Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

SERVER

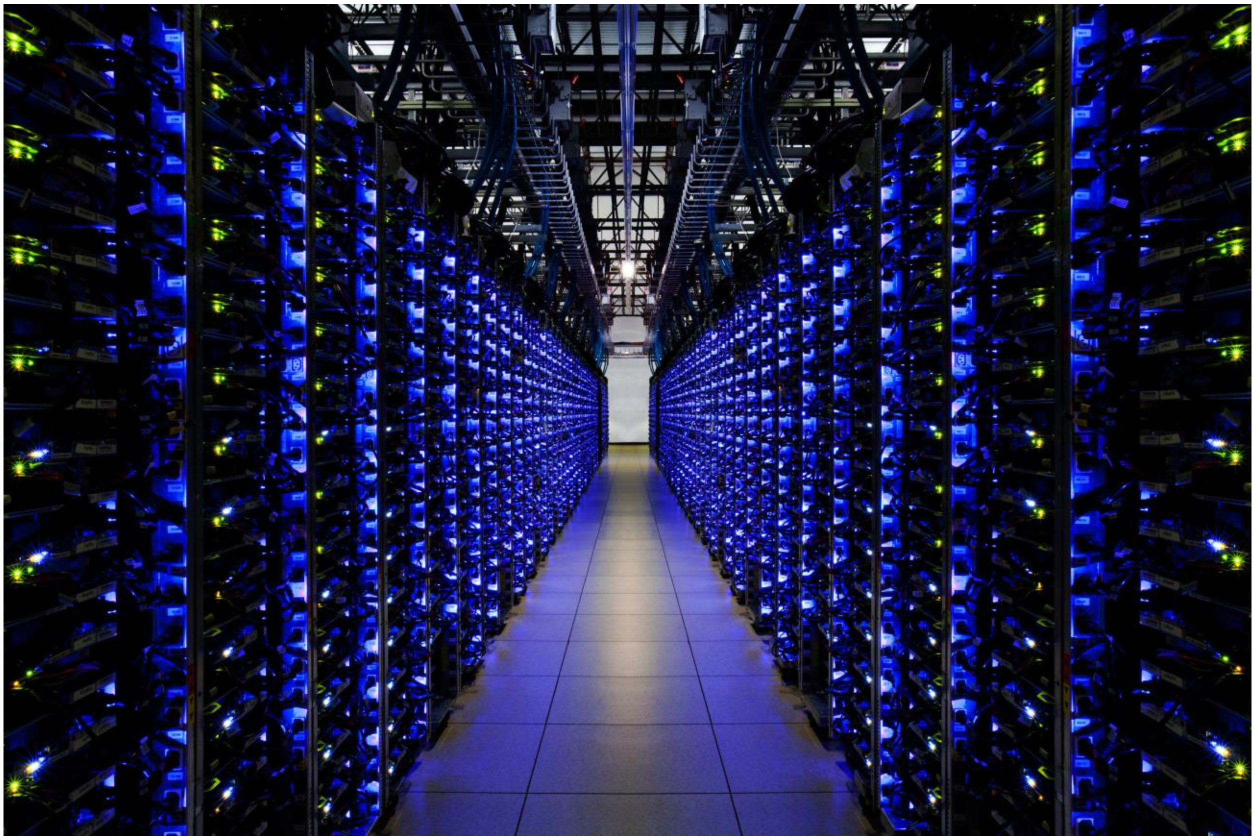
A server is a computer program that provides services to other computer programs (and their users) in the same or other computers. The computer that a server program runs in is also frequently referred to as a server. That machine may be a dedicated server or used for other purposes as well.

In the client/server programming model, a server program awaits and fulfills requests from client programs, which may be running in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a *server* of requests from other programs.

Servers are often categorized in terms of their purpose. A Web server, for example, is a computer program that serves requested HTML pages or files. A Web *client* is the requesting program associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



Here are a few types of servers, among a great number of other possibilities:

An application server is a program in a computer in a distributed network that provides the business logic for an application program.

A proxy server is software that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service.

A mail server is an application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

A virtual server is a program running on a shared server that is configured in such a way that it seems to each user that they have complete control of a server.

A blade server is a server chassis housing multiple thin, modular electronic circuit boards, known as server blades. Each blade is a server in its own right, often dedicated to a single application.

A file server is a computer responsible for the central storage and management of data files so that other computers on the same network can access them.

A policy server is a security component of a policy-based network that provides authorization services and facilitates tracking and control of files.

An Introduction to FTP

What Is FTP?

FTP stands for "file transfer protocol." FTP powers one of the fundamental Internet functions and is the prescribed method for the transfer of files between computers. It is also the easiest and most secure way to exchange files over the Internet.

An FTP address looks a lot like an HTTP or web site address except it uses the prefix ftp:// instead of http://.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

What are some common uses of FTP?

The most common use of FTP is to download files. FTP is vital to the MP3 music sharing, most online auctions and game enthusiasts. The ability to transfer files quickly and reliably is essential for everyone creating and maintaining a web page.

How can I use FTP?

- Most web hosting services provide FTP access to their customers to allow them to upload the contents of their web sites.
- Companies often have FTP servers that allow users to send and receive files.
- Most universities have FTP servers that allow their students to download course materials and upload assignments for submission.
- Use FTP to transfer files among users, especially if the files are too large to attach to an email.
- Use FTP to browse through a collection of downloadable files on a public software archive.

What is an FTP Server?

Typically, a computer with an FTP address is dedicated to receive an FTP connection. A computer dedicated to receiving an FTP connection is referred to as an FTP server or FTP site.

What do I need to start using FTP?

You need two things to begin using FTP:

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

1. An FTP client application and

2. An FTP server.

Where can I get an FTP Client?

Most computer operating systems already come with an FTP client; however, it is not user-friendly. Start up a command prompt window, type "ftp" and then press “enter.” Chances are you will be greeted by an "ftp>" prompt. Unless you are well-versed with using command lines and enjoy typing, there are much easier ways to FTP.

FTP Explorer is an FTP client application. It is designed to make FTP simple and hassle-free. Most people agree it is much easier to use than a command line FTP client. Download FTP Explorer here.

Where can I get an FTP server?

In many cases, the FTP server you want to connect to is already out there somewhere, waiting for you to establish a connection to it.

If, however, you want to set up your own FTP server so other users can connect to your server and transfer files, you have a few options:

- Many operating systems come with an FTP server, but it is often disabled for security reasons. Windows XP Pro includes an FTP server as part of Internet Information Server, but it is disabled by default. Most Unix and Linux systems include FTP "daemons" as part of their distributions. Check with the vendor of your operating system to determine if you already have FTP server software.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

- There are also a variety of third party FTP servers available.

Control Connection -- the conversation channel

The protocol can be thought of as interactive, because clients and servers actually have a conversation where they authenticate themselves and negotiate file transfers. In addition, the protocol specifies that the client and server do not exchange data on the conversation channel. Instead, clients and servers negotiate how to send data files on separate connections, with one connection for each data transfer. Note that a directory listing is considered a file transfer.

To illustrate, we'll just present (an admittedly contrived) example of how the FTP would work between human beings rather than computer systems. For our example, we'll assume we have a client, Carl **Clinton**, who wishes to transfer files from Acme Mail **Service** that manages his post office box. Below is a transcript of a phone call between Carl Clinton and Acme Mail Service.

Clinton: (Dials the phone number for the mail service)

Service: "Hello, this is the Acme Mail Service. How may I help you today?"

Clinton: "Hello, this is Carl Clinton. I would like to access mailbox number MB1234."

Service: "OK, Mr. Clinton, I need to verify that you may access mailbox MB1234. What is your password?"

Clinton: "My password is QXJ4Z2AF."

Service: "Thank you Mr. Clinton, you may proceed."

Clinton: "For now, I'm only interested in looking at the bills and invoices, so look at the folder marked "bills" in my mailbox."

Service: "OK."

Clinton: "Please prepare to have your assistant call my secretary at +1 402 555 1234."

Service: "OK."

Clinton: "Now call my secretary and tell him the names of all the items in the bills folder of my mailbox. Tell me when you have finished."

Server: "My assistant is calling your secretary now."

Server: "My assistant has sent the names of the items."

Clinton: (Receives the list from his secretary and notices a bill from Yoyodyne Systems.)

"Please prepare to have your assistant send to my fax machine +1 402 555 7777."

Service: "OK."

Clinton: "Now fax a copy of the bill from Yoyodyne Systems."

Server: "My assistant is calling your fax machine now."

Server: "My assistant has finished faxing the item."

Clinton: "Thank you, that is all. Good bye."

Server: "Goodbye."

Now let's look at how this same conversation would appear between computer systems communicating with the FTP protocol over a TCP/IP connection.

Client: Connects to the FTP service at port 21 on the IP address 172.16.62.36.

Server: 220 Hello, this is the Acme Mail Service.

Client: USER MB1234

Server: 331 Password required to access user account MB1234.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Client:	PASS QXJ4Z2AF	Note that this password is not encrypted. The FTP is susceptible to eavesdropping!
Server:	230 Logged in.	
Client:	CWD Bills	Change directory to "Bills."
Server:	250 "/home/MB1234/Bills" is new working directory.	
Client:	PORT 192,168,1,2,7,138	The client wants the server to send to port number 1930 on IP address 192.168.1.2. In this case, 192.168.1.2 is the IP address of the client machine.
Server:	200 PORT command successful.	
Client:	LIST	Send the list of files in "Bills."
Server:	150 Opening ASCII mode data connection for /bin/ls.	The server now connects out from its port 20 on 172.16.62.36 to port 1930 on 192.168.1.2.
Server:	226 Listing completed.	That succeeded, so the data is now sent over the established data connection.
Client:	PORT 192,168,1,2,7,139	The client wants the server to send to port number 1931 on the client machine.
Server:	200 PORT command successful.	
Client:	RETR Yoyodyne.TXT	Download "Yoyodyne.TXT."
Server:	150 Opening ASCII mode data connection for Yoyodyne.TXT.	The server now connects out from its port 20 on 172.16.62.36 to port 1931 on 192.168.1.2.

Server: `226 Transfer completed.`

That succeeded, so the data is now sent over the established data connection.

Client: `QUIT`

Server: `221 Goodbye.`

When using FTP, users use FTP client programs rather than directly communicating with the FTP server. Here's our same example using the stock "`ftp`" program which is usually installed as `/usr/bin/ftp` on UNIX systems (and `FTP.EXE` on Windows). The items the user types are in **bold**.

```
ksh$ /usr/bin/ftp
ftp> open ftp.acmemail.example.com
Connected to ftp.acmemail.example.com (172.16.62.36).
220 Hello, this is the Acme Mail Service.
Name (ftp.acmemail.example.com:root): MB1234
331 Password required to access user account MB1234.
Password: QXJ4Z2AF
230 Logged in.
ftp> cd Bills
250 "/home/MB1234/Bills" is new working directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
-rw-r--r--    1 ftpuser  ftpusers     14886 Dec  3 15:22 Acmemail.TXT
-rw-r--r--    1 ftpuser  ftpusers    317000 Dec  4 17:40 Yoyodyne.TXT
226 Listing completed.
ftp> get Yoyodyne.TXT
local: Yoyodyne.TXT remote: Yoyodyne.TXT
200 PORT command successful.
150 Opening ASCII mode data connection for Yoyodyne.TXT.
226 Transfer completed.
317000 bytes received in 0.0262 secs (1.2e+04 Kbytes/sec)
ftp> quit
221 Goodbye.
```

As you can see, FTP is designed to allow users to browse the filesystem much like you would with a regular UNIX login shell or MS-DOS command prompt. This differs from other protocols that are transactional (i.e. HTTP), where a connection is established, clients issue a single message to a server that replies with a single reply, and the connection is closed. On the other hand, client programs can be constructed to simulate a transactional environment if they know in advance what they need to do. In effect, FTP is a stateful sequence of one or more transactions.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Command primitives, result codes and textual responses

The client is always responsible for initiating requests. These requests are issued with FTP command primitives, which are typically 3 or 4 characters each. For example, the command primitive to change the working directory is `CWD`.

The server replies are specially formatted to contain a 3-digit result code first, followed by a space character, followed by descriptive text (there is also a format for multi-line responses). The protocol specifies that clients must only rely upon the numeric result code, since the descriptive text is allowed to vary (with a few exceptions). In practice, the result text is often helpful for debugging, but is generally no longer useful for end users.

How do I publish my web site to an FTP server?

To upload files, you must first be connected to an FTP server using the appropriate login and password (most servers do NOT allow anonymous users to upload). Contact the administrator of the FTP server to determine the appropriate login information.
Once connected, you must navigate to the proper folder. You may not have rights to upload into every folder to which you have access. Contact the administrator of the FTP server to determine the folder that you should be uploading to.

Once connected and in the proper folder, you have several options for uploading at your disposal:

A. Upload Menu Option

1. Choose the FILE | UPLOAD menu option
2. Select file(s) to upload from the Upload dialog box

B. Upload Toolbar Button
1. Select the Upload toolbar button
2. Select file(s) to upload from the Upload dialog box

C. Drag and Drop
1. Open a windows explorer view, such as My Computer
2. Navigate to the files that you wish to upload
3. Drag and drop the files onto the right pane of FTP Explorer

NOTE: Drag and drop is currently the only way to upload entire folders.

What is Anonymous FTP?

Many FTP servers allow "anonymous" access. Usually these servers will only allow you to download anonymously and will prohibit uploading.

To connect with an anonymous FTP server:
1. Use "anonymous" for the login name
2. Use your email address for the password

What is PASV mode?

An FTP session generally consists of two connections between the client and the server.

The first connection is known as the "control connection" and is used by the client to send commands to the server and receive responses from the server. This connection is usually made via TCP port 21.

The second connection is known as the "data connection" and is used to transfer the actual data (such as files or directory listings) between the client and server.

The client establishes a control connection to the server and logs in. Subsequently, client submits a transfer command (such as RETR, STOR, or LIST), that requires a data connection to be established. Normally, the client will specify a TCP port that the server should connect to, and the server will then initiate a connection back to the client on that port and begin transferring the data. Many modern firewalls and routers will block this connection by default, as it is generally a security risk for a client to accept connections. This is where PASV mode is useful.

When PASV mode is used, the client sends a command to the server informing the server of its intent to use PASV mode, and the server responds with a TCP port. The client then initiates a connection to the server on this port and the server begins transferring data.

In general, it is usually better to use PASV mode.

What FTP Terminology Should I Know?

Anonymous FTP: Transfers files from the public portion of an FTP server. "Anonymous" means that you don't have to have an account on the server. In most cases, use anonymous as your user name and your email address as your password.

Archive: An FTP site that contains a selection of files for download.

Download: Also called "Get". Copy a file from an FTP site to another computer. If you're merely downloading shared files an anonymous account is usually sufficient. However, if you're downloading Web pages for update, a password and user privileges is usually required.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

FTP site: A Web site that stores files for download. You can access the sites with a Web browser by typing in the address. All FTP site addresses begin with ftp:// (instead of http://).

Upload: Also called "Put". Place files on an FTP server. Upload privileges are usually password protected to keep unauthorized users from placing files that could contain viruses or other malicious code on the server.

An Introduction to FTP

What Is DNS?

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality of the Internet, that has been in use since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their allocated name space to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid a single large central database.

The Domain Name System also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite.

Shamsunnabi Taqib

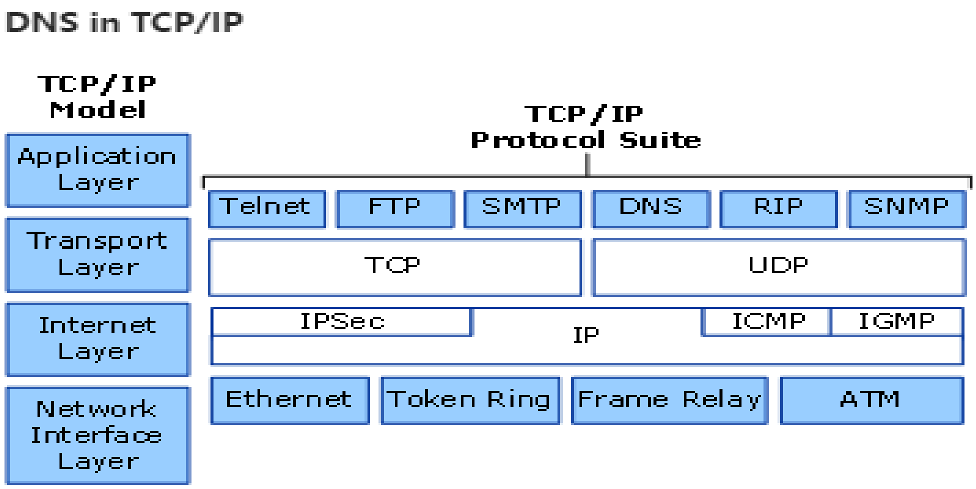
DIFFERENT TYPE OF SERVER

Historically, other directory services preceding DNS were not scalable to large or global directories as they were originally based on text files, prominently the HOSTS.TXT resolver.

Domain Name System (DNS) is one of the industry-standard suite of protocols that comprise TCP/IP. Microsoft Windows Server 2003. DNS is implemented using two software components: the DNS server and the DNS client (or resolver). Both components are run as background service applications.

Network resources are identified by numeric IP addresses, but these IP addresses are difficult for network users to remember. The DNS database contains records that map user-friendly alphanumeric names for network resources to the IP address used by those resources for communication. In this way, DNS acts as a mnemonic device, making network resources easier to remember for network users.

The Windows Server 2003 DNS Server and Client services use the DNS protocol that is included in the TCP/IP protocol suite. DNS is part of the application layer of the TCP/IP reference model.



By default, Windows Server 2003 DNS is used for all name resolution in a Windows Server 2003 network. In the most typical scenario, when a

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Windows Server 2003 network user specifies the name of a network host or an internet DNS domain name, the DNS Client service running on the Windows Server 2003 computer of the user contacts a DNS server to resolve the name to an IP address.

Technologies That Use DNS

DNS and Active Directory

Windows Server 2003 Active Directory directory service uses DNS as its domain controller location mechanism. When any of the principal Active Directory operations is performed, such as authentication, updating, or searching, Windows Server 2003 computers use DNS to locate Active Directory domain controllers and these domain controllers use DNS to locate each other. For example, when a network user with an Active Directory user account logs in to an Active Directory domain, the user's computer uses DNS to locate a domain controller for the Active Directory domain to which the user wants to log in. For more information about integrating DNS and Active Directory, see "How DNS Works" in this collection.

DNS and WINS

The earlier method of name resolution for a Windows network was Windows Internet Name Service (WINS). DNS is different than WINS in that DNS is a hierarchical namespace and WINS is a flat namespace. Down-level clients and applications that rely on NetBIOS names continue to use WINS for name resolution. Since Windows Server 2003 DNS is WINS-aware, a combination of both DNS and WINS can be used in a mixed environment to achieve maximum efficiency in locating various network services and resources. For more information about using DNS in a mixed environment, see "How DNS Works" in this collection.

DNS and DHCP

For Windows Server 2003 DNS, the DHCP service provides default support to register and update information for legacy DHCP clients in DNS zones. Legacy clients typically include other Microsoft TCP/IP client computers that were released prior to Windows 2000. The Windows Server 2003 DNS-DHCP integration enables a DHCP client that is unable to dynamically update DNS resource records directly to have this information updated in DNS forward and reverse lookup zones by the DHCP server.

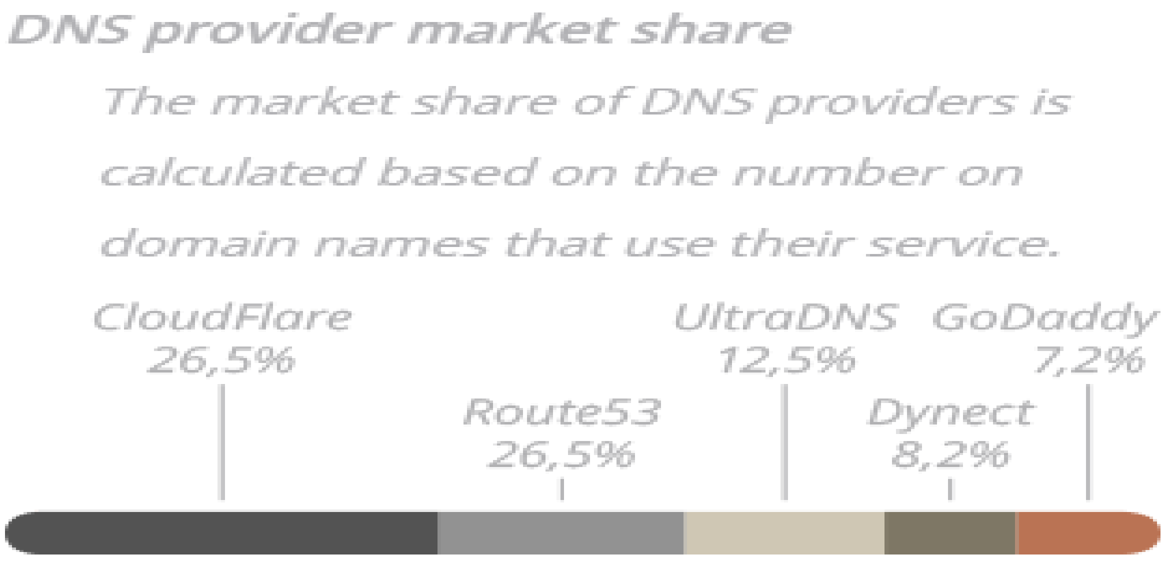
How DNS Works

In its simplest form, the DNS is a database that maintains the names of websites, such as webhostinggeeks.com, and links them to particular IP addresses that consist of a number pattern (i.e. 162.247.79.100). However, this can be understood as its simplest task. Linking addresses to names is the basic function of DNS, as is it used for a variety of services, apart from host-to-address mapping.

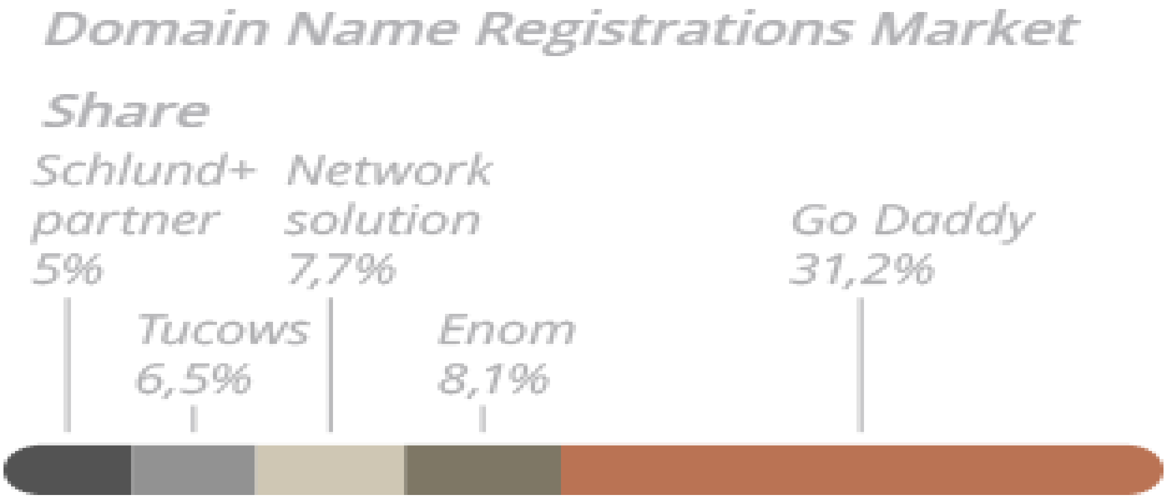
Some of the major functions of DNS include locating IP addresses to specific site names, and then storing this data. This process is also known as “maintaining records”. A second function is to distribute the DNS over a vast network of connections, and a DNS can also store a vast library of records. For many experts, DNS is the term used to define a database and, most importantly, a database that can be easily shared. This is because each server holds only a minor portion of the host name to IP address mapping details.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

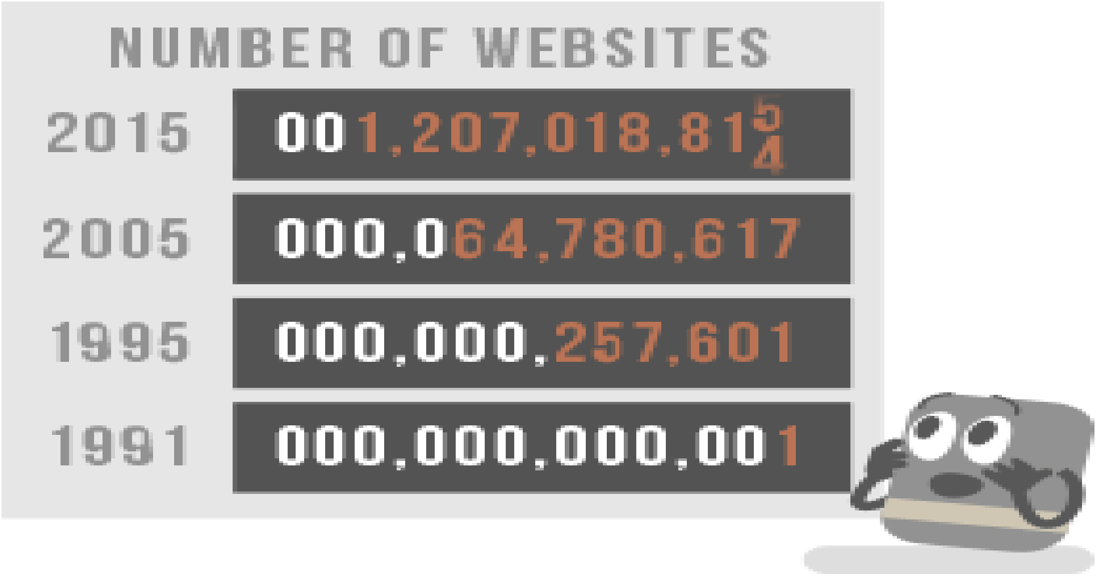


DNS servers are configured with a special record that informs where the DNS server is located. Due to this process, each DNS server holds a small part of the host to IP mapping address. This collection of host to IP address mapping is also called the namespace. When looking up a name in the DNS system, the user must first check the high-level database, which tells the client how to check the DNS server host. As a next step in the process, it specifies queries the client can address through the hostname given by the DNS server. The process continues until the user finds the correct server that hosts the DNS required.



Additionally, finding the correct DNS and identifying the correct mapping of records stored by the database permits the DNS to maintain records. These record types are useful for several other purposes and may help other applications. For example, the record of the Mail Exchanger provides mail servers with the data needed to pass on sender-to-recipient emails. Another important record used by Microsoft Active Directory is to locate network services accurately.

Although it may seem as if DNS is complicated, its importance lies in the fact that other processes solely rely on it to function.



World Wide Web

The WWW relies on DNS for human-friendly navigation. Users can easily access a website by entering the IP address of a particular site or web browser. However, remembering several numbers is not the best way to approach the site. Therefore, it is much easier to remember the DNS name for a website that will present user-friendly names, such as webhostinggeeks.com.

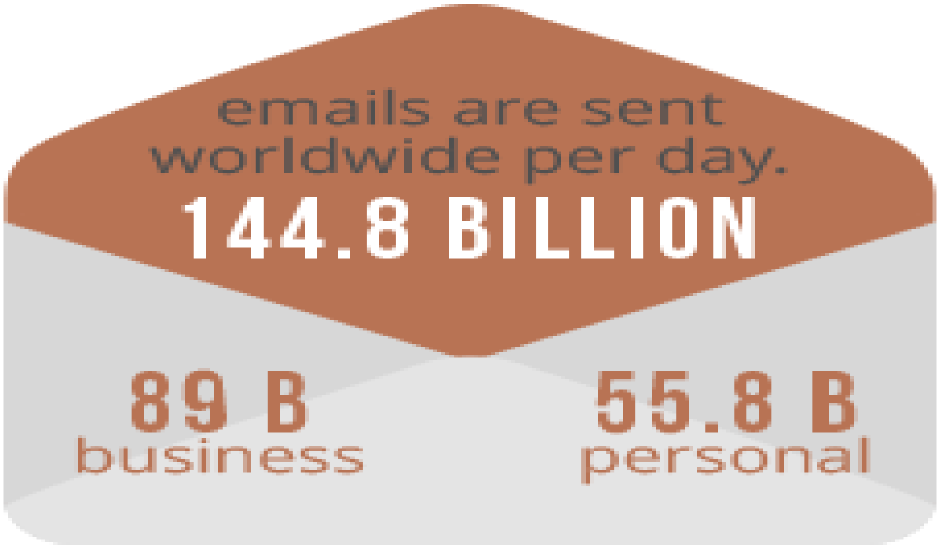
Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

E-Mails

E-mail is the main reason the DNS was developed and is one of the most popular functions of the DNS. Through the web, DNS links the names to IP addresses for various sites, although email servers need a more advanced record than what is required of basic host names. For instance, when an email is sent by a user through Outlook or Gmail, it can either be sent to the recipient at their domain or to another email server that is providing a similar service. If the email specifies an outgoing mail server which is not the target domain, then the user is using a reliable process.

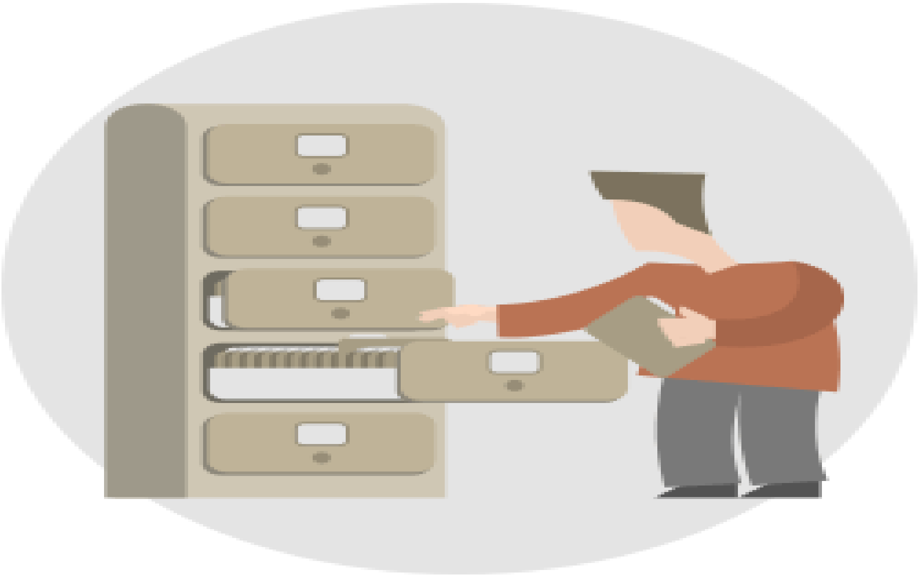
An email address contains two portions: a host and a recipient. For instance, in the address mailbox@webhostinggeeks.com, 'mailbox' is the recipient and the mail transfer agent is responsible for ensuring that the message reaches the recipient. In actuality, any application that requires the Internet connects two or more hosts, which then shares information or communicates using DNS services.



Other uses of DNS servers include the more recent upgrade in 2008 that supports a zone type called the Stub Zone. This is a zone that contains features and records of resources that are used to identify contained DNS servers. The zone operates in such a way that lets the parent zone be aware of a forceful DNS server for its child zone. Another key feature of the DNS is that it provides integration with other Microsoft networking services. These features include connection with services, such as Windows Internet Name Service and Dynamic Host Configuration Protocol. With its improved ease of administration, DNS now allows a graphical user interface to manage DNS server services, in addition to other applications.

Structure

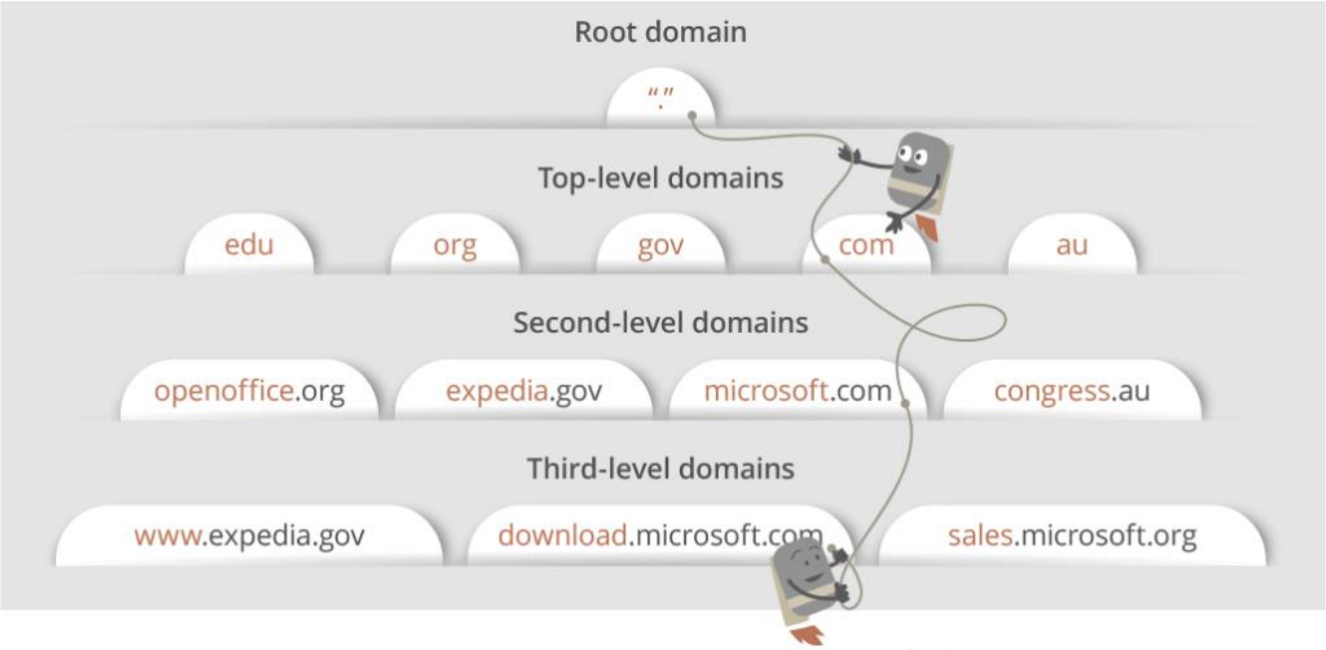
The DNS architecture is defined by a **hierarchical distributed database and a set of protocols**. It is a mechanism for updating, replicating information and a schema of the database. DNS was conceptualized in the Internet's early days when it was just a minor network established by the United States Department of Defense. The various host names in DNS were administered by a single host that was located in the central server, and anyone that required the host name downloaded this file. On the other hand, as the Internet grew, the size of this file expanded with the traffic it generated. The need for a new host soon rose, which further featured support for various data types.



For the DNS, the host name is stored in a database that can be distributed among multiple servers. This will then decrease the pressure on a single server and will also allow access to the database without any location constraints. DNS is said to support hierarchical names and allows the use of various data, in addition to mapping. Since the data is shared and the size of the host is unlimited, the performance of the DNS does not degrade when more servers are added.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



The names in the DNS form a hierarchical tree structure; this is called the domain namespace. The domain name lies at the top of the hierarchy. These names are of individual labels, which are subsequently divided through dots. A fully qualified domain name is unique enough to be easily identified by the host's position in the DNS's structure. This can be done through the hierarchical tree or by specifying the dots that state the path from the host to the root. The namespace is dependent on the concept of a tree that consists of named domains. Each level, branch or leaf can represent a different stage of the hierarchy. Adding on a branch is a stage in which more than one name is used to identify the collection of named resources. A leaf represents a single name that is used only once to mention a specific resource.

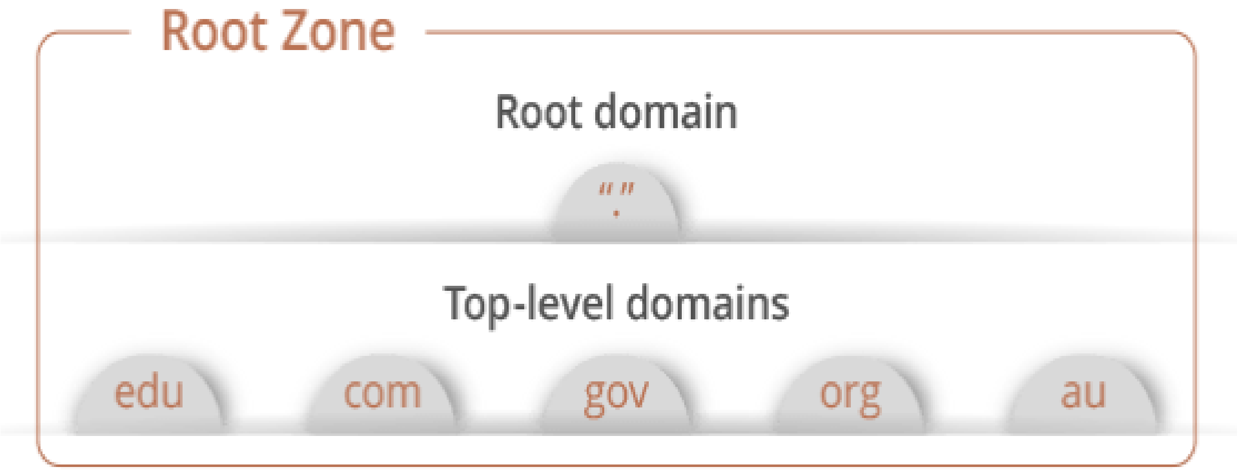
Any name that is used in the tree is technically a domain. However, experts have found that there are five main levels for domains. For example, a DNS domain name assigned to Microsoft is a second-level domain. This occurs due to the name having two parts that indicate whether they are located near the root or the top of the tree. Several DNS names have two or more labels, each of which indicate an additional stage in the tree.

Internet domain names are managed by a name registration authority on the Internet, which is responsible for maintaining the profile of top-level domains (TLDs) that are allocated by countries and regions. These follow international compliant standards and often exist in abbreviations reserved for organizations, as well as for countries.

A DNS database can be divided into several zones, and each zone carries a portion of the DNS database. These contain the resource records of the owner names that are part of the namespace. Zone files are part of the DNS servers, and these can be configured to host zero or multiple zones. Characteristically, each zone is then part of a particular domain name, which is referred to as its root. This zone contains all the information about the names and ends in the zone's domain root name. A name within the zone can also be associated with different zones, which are hosted by a different DNS server. This delegation is a process of giving the responsibility of the DNS namespace to a DNS server owned by a separate entity. This can be another organization or working group.

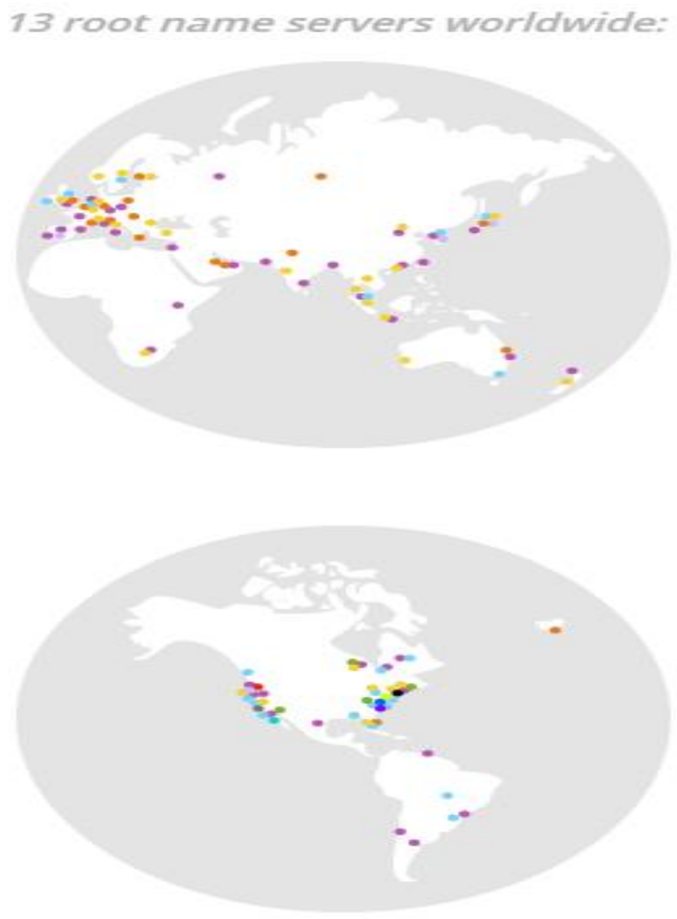
Zones and root name servers

The root zone is a global list of top domain levels. The information that root zones contain can vary. These include two letter codes, which represent each country, e.g. .se to symbolize Sweden. In addition to this, internationalized top-level domains are incorporated, which indicates that countries are coded and grouped together. Individually, each of these top-level domains contains its own root zone in the numeric addresses of name servers. These aid with the top-level domain's subjects, and the root servers respond to reports when requested about a top-level domain.



Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



Collectively, each of those top-level domains, contains its own root zone in the numeric addresses of name servers. These aid with the top level domain’s subjects, and the root servers respond to reports when requested about a top level domain.

Some organizations that operate these root servers are US Army Research Lab, Internet Systems Consortium, NASA AMES Research Center, US Department of Defense, University of Maryland, Cogent, University of Southern California, Netnod, RIPE, Verisign, ICANN, and WIDE. Currently, these are the top 12 organizations using the root servers, and some of these firms have been using the root servers since the invention of the Domain Name System.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

- ● *Verisign*
- ● *USC-ISI*
- ● *Cogent Communications*
- ● *University of Maryland*
- ● *NASA*
- ● *Internet Systems Consortium*
- ● *Defense Information Systems Agency*
- ● *U.S. Army Research Lab*
- ● *Netnod*
- ● *Verisign*
- ● *RIPE NCC*
- ● *ICANN*
- ● *WIDE Project*

In other words, there are over three hundred root servers that have been distributed globally and onto the six most populated organizations. Moreover, each one can be reached through thirteen different IP addresses. Each organization can have one or two IP addresses, such as Verisign, which has two. In addition, any DNS query sent through these addresses will get a fast response. The number of root servers has increased significantly since the start of the last decade, when there were only 13 worldwide. The use of anycast addressing permits the actual number of root server instances to be much larger, and is 504 as of January 2016.

The root name server is a name server for the root zone of the DNS. It is known to answer requests directly through the root zone, as well as to record other requests through several authoritative name servers by assigning proper top-level domains, also referred to as TLD. These root servers are essential, as they are used primarily to solve or interpret human decipherable host terms into IP addresses. This is key for communicating between different Internet hosts. The translation is done through a resolver, which answers users’ queries directly. Likewise, it tries to identify each and every command word by word.

UDP (User Datagram Protocol) is the combination of several protocols and certain limits in the DNS. The practical size of non-fragmented UDP led to the conclusion that the number of root servers can be limited to thirteen server addresses. However, it should be noted that if any cast is used, then the root server number tends to be higher than predicted.

gTLD and ccTLD

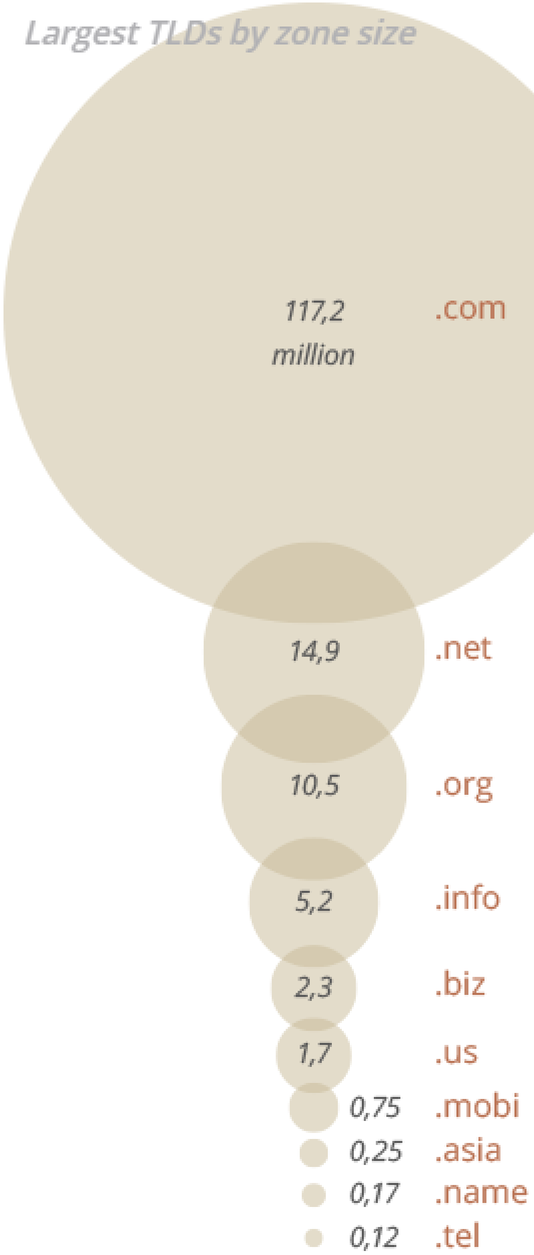
TLD (top-level domain) can be seen whenever one writes the domain name, the web address, or the URL. To be exact, wherever your email address ends up is where the top-level domain resides. TLD is commonly known as the last part of the name of any website, domain, or email address. Some examples of TLD include .com, .biz, .org, .net, and so on.

These TLDs can be categorized into two basic forms, mainly the gTLDs and the ccTLDs. TLDs are taken care of by the Internet Assigned Number Authority, popularly known as IANA. This is the administration that is responsible for the root of the Domain Name System, or DNS. The IANA is being operated by the ICANN, which stands for the Internet Corporation for Assigned Names and Numbers. It should be considered that the second part of the TLD is the dot, which helps us separate the TLDs. This is known as the second level domain and is supposed to be registered with a registrar.

The generic top-level domains, or gTLDs, as the name suggests, are generic. Hence, they are not for any specific country. These can be used by anyone who is surfing the Internet. Some of the top-level domains include .com, .org, .net, .gov, and .mil. These are generic top-level domains that can be expanded to 22 gTLDs. Therefore, gTLDs tend to be more restricted, dictating that only a specific group can register and access them, after which they will be eligible. However, they are never bound to a specific country.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



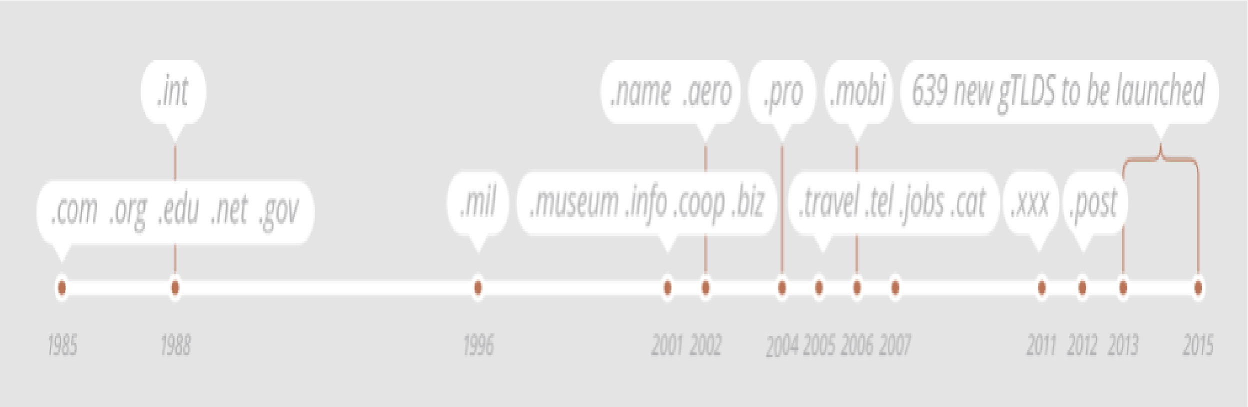
On the other hand, ccTLDs denote country code top-level domains. These are more commonly known as the two-letter TLDs, which means they are allotted to countries established customarily on the ISOC 3166 list of country codes.

The Original 22 gTLDs

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Some countries have opted to function their ccTLD solely for domains that will be used inside their country or within its geographic territory. It should be considered that some countries do not permit individuals to record the second-level domains under the TLD. However, as an alternative, they permit individuals to register third-level domains under one of the wide range of different second-level domains available. Some countries, such as the United Kingdom, are required to register their domains of .uk, such as .co.uk or .org.uk. This will basically change the generic top-level domain to a country code top-level domain.

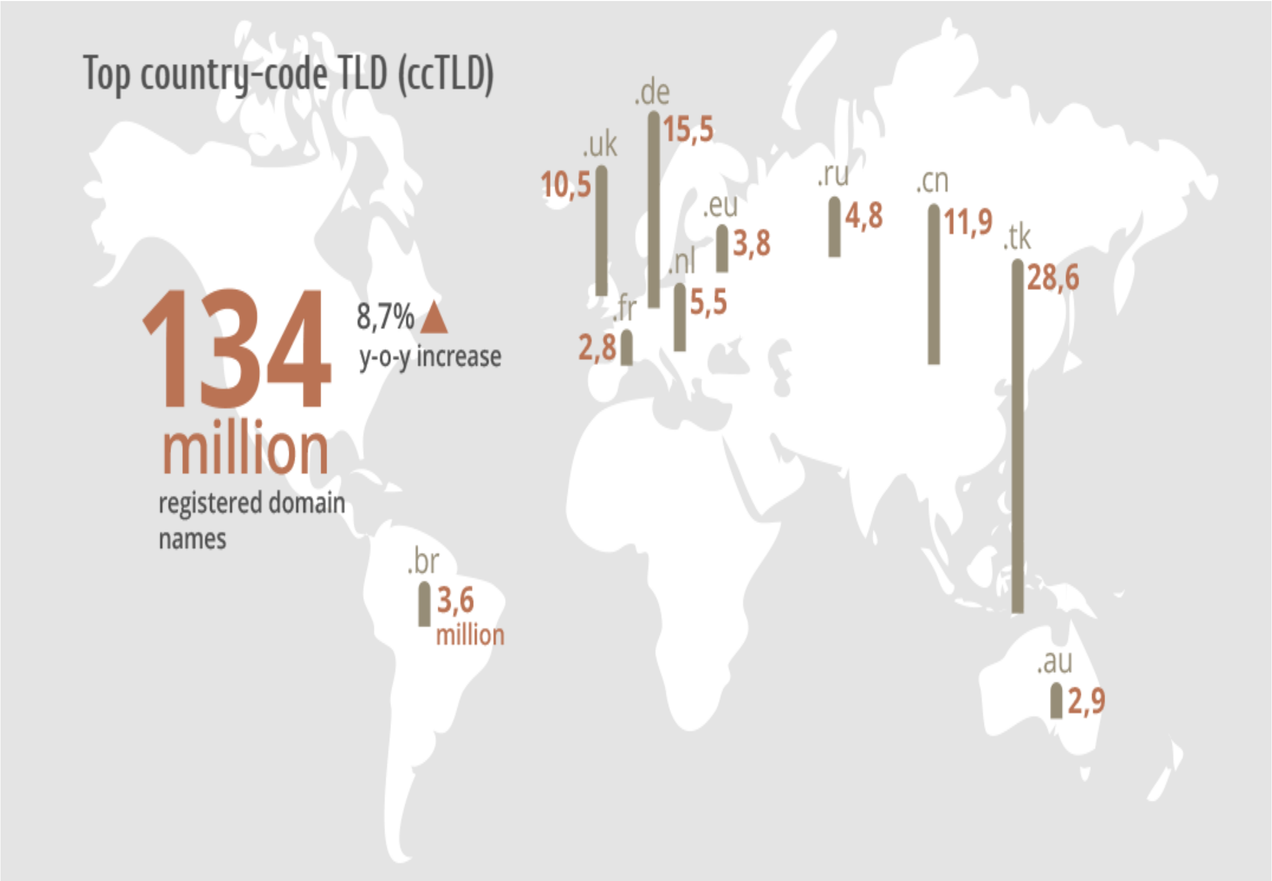


Top country-code TLD (ccTLD)

The country code top-level domain is specific to certain countries. Hence, each domain is based on the country extension. Although some have restrictions on who can register, most do not have this formality. For example, .tv, .me, .cc, and .ws are some of the extensions that are said to be open for registration by the common public. Some of these extensions have also been repurposed for general usage.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



IIS (Internet Information Services)

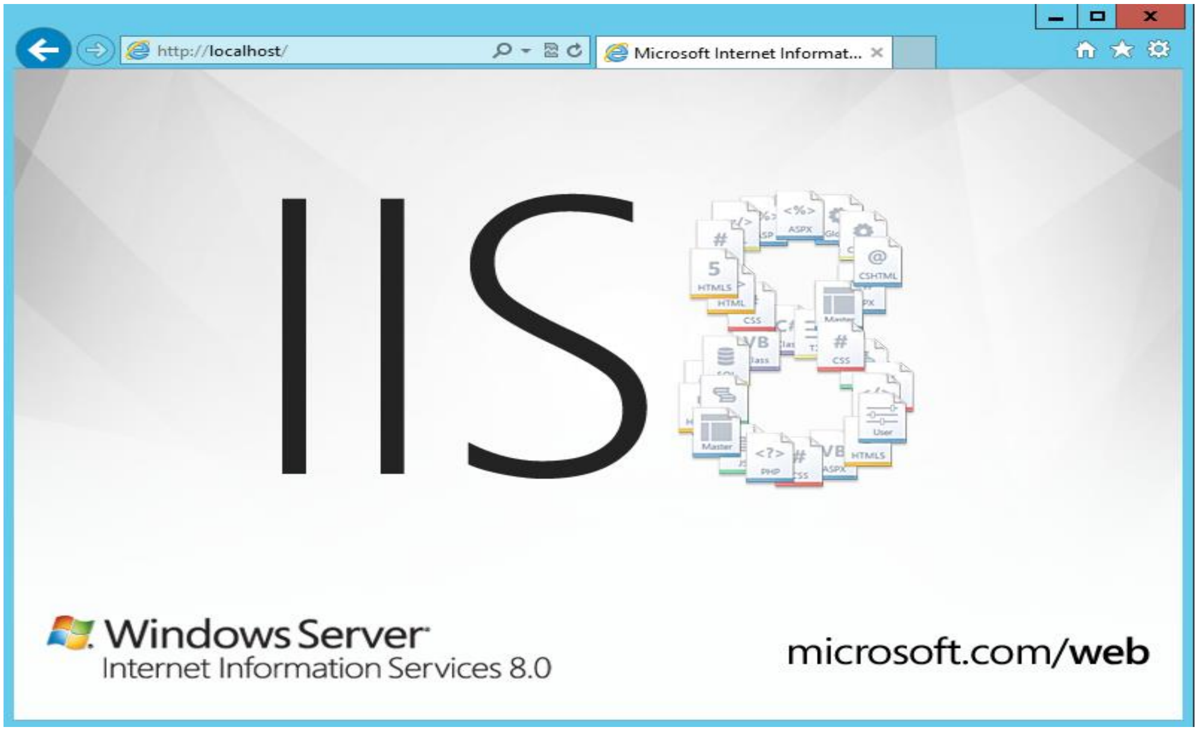
Internet Information Services (IIS) is a flexible, general-purpose web server from Microsoft that runs on Windows systems to serve requested HTML pages or files.

An IIS web server accepts requests from remote client computers and returns the appropriate response. This basic functionality allows web servers to share and deliver information across local area networks, such as corporate intranets, and wide area networks, such as the internet.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

A web server can deliver information to users in several forms, such as static webpages coded in HTML; through file exchanges as downloads and uploads; and text documents, image files and more.


http://localhost/
Microsoft Internet Informat...
IIS 8
Windows Server
Internet Information Services 8.0
microsoft.com/web

Web servers provide portals

Modern web servers can provide far more functionality for a business and its users. Web servers are often used as portals for sophisticated, highly interactive, web-based applications that tie enterprise middleware and back-end applications together to create enterprise-class systems. For example, Amazon Web Services allows users to administer public cloud resources through a web-based portal. Meanwhile, streaming media services, such as Spotify for music and Netflix for movies, deliver real-time streaming content through web servers.

How IIS works

IIS works through a variety of standard languages and protocols. HTML is used to create elements such as text, buttons, image placements, direct interactions/behaviors and hyperlinks. The Hypertext Transfer Protocol (HTTP) is the basic communication protocol used to exchange information between web servers and users. HTTPS -- HTTP over Secure Sockets Layer (SSL) -- uses Transport Layer Security or SSL to encrypt the communication for added data security. The File Transfer Protocol, or its secure variant, FTPS, can transfer files.

Additional supported protocols include the Simple Mail Transfer Protocol, to send and receive email, and the Network News Transfer Protocol, to deliver articles on Usenet.

IIS works with ASP.NET Core

The ASP.NET Core framework is the latest generation of Active Server Page (ASP), a server-side script engine that produces interactive webpages. A request comes in to the IIS server from the web, which sends the request to the ASP.NET Core application, which processes the request and sends its response back to the IIS server and the client who originated the request. Examples of applications written on ASP.NET Core include blog platforms and content management systems.

Developers can produce IIS websites with a number of tools, including Web Distributed Authoring and Versioning, which can create and publish web content. Developers can also use integrated development tools, such as Microsoft Visual Studio.

Versions of IIS

IIS has evolved along with Microsoft Windows. Early versions of IIS arrived with Windows NT. IIS 1.0 appeared with Windows NT 3.51, and evolved through IIS 4.0 with Windows NT 4.0. IIS 5.0 shipped with Windows 2000. Microsoft added IIS 6.0 to Windows Server 2003. IIS 7.0 offered a major redesign with Windows Server 2008 (IIS 7.5 is in Windows Server 2008 R2).

IIS 8.0 came with Windows Server 2012 (Windows Server 2012 R2 uses IIS 8.5). And IIS 10 arrived with Windows Server 2016 and Windows 10.

With each iteration of IIS, Microsoft has added new features and updated existing functionality. For example, IIS 3.0 added ASP for dynamic scripting; IIS 6.0 added support for IPv6 and improved security and reliability; and IIS 8.0 brought multicore scaling on non-uniform memory access hardware, centralized SSL certificate support and Server Name Indication.

Features in IIS 10

IIS 10 also adds a number of new features and functionality.

IIS 10 adds support for the HTTP/2 protocol, to offer more efficient resource use and lower latency compared to HTTP 1.1. IIS 10 works on the minimal server deployment model Nano Server under Windows Server 2016, and can run ASP.NET Core, Apache Tomcat and PHP workloads on IIS on the Nano Server.

IIS 10 works in a container and virtual machine, so developers and administrators have more flexibility in deployment choices, as well as the density to accommodate a broad range of web applications.

IIS Express for testing

Microsoft provides a self-contained version of IIS, called IIS Express, for developers to test websites. IIS Express offers all the major capabilities of the full IIS web server, but allows many tasks to be performed without administrative privileges.

Introduction to Apache

If Apache has always seemed like a black box to you, it's time to learn just what's going on behind the scenes!

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Apache is the most popular web server available.

A web server's job is basically to accept requests from clients and send responses to those requests. A web server gets a URL, translates it to a filename (for static requests), and sends that file back over the internet from the local disk, or it translates it to a program name (for dynamic requests), executes it, and then sends the output of that program back over the internet to the requesting party. If for any reason, the web server was not able to process and complete the request, it instead returns an error message. The word, web server, can refer to the machine (computer/hardware) itself, or the software that receives requests and sends out responses.

Apache is the most popular web server (after which comes Microsoft's IIS) available. The reasons behind its popularity, to name a few, are:

1. It is free to download and install.
2. It is open source: the source code is visible to anyone and everyone, which basically enables anyone (who can rise up to the challenge) to adjust the code, optimize it, and fix errors and security holes. People can add new features and write new modules.
3. It suits all needs: Apache can be used for small websites of one or two pages, or huge websites of hundreds and thousands of pages, serving millions of regular visitors each month. It can serve both static and dynamic content.

What is Apache?

Functionality that you don't need or want can easily be removed.

The Apache HTTP server is a software (or program) that runs in the background under an appropriate operating system, which supports multi-tasking, and provides services to other applications that connect to it, such as client web browsers. It was first developed to work with Linux/Unix operating systems, but was later adapted to work under other systems, including Windows and Mac. The Apache binary running under UNIX is called *HTTPd* (short for HTTP daemon), and under win32 is called *Apache.exe*.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Installing Apache on Linux does require a bit of programming skills (though it is not too difficult). Installing it on a Windows platform is straight forward, as you can run it through a graphical user interface.

Apache's original core is fairly basic and contains a limited number of features. Its power rather comes from added functionality introduced through many modules that are written by programmers and can be installed to extend the server's capabilities. To add a new module, all you need to do is install it and restart the Apache server. Functionality that you don't need or want can easily be removed which is actually considered a good practice as it keeps the server small and light, starts faster, consumes less system resources and memory, and makes the server less prone to security holes. The Apache server also supports third party modules, some of which have been added to Apache 2 as permanent features. The Apache server very easily integrates with other open source applications, such as PHP and MySQL, making it even more powerful than it already is

A web server in its simplest form is a computer with special software, and an internet connection that allows it to connect to other devices.

Every device connected to a network has an IP address through which others connect to and communicate with it. This IP address is sort of like a regular address that you need in real life to call or visit any contact of yours. If they didn't have an address, you wouldn't know how to call or reach them. IP addresses serve the exact same purpose. If a device didn't have one, the other machines on the same network wouldn't know how to reach it.

The Apache server offers a number of services that clients might make use of. These services are offered using various protocols through different ports, and include: hypertext transfer protocol (HTTP), typically through port 80, simple mail transfer protocol (SMTP), typically through port 25, domain name service (DNS) for mapping domain names to their corresponding IP addresses, genearlly through port 53, and file transfer protocol (FTP) for uploading and downloading files, usually through port 21.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

How Apache Works

Apache's main role is all about communication over networks, and it uses the TCP/IP protocol (Transmission Control Protocol/Internet Protocol which allows devices with IP addresses within the same network to communicate with one another).

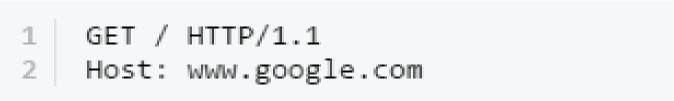
> *The TCP/IP protocol is a set of rules that define how clients make requests and how servers respond, and determine how data is transmitted, delivered, received, and acknowledged.*

The Apache server is set up to run through configuration files, in which directives are added to control its behavior. In its idle state, Apache listens to the IP addresses identified in its config file (HTTPd.conf). Whenever it receives a request, it analyzes the headers, applies the rules specified for it in the Config file, and takes action.

But one server can host many websites, not just one - though, to the outside world, they seem separate from one another. To achieve this, every one of those websites has to be assigned a different name, even if those all map eventually to the same machine. This is accomplished by using what is known as virtual hosts.

Since IP addresses are difficult to remember, we, as visitors to specific sites, usually type in their respective domain names into the URL address box on our browsers. The browser then connects to a DNS server, which translates the domain names to their IP addresses. The browser then takes the returned IP address and connects to it. The browser also sends a *Host* header with the request so that, if the server is hosting multiple sites, it will know which one to serve back.

For example, typing in www.google.com into your browser's address field might send the following request to the server at that IP address:



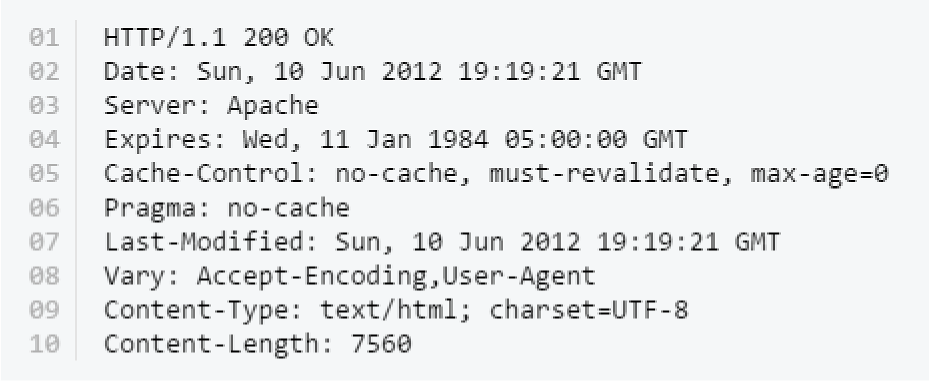
```
GET / HTTP/1.1
Host: www.google.com
```

The first line contains several pieces of information. First, there is the method (in this case it's a GET), the URI, which specifies which page to be retrieved or which program to be run (in this case it's the root directory denoted by the /), and finally there is the HTTP version (which in this case is HTTP 1.1).

HTTP is a request / response stateless protocol.

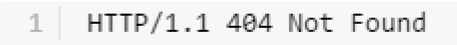
HTTP is a request / response stateless protocol. It's a set of rules that govern communication between a client and the server. The client (usually but not necessarily a web browser) makes a request, the server sends back a response, and communication stops. The server doesn't look forward for more communication as is the case with other protocols that stay at a waiting state after the request is over.

If the request is successful, the server returns a 200 status code (which means that the page is found), response headers, along with the requested data. The response header of an Apache server might look something like the following:



```
HTTP/1.1 200 OK
Date: Sun, 10 Jun 2012 19:19:21 GMT
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Last-Modified: Sun, 10 Jun 2012 19:19:21 GMT
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=UTF-8
Content-Length: 7560
```

The first line in the response header is the status line. It contains the HTTP version and the status code. The date follows next, and then some information about the host server and the retrieved data. The `Content-Type` header lets the client know the type of data retrieved so it knows how to handle it. `Content-Length` lets the client know the size of the response body. If the request didn't go throw, the client would get an error code and message, such as the following response header in case of a page not found error:



```
HTTP/1.1 404 Not Found
```

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

TCP/IP Protocol

TCP/IP is actually two protocols built one on top of the other.

TCP/IP is actually two protocols built one on top of the other. The IP protocol is responsible for getting the transferred data from one point to another. It takes the data to be transferred between the two points, splits it into smaller packets, attaches the source and destination addresses to each packet, and transfers the data.

TCP handles the part that includes establishing the connection between the two parties, making sure the data arrives to its destination, taking care of any data loss and managing data recovery.

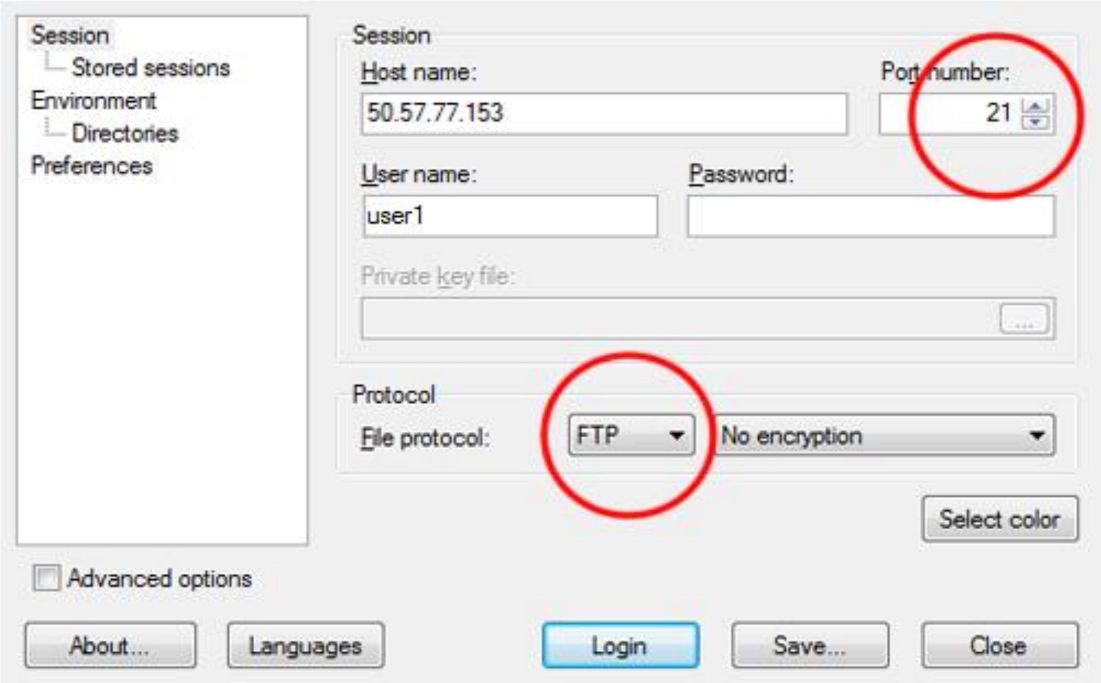
Once a message is received, the destination party sends an *Acknowledged (ACK)* message to the sending host if all goes well, notifying it of data arrival. If something goes wrong, such as the occurrence of a data loss situation, the destination sends a Not Acknowledged (NAK) message instead, notifying the sending host of the problem and informing it of the need to resend the data packet.

As discussed earlier, Apache offers many services, which clients might want to connect to, to make use of or benefit from. TCP manages each service so that it is accessed through a particular port to differentiate between the various services. This way, it ensures that any one given interface (or host) can offer multiple services. So when a client connects to a host, it passes the port number along with the IP address. Browsers use the HTTP protocol which by default uses port 80, so there's no need for further specification.

The following image is a snap shot of my FTP software (WinScp). As you can see, to FTP my server I not only need to provide the IP address (or alternatively type in the domain name), but I also need to specify the port number that my server provides the service through. In the case of FTP, the port number is 21. In the case of SFTP (secure FTP), the port number is 22.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER



Session

Host name: 50.57.77.153

Port number: 21

User name: user1

Password:

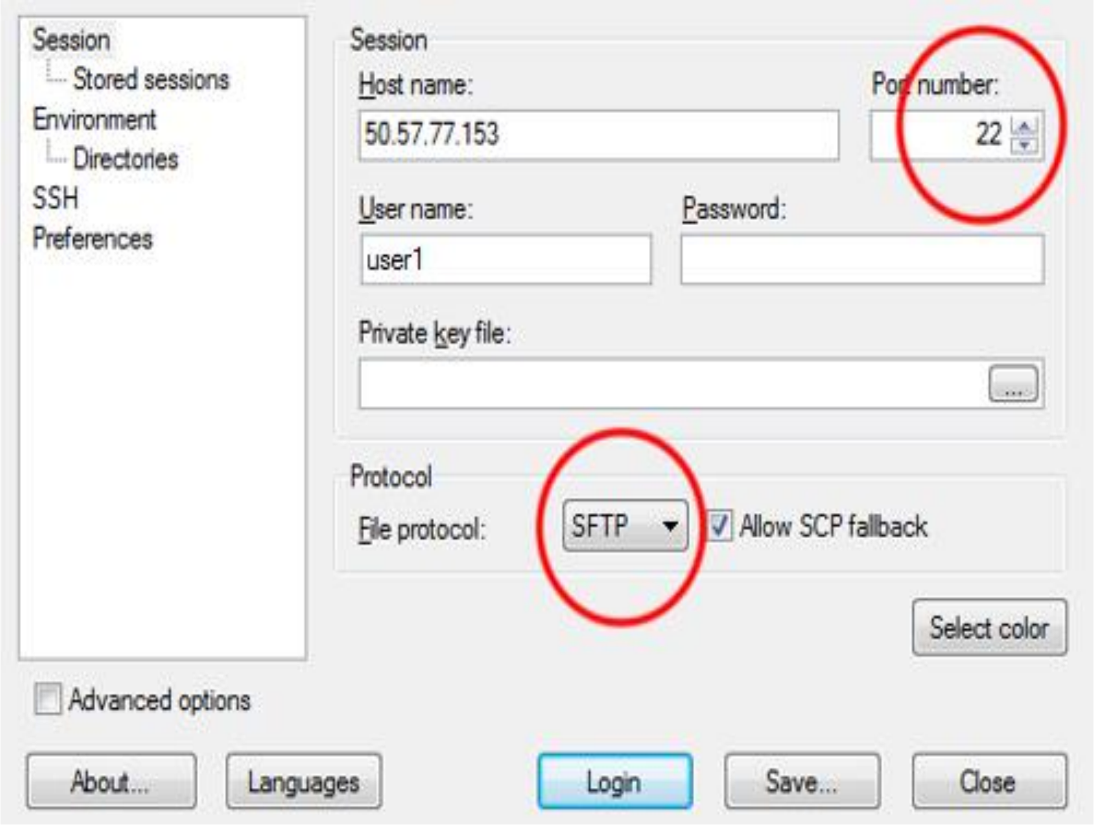
Private key file:

Protocol

File protocol: FTP

No encryption

□ Advanced options



Session

Host name: 50.57.77.153

Port number: 22

User name: user1

Password:

Private key file:

Protocol

File protocol: SFTP

☑ Allow SCP fallback

□ Advanced options

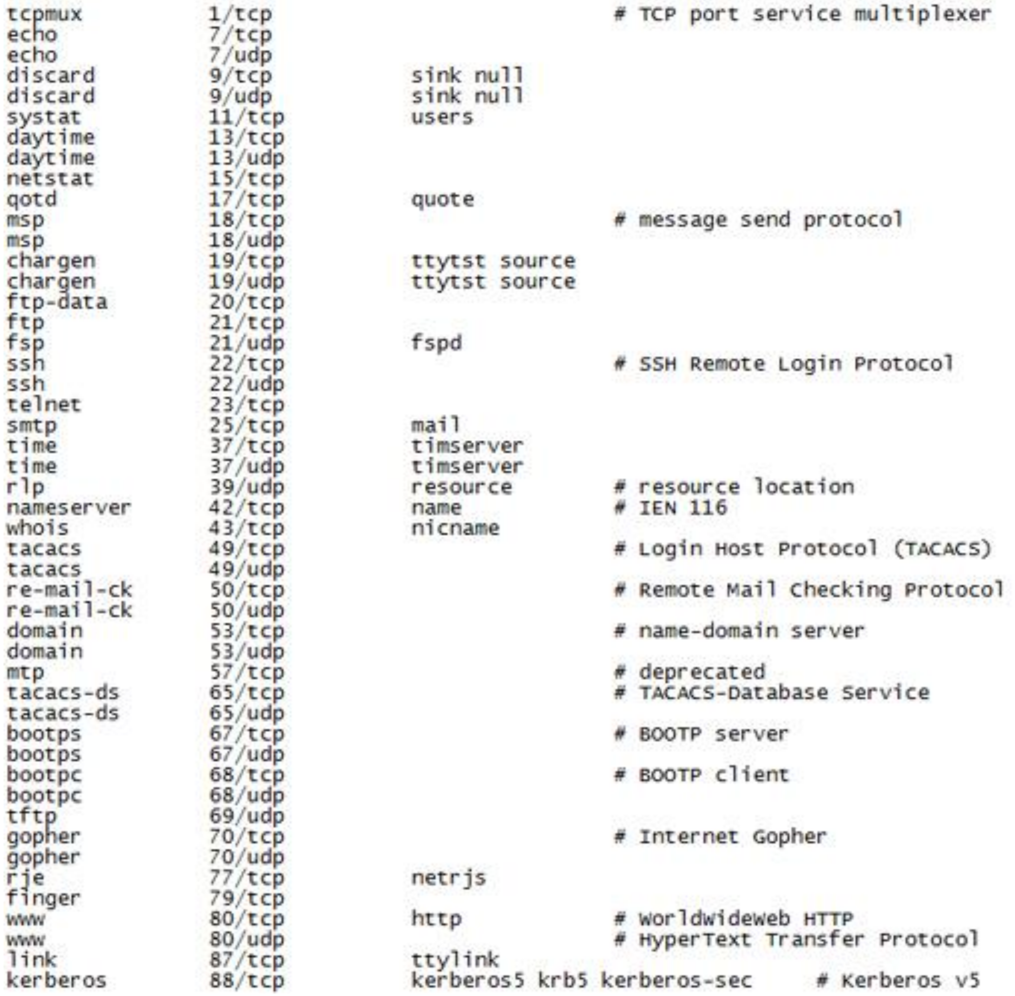
Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Under UNIX, a list of services offered along with their respective port numbers can be found in the file */etc/services*. The following command will display the contents of the file:

```
more /etc/services
```

Below is a screenshot showing a part of the file. As you can see, services are listed in the first column, followed by the port number to be accessed at and the protocol name the service uses.



```
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
domain          53/tcp                          # name-domain server
domain          53/udp
mtp             57/tcp                          # deprecated
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
www             80/udp                          # HyperText Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
```

Under windows the file is called Services, and can be found under C:\WINNT\system32\drivers\etc\

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

Inetd

To preserve system resources, UNIX handles many of its services through the internet daemon.

To preserve system resources, UNIX handles many of its services through the *internet daemon (inetd)*, as opposed to a constantly running daemon. The *inetd* is a super server that listens to the various ports and handles connection requests as it receives them by initiating a new copy of the appropriate daemon (program). The new copy of the program then takes it from there and works with the client, and *inted* goes back to listening to the server ports waiting for new client requests to handle. Once the request is processed and the communication is over, the daemon exits.

General Structure

As mentioned earlier, Apache can be installed on a variety of operating systems. Regardless of the platform used, a hosted website will typically have four main directories: *htdocs*, *conf*, *logs*, *cgi-bin*.

htdocs is the default Apache web server document directory, meaning it is the public directory whose contents are usually available for clients connecting through the web. It contains all static pages and dynamic content to be served once an HTTP request for them is received. Since files and sub-directories under htdocs are available to the public, correct handling of file permissions is of great importance so as not to compromise the server's safety and security.

conf is the directory where all server configuration files are located. Configuration files are basically plain text files where directives are added to control the web server's behavior and functionality. Each directive is usually placed on a separate line, and the hash (#) key indicates a comment so the line proceeded by it is ignored.

logs is the directory where server logs are kept, and includes Apache access logs and error logs. The Apache HTTP Server provides a variety of different mechanisms for logging everything that happens on it, from the initial request, through the URL mapping process, to the final resolution of the connection, including any errors that may have occurred in the process. In addition to this, third-party modules may provide logging capabilities, or inject entries into the existing log files, and applications such as PHP scripts, or other handlers, may send messages to the server error log.

cgi-bin is the directory where CGI scripts are kept. The CGI (Common Gateway Interface) defines a way for a web server to interact with external content-generating programs, which are often referred to as CGI programs or CGI scripts. These are programs or shell scripts that are written to be executed by Apache on behalf of its clients.

It is important to note that the above discussed file and directory names (as well as locations) can differ from one server to another depending on the Apache flavor installed and the operating system it runs under. The roles though remain the same.

Conclusion

...with more than half of the sites on the web running on it.

Apache has been the most popular web server on the internet since 1996, with more than half the sites on the web running on it. It played a key role in shaping and making the World Wide Web what it is today. The reasons behind its success are obvious and the way things are looking, it will probably stay in the lead at least for quite some time. This was meant to be an introductory session to this powerful piece of software and I hope it was of help in understanding what this great tool is and how it generally works.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

mail server (mail transfer/transport agent, MTA, mail router, Internet mailer)

A mail server (also known as a *mail transfer agent* or MTA, a *mail transport agent*, a *mail router* or an *Internet mailer*) is an application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, qmail, Exim and sendmail are among the more common mail server programs.

The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook or Eudora, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a *message store* to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

SMTP usually is implemented to operate over Internet port 25. An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.

ESMTP (Extended Simple Mail Transfer Protocol)

ESMTP (Extended Simple Mail Transfer Protocol) specifies extensions to the original protocol for sending e-mail that supports graphics, audio and video files, and text in various national languages. The original Internet protocols for sending e-mail are described in Request for Comments (RFC) 822, Standard for the Format of ARPA Internet Text Messages, and in RFC 821, Simple Mail Transfer Protocol (SMTP). As users began to want to attach various kinds of files to e-mail, the need for additional capabilities arose and resulted in RFC 1869, Extended Simple Mail Transfer Protocol.

ESMTP provides the capability for a client e-mail program to ask a server e-mail program which capabilities it supports and then communicate accordingly. Currently, most commercial e-mail servers and clients support ESMTP.

IMAP (Internet Message Access Protocol)

IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s). This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

IMAP can be contrasted with another client/server email protocol, Post Office Protocol 3 (POP3). With POP3, mail is saved for the end user in a single mailbox on the server and moved to the end user's device when the mail client opens. While POP3 can be thought of as a "store-and-forward" service, IMAP can be thought of as a remote file server.

Most implementations of IMAP support multiple logins; this allows the end user to simultaneously connect to the email server with different devices. For example, the end user could connect to the mail server with his Outlook iPhone app and his Outlook desktop client at the same time. The details for how to handle multiple connections are not specified by the protocol but are instead left to the developers of the mail client.

Even though IMAP has an authentication mechanism, the authentication process can easily be circumvented by anyone who knows how to steal a password by using a protocol analyzer because the client's username and password are transmitted as clear text. In an Exchange Server environment, administrators can work around this security flaw by using Secure Sockets Layer (SSL) encryption for IMAP.

POP3 (Post Office Protocol 3)

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. This standard protocol is built into most popular e-mail products, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.

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.

Shamsunnabi Taqib

DIFFERENT TYPE OF SERVER

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.

REFERENCES

I. http://whatis.techtarget.com/definition/server
II. http://www.ncftp.com/libncftp/doc/ftp_overview.html
III. http://www.ftpx.com/ftpintro.aspx
IV. https://webhostinggeeks.com/guides/dns/
V. https://en.wikipedia.org/wiki/Domain_Name_System
VI. https://technet.microsoft.com/en-us/library/cc772774(v=ws.10).aspx
VII. https://code.tutsplus.com/tutorials/an-introduction-to-apache--net-25786
VIII. http://searchexchange.techtarget.com/definition/POP3
IX. http://searchexchange.techtarget.com/definition/IMAP

X. http://searchmicroservices.techtarget.com/definition/mail-server-mail-transfer-transport-agent-MTA-mail-router-Internet-mailer

XI. http://searchexchange.techtarget.com/definition/SMTP

XII. http://searchexchange.techtarget.com/definition/ESMTP