minutes before it was sent, and there even was a reply two minutes before the message was sent.

Even on a single computer some applications have trouble when the time jumps backwards. For example, database systems using transactions and crash recovery like to know the time of the last good state. Therefore, air traffic control was one of the first applications for NTP.

What are the basic features of NTP?

There exist several protocols to synchronize computer clocks, each having distinguished features. Here is a list of NTP's features:

- NTP needs some reference clock that defines the true time to operate. All clocks are set towards that true time. (It will not just make all systems agree on some time, but will make them agree upon the true time as defined by some standard.)
  NTP uses UTC as reference time (See also What is UTC?).
- NTP is a fault-tolerant protocol that will automatically select the best of several available time sources to synchronize to. Multiple candidates can be combined to minimize the accumulated error. Temporarily or permanently insane time sources will be detected and avoided.
- NTP is highly scalable: A synchronization network may consist of several reference clocks. Each node of such a network can exchange time information either bidirectional or unidirectional. Propagating time from one node to another forms a hierarchical graph with reference clocks at the top.
- Having available several time sources, NTP can select the best candidates to build its estimate of the current time. The protocol is highly accurate, using a resolution of less than a nanosecond (about 2^-32 seconds). (The popular protocol used by rdate and defined in [RFC 868] only uses a resolution of one second).
- Even when a network connection is temporarily unavailable, NTP can use measurements from the past to estimate current time and error.

- For formal reasons NTP will also maintain estimates for the accuracy of the local time.

BOOTP

BOOTP (Bootstrap Protocol) is the successor of RARP (Reverse ARP) and the predecessor of DHCP.
RARP is a link layer protocol and the problem of RARP is that you can't route these packets. You need a RARP server on every subnet. BOOTP uses the UDP transport protocol and rides on top of IP so it can be routed. BOOTP supports relay servers so you can have a central BOOTP server that assigns IP addresses to hosts in all of your subnets.
Another issue with RARP is that it only allows you to assign an IP address, that's it. No default gateway, DNS servers, etc. BOOTP supports all of this. You can assign an IP address, default gateway, subnet mask, DNS servers, and other options.
BOOTP uses UDP port 67 and 68. If you have seen DHCP before then everything I explained so far might sound very familiar. In fact, DHCP is based on BOOTP. The port numbers are the same so you can't run a BOOTP and DHCP server at the same time.
There is a key difference between BOOTP and DHCP though. BOOTP uses a static database that you have to fill yourself. Similar to RARP, you need to enter all MAC addresses and the IP addresses (and other options like a default gateway) you want to use in the database yourself. When a BOOTP server receives a request, it looks in its database for a matching entry and then returns the result to the host.
DHCP servers use a "pool" of addresses. When the DHCP server receives a request, it returns an IP address from the pool that you configured. It doesn't care about the MAC address unless you use a reservation. This is more efficient since you don't waste any IP addresses that are not in use.

DHCP

DHCP stands for Dynamic Host Configuration Protocol.
As the name suggests, DHCP is used to control the network configuration of a host through a remote server. DHCP functionality comes installed as a default feature in most of the contemporary operating systems. DHCP is an excellent alternative to the time-consuming manual configuration of network settings on a host or a network device.
DHCP works on a client-server model. Being a protocol, it has it's own set of messages that are exchanged between client and server.
How DHCP Works?
Before learning the process through which DHCP achieves it's goal, we first have to understand the different messages that are used in the process.
1. DHCPDISCOVER
It is a DHCP message that marks the beginning of a DHCP interaction between client and server. This message is sent by a client (host or device connected to a network) that is connected to a local subnet. It's a broadcast message that uses 255.255.255.255 as destination IP address while the source IP address is 0.0.0.0
2. DHCPOFFER
It is DHCP message that is sent in response to DHCPDISCOVER by a DHCP server to DHCP client. This message contains the network configuration settings for the client that sent the DHCPDISCOVER message.
3. DHCPREQUEST
This DHCP message is sent in response to DHCPOFFER indicating that the client has accepted the network configuration sent in DHCPOFFER message from the server.
4. DHCPACK
This message is sent by the DHCP server in response to DHCPREQUEST recieved from the client. This message marks the end of the process that started with DHCPDISCOVER. The DHCPACK message is nothing but an acknowledgement by the DHCP server that authorizes the DHCP client to start using the network configuration it received from the DHCP server earlier.
5. DHCPNAK
This message is the exact opposite to DHCPACK described above. This message is sent by the DHCP server when it is not able to satisfy the DHCPREQUEST message from the client.
6. DHCPDECLINE
This message is sent from the DHCP client to the server in case the client finds that the IP address assigned by DHCP server is already in use.
7. DHCPINFORM
This message is sent from the DHCP client in case the IP address is statically configured on the client and only other network settings or configurations are desired to be dynamically acquired from DHCP server.
8. DHCPRELEASE
This message is sent by the DHCP client in case it wants to terminate the lease of network address it has be provided by DHCP ser

WINS

Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names. WINS is a system that determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangementsThis is the predecessor to DNS and has been deprecated by Microsoft.[1]

DNS

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

The Domain name system comprises of Domain Names, Domain Name Space, Name Server that have been described below:

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as com, edu, gov, net etc, while some country level domain names such as au, in, za, us etc.

DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:

- When we type www.tutorialspoint.com into the browser, it asks the local DNS Server for its IP address.

  Here the local DNS is at ISP end.
- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that I do not know the IP address of www.tutorialspoint.com but know the IP address of DNS Server.
- The local DNS server then asks the com DNS Server the same question.
- The com DNS Server replies the same that it does not know the IP address of www.tutorialspont.com but knows the address of tutorialspoint.com.
- Then the local DNS asks the tutorialspoint.com DNS server the same question.
- Then tutorialspoint.com DNS server replies with IP address of www.tutorialspoint.com.
- Now, the local DNS sends the IP address of www.tutorialspoint.com to the computer that sends the request.

NAT

There are several situations where we need address translation such as, a network which do not have sufficient public IP addresses want to connect with the Internet, two networks which have same IP addresses want to merge or due to security reason a network want to hide its internal IP structure from the external world. NAT (Network Address Translation) is the process which translates IP address. NAT can be performed at firewall, server and router.

Situations where NAT is used

There are no hard and fast rules about where we should use NAT or where we should not use the NAT. Whether we should use the NAT or not is purely depends on network requirement for example NAT is the best solution in following situations: -

- Our network is built with private IP addresses and we want to connect it with internet. As we know to connect with internet we require public IP address. In this situation we can use NAT device which will map private IP address with public IP address.
- Two networks which are using same IP address scheme want to merge. In this situation NAT device is used to avoid IP overlapping issue.
- We want to connect multiple computers with internet through the single public IP address. In this situation NAT is used to map the multiple IP addresses with single IP address through the port number.

Advantages and disadvantages of NAT

Nat provides following advantages: -

- NAT solves IP overlapping issue.
- NAT hides internal IP structure from external world.
- NAT allows us to connect with any network without changing IP address.
- NAT allows us to connect multiple computers with internet through the single the public IP address.

NAT has following disadvantages: -

- NAT adds additional delay in network.
- Several applications are not compatible with NAT.
- End to end IP traceability will not work with NAT.
- NAT hides actual end device.

Ipv6 and ICMPv6

The term ICMP refers to ICMP in general, and the terms ICMPv4 and ICMPv6 to refer specifically to the versions of ICMP used with IPv4 and IPv6, respectively. ICMPv6 plays a far more important role in the operation of IPv6 than ICMPv4 does for IPv4.
In IPv6, ICMPv6 is used for several purposes beyond simple error reporting and signaling. It is used for:

- Neighbor Discovery (ND), which plays the same role as ARP does for IPv4 (Chapter 4).
- Router Discovery function used for configuring hosts (Chapter 6) and multicast address management (Chapter 9).
- Manageing hand-offs in Mobile IPv6.

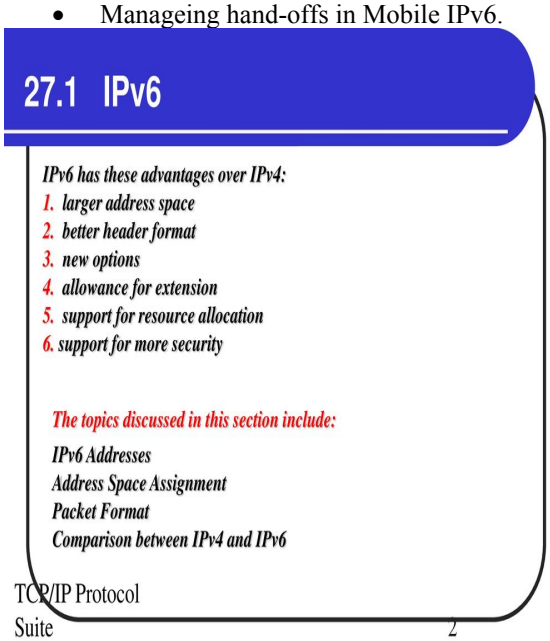


Table 27.7 ***Comparison of error-reporting messages in ICMPv4 and ICMPv6***

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes