Application Layer, DNS and Active Directory

Bhavneet Soni

**Application Layer, DNS and Active Directory**

To have effective communication entities involved need to understand and follow a set of rules or protocols. These protocols are followed across all types of communications be it human or computer. Set of protocols that govern successful communication are:

1. An identified sender and receiver - who is sending the message and who is receiving the message (encapsulation)
2. Agreed upon method of communication (ethernet, wan etc)
3. Common language and grammar (syntax and type of message – message format, encoding)
4. Speed and timing of delivery
5. Acknowledgement of message received

Sending commination over a network needs to have certain aspects as shown in *Figure 1 Communication Protocols* below. Timing dictates the speed at which the data is transmitted over the network. It determines how much data and how and when it can be transmitted. The size of the message being transmitted is dependent on the channel used for transmission, it might have to be broken up into small chunks to ensure reliable delivery of the message. To send the message over a network it needs to have some additional information added to the message header, like the addressing information that identifies the source and destination hosts and the correct application on the destination host. One must also specify the message format or structure based on the type of message and the channel used for delivery of the message. Since the message is being sent over network that might be susceptible to interception therefore its important to encode these messages. Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message. For interactive nature of internet messages usually require some type of acknowledgment before the next message can be sent. This type of request/response pattern is a common aspect of many networking protocols. However, there are other types of messages that may be simply streamed across the network, without concern as to whether or not they reach their destination.

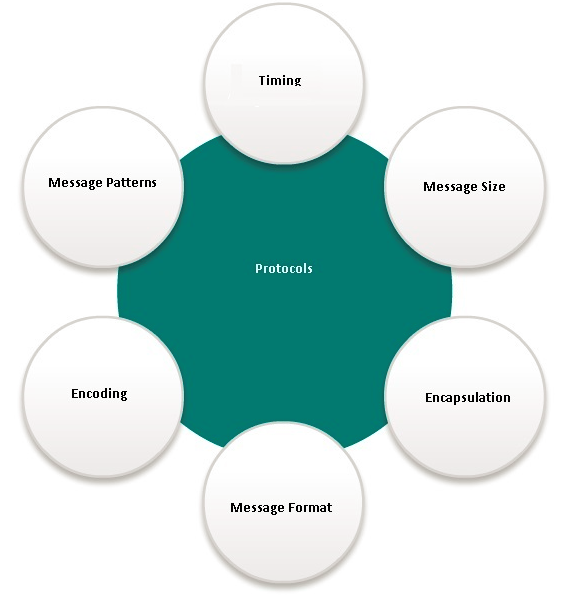


Figure Communication Protocols

Computers on a network communicate by following Network Protocols Communication Protocols. There are different types of network models followed in the industry Protocol model or Reference model Figure 2 and Figure 3 shows different layers in each of these models. These are a superset for various types of communication and data sharing followed by computers at both hardware and software level. The interaction between these protocols are shown as a protocol stack, in *Figure 2 OSI Reference and TCP/IP Protocol Models*  below. The stack illustrates the protocols as layers, with each higher-level protocol depending on the services of the protocols in the lower levels. Splitting the functions into layers enables each layer in the stack to operate independently of others. For example, you can be connected to a ethernet cable to access a website, or view the same website while being connected wireless at the library. The function of the web browser is not affected by the change in the physical location nor the method of connectivity. So, when a device sends or receives a message it uses several protocols. The protocols are described as below.

1. Ethernet protocols – devices and network interface
2. IP – where the sender and receiver are located
3. TCP -
4. HTTP – what data (HTML) is being exchanged

Reference model as shown in *Figure 2 OSI Reference and TCP/IP Protocol Models* is a more detailed model that describe the function developed in early 1980s that must be completed on each layer however it does not govern how they must be accomplished.

TCP and IP model developed in the early 1970s follow a structured layer model consisting of the following layers

1. Application Layer –It represents data to the users and encoding and dialog control
2. Transport Layer – It provides support for communication between diverse devices across diverse networks
3. Internet Layer – Best path through the network
4. Network Access Layer – controls hardware devices and interface of the network

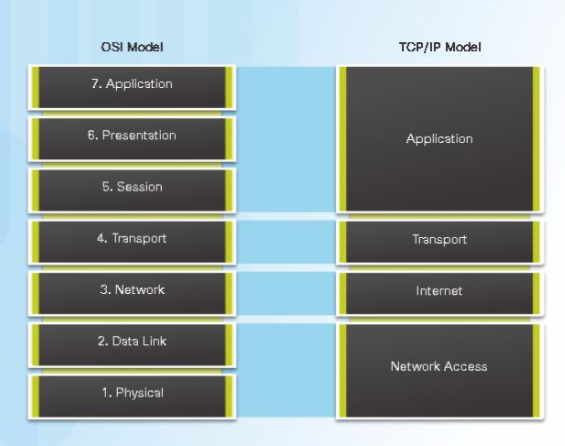
**

Figure OSI Reference and TCP/IP Protocol Models

The functions that occur at the Internet layer in the TCP/IP model are contained in the network layer of the OSI Model, as shown in the figure. The transport layer functionality is the same between both models. However, the network access layer and the application layer of the TCP/IP model are further divided in the OSI model to describe discrete functions that must occur at these layers.

The application layer is a layer in the very top layer of Open Systems Interconnection (OSI) seven-layer model and in the TCP/IP protocol suite. It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services. The application layer provides many services, including:

* Simple Mail Transfer Protocol (SMPT)
* File transfer (FTP)
* Web surfing
* Web chat
* Email clients(IMAP4 POP3)
* Network data sharing
* Virtual terminals
* Various file and data operations

Application communications are mostly of two types, client server or peer to peer (skype, bit torrents etc). To talk to a computer, one needs its IP address and port number. While Ports belong to the transport services while (TCP UDP) layer 4, IP address belongs to layer 3 of the TCP/IP model. Port is a logical place on a computer and where an application listens to from all the above protocols. A computer or a network connection can communicate with multiple connections simultaneously based on the type of application protocol.

Default ports used by some of the popular applications are discussed below.

* FTP – file transfer runs on Port 20 and 21, 20 to setup data and 21 to transfer two connections one for command and control while data port is used for exchange for data, While control connection is persistent i.e. it is in communication with the server all the time while data connection is not persistent and is initiated and data transfer takes place when the file transfer is required and is closed as and when the transfer is complete. Server maintains full state awareness of the files and the data transfer. Control is out of band

Active mode:

* Client opens up command channel from client port 2000(a) to server port 21(b).
* Client sends PORT 2001(a) to server and server acknowledges on command channel.
* Server opens up data channel from server port 20(b) to client port 2001(a).
* Client acknowledges on data channel.

Passive mode:

* Client opens up command channel from client port 2000(a) to server port 21(b).
* Client sends PASV to server on command channel.
* Server sends back (on command channel) PORT 1234(a) after starting to listen on that port.
* Client opens up data channel from client 2001(a) to server port 1234(a).
* Server acknowledges on data channel.
* SMPT -simple mail transfer protocol – it is one of the oldest protocol and was developed in the beginning of the internet age. Older protocol used to allow only for 7 bit ASCII messages, all binary objects have to be converted into ASCII. SMPT is by default available on port 25 – it’s kind of a store and forward system. Persistent TCP connection and it is used to send the email and does only push. Each email service has their own server that will store all the sent message in a queue and will send them to the destination emails server when its available.
* To get mail applications use Post office protocol POP3 and are used for only receiving message by pulling message.
* While fetching email from server the Authorization phase and transaction phase uses port 110 to setup connection with the server.
* IMAP4 is more advanced version of POP3, POP3 only maintain a copy of the email on the local machine while IMAP keeps the local and the server mail boxes in sync. Any change on one end is synchronized on the other as well.
* HTTP – web browsing on Port 80 has only one connection and use in band control have 4 basic commands like Get, Put, Post, Delete
* HTTPS – Hyper Text Transport Protocol – Secure uses port 443 for communication instead of port 80 as used by HTTP.
* Telnet – Remote control Port 23 not very secured
* DHCP servers use port 67 and 68 for sending and for receiving respectively

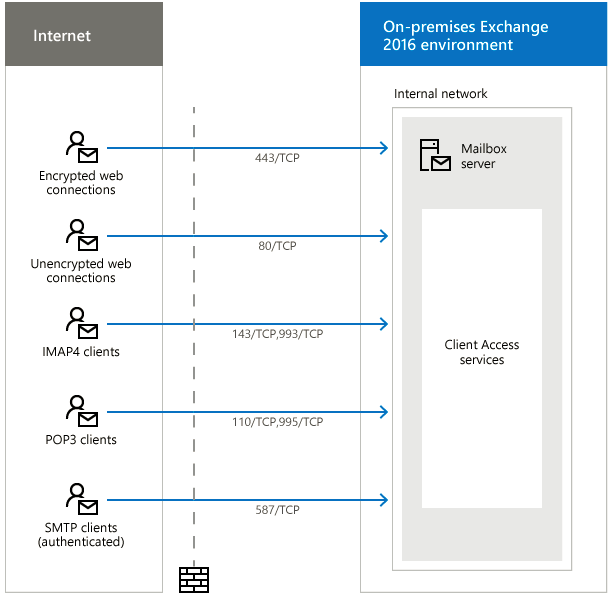


Figure TCP Ports used by different protocols

DNS stands for Domain Name System - DNS – is responsible for IP address to Name resolution and is available by default at Port 53. Computers go by IP or Mac address which is very difficult for us to remember. Humans find it easy to remember names of websites or computers rather than their IP addresses. Hence DNS provides a great service as in it translates human readable host name to IP address. DNS is a distributed database of all the IP addresses in the world. under it and When a computer needs the address of a computer or domain it will check if DNS stores have a cached address of the destination and will provide proper IP address for the requested client name. If a DNS server does not have a information about the requested host name it ask its parent DNS server if it knows and so on and so forth. DNS is a hieratical tree structure with (.) DNS sitting at the root There are 13 different root servers in the world that are strategically placed all over the world. Each of these severs have unique IP address. These root servers have further Top Level Domain (TLD) servers such as com, edu, org, biz etc. However, these server sill don’t have the ip address of the other computers, in turn these will direct the request to authoritative name servers will resolve the IP address of the name. When a server gets a new entry from its parent it keeps a copy of the information in its data base so as it can serve the request faster the next time someone will ask for it again. Each IP is associated with the name for a specific period of time and keep changing unless it s a static IP address. DNS keeps records Resource Records = (Name, Value, Type, TTL) TTL is time to live, i.e how long the IP address or the value is valid, anything older then the TTL value is discarded and the server asks for its fresh copy from the parent node.

DNS is also responsible for Host aliasing, mail server aliasing and load distribution. e.g some Busy websites such as google have such high demand that only one server cannot serve all the requests form the same server. So in that case Google serve its content from various locations and various servers, however it uses the DNS to load balance. When you type in google in your browser, browser will look in the cache if it has Google’s IP it calls it otherwise ask the parent. DNS severs can decide which IP address that is closest or least busy is served. Similarly, a single server can host multiple small websites and different IP address will still map to the same server. Likewise, Multiple email domain names can still be served by the same server by mapping the names to same IP.

Similar to DNS, Active directory is for Windows Server. Since Windows 2008 server Active directory is called Active Directory directory services. AD is mainly used in organizations with 10 – 100 thousand users. AD is used to Control computers and networks in corporate environment. AD is dependent on DNS, apart IP address it also has user and computer information. Domain controller controls is the server that controls the AD services and the users and computers part of these. Domain controllers creates domains, and all the users and computer part of the enterprise network will belong to one domain or another.

AD contains a database (schema) of User accounts and Computer accounts that contains all the data related to different user and computer accounts. Each of these computers and users are made part of different groups. Groups will have certain permissions to access to certain files or resources. The rights and permissions are inherited from the groups a user or computer is part of. Groups are used to manage the security and accessibility of enterprise resources. Groups are further part of Organizational Units, which are used to lock the settings down and can be given permission to have administrative privileges.

AD is also the most fundamental resource for application of Single sign on services on your enterprise controlled by the Active directory directory services give individual computer security permissions and access to each of them.

References

(n.d.). Retrieved from Coursera.org: https://www.coursera.org/learn/network-protocols-architecture/

(n.d.). Retrieved from www.techopedia.com: https://www.techopedia.com/definition/6006/application-layer

Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (n.d.). *DISTRIBUTED SYSTEMS Concepts and Design.* Addison Wesley.