**Application Layer**

The Application Layer is topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

**Functions of Application Layer:**

* Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
* This layer allows users to access, retrieve and manage files in a remote computer.
* It allows users to log on as a remote host.
* This layer provides access to global information about various services.
* This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
* It provides protocols that allow software to send and receive information and present meaningful data to users.
* It handles issues such as network transparency, resource allocation and so on.
* This layer serves as a window for users and application processes to access network services.
* Application Layer is basically not a function, but it performs application layer functions.
* The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
* Application Layer helps us to identify communication partners, and synchronizing communication.
* This layer allows users to interact with other software applications.
* In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0’s or 1’s).
* This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
* This layer also receives and preserves data from it’s previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).
* The protocols which are used in this application layer depend upon what information users wish to send or receive.
* This application layer, in general, performs host initialization followed by remote login to hosts.

**Features provided by Application Layer Protocols:**  
To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.  
The following are some of the features which are provided by Application layer protocols-

* The Application Layer protocol defines process for both parties which are involved in communication.
* These protocols define the type of message being sent or received from any side (either source host or destination host).
* These protocols also define basic syntax of the message being forwarded or retrieved.
* These protocols define the way to send a message and the expected response.
* These protocols also define interaction with the next level.

[**Application Layer Protocols:**](https://www.geeksforgeeks.org/protocols-application-layer/) The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users.  
The following are some of the protocols which are provided by the application layer.

* [**TELNET:**](https://www.geeksforgeeks.org/introduction-to-telnet/) Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
* [**DNS:**](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
* [**DHCP:**](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.
* [**FTP:**](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/) FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.
* [**SMTP:**](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587.
* [**HTTP:**](https://www.geeksforgeeks.org/http-full-form/) HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per the given state), which means the server is not responsible for maintaining the previous client’s requests. HTTP uses port number 80.
* [**NFS:**](https://www.geeksforgeeks.org/network-file-system-nfs/) NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally. NFS uses the port number 2049.
* [**SNMP:**](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/) SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at fixed or random intervals, requiring them to disclose certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).

**Domain Name System (DNS) in Application Layer**

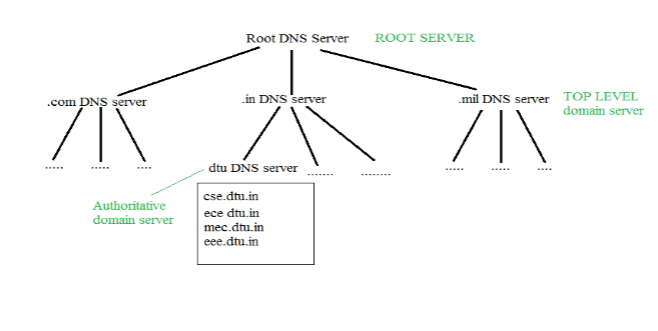
DNS is a hostname for IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

**Requirement:** Every host is identified by the IP address but remembering numbers is very difficult for the people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

**Domain:** There are various kinds of DOMAIN:

1. Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

**Organization of Domain:**

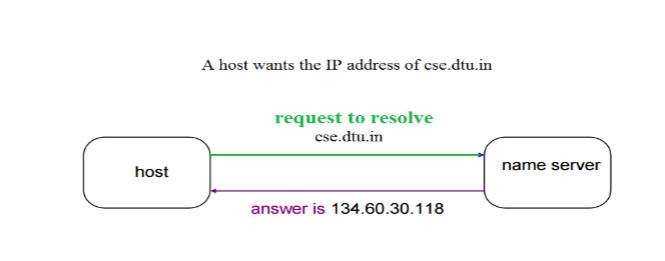
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS.png)

It is very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.

**DNS record:** Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

**Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.

**Name server:** It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

**Name to Address Resolution:**[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS_2.png)

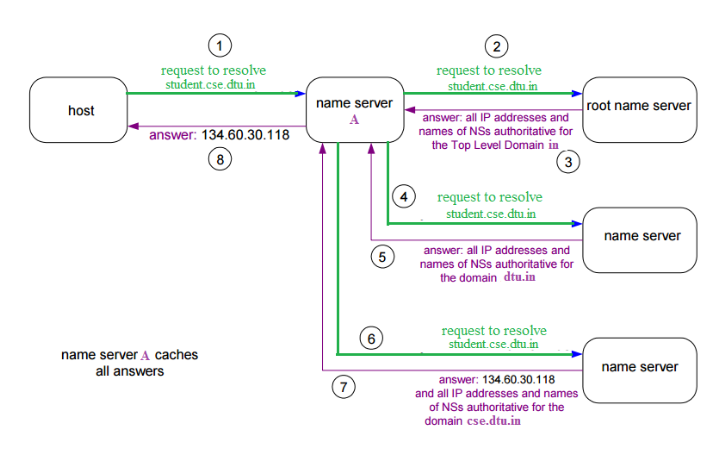
The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

**Hierarchy of Name Servers** **Root name servers:** It is contacted by name servers that cannot resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.

**Top level domain (TLD) server:** It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.

**Authoritative name servers**are the organization’s DNS server, providing authoritative host Name to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

**Domain Name Server**

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS_3.png)

The client machine sends a request to the local name server, which, if root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to an top-level domain (TLD) or authoritative name server. The root name server can also contain some host Name to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

**Simple Network Management Protocol (SNMP)**

If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

**Simple Network Management Protocol (SNMP) –**   
SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

**SNMP components –**   
There are 3 components of SNMP: 

1. **SNMP Manager –**   
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)
2. **SNMP agent –**   
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
3. **Management Information Base –**   
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

**SNMP messages –**   
Different variables are:

1. **GetRequest –**   
   SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
2. **GetNextRequest –**   
   This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.
3. **GetBulkRequest –**   
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –**   
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –**   
   It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
6. **Trap –**   
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **Inform Request –**   
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.

**SNMP security levels –**   
It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely: 

1. **noAuthNoPriv –**   
   This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

**SNMP versions –**   
There are 3 versions of SNMP: 

1. **SNMPv1 –**   
   It uses community strings for authentication and uses UDP only.
2. **SNMPv2c –**   
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. **SNMPv3 –**   
   It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.