IT-3013 Networking 1

James Aaron F. Guevarra
Christian Jay B.Tantan
Ronnie V. Edec

Bachelor of Science in Information Technology
College of Computing Studies

Table of Contents

MODULE 8
THE APPLICATION LAYER

Introduction

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host (Callaway, Jason 2020).

Learning Outcomes

At the end of this lesson, the student should be able to:

- ✓ Understand and explain Data Communications System and its components.
- ✓ Identify the different types of network topologies and protocols.
- ✓ Enumerate the layers of the OSI model and TCP/IP. Explain the function(s) of each layer.
- ✓ Identify the different types of network devices and their functions within a network.

What is Application Layer?

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their respective highest level layer, the detailed definitions and purposes are different (Callaway, Jason 2020).

Sitting at Layer 7, the very top of the Open Systems Interconnection (OSI) communications model -- the application layer provides services for an application program to ensure that effective communication with another application program on a network is possible. The application layer should not be thought of as an application as most people understand it. Instead, the application layer is a component within an application that controls the communication method to other devices. It's an abstraction layer service that masks the rest of the application from the transmission process. The application layer relies on all the layers below it to complete its process. At this stage, the data, or the application, is presented in a visual form the user can understand (Callaway, Jason 2020).

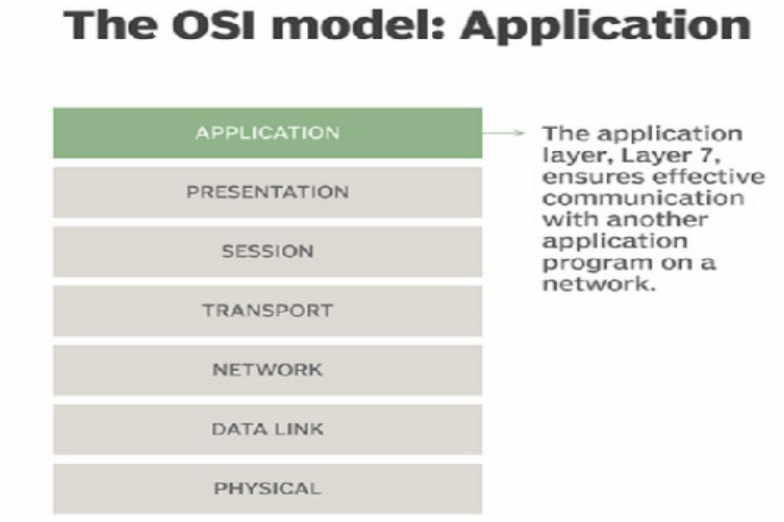


Figure 8.1. The OSI Model: Application

Source: HYPERLINK "https://www.tutorialspoint.com/data_communication" https://www.tutorialspoint.com/data_communicationcomputer_network/application_layer_introduction.htm

Functions of the application layer

- ✓ Ensures that the receiving device is identified, can be reached and is ready to accept data.
- ✓ Enables, if appropriate, authentication to occur between devices for an extra layer of security.
- ✓ Makes sure necessary communication interfaces exist. For example, is there an Ethernet or Wi-Fi interface in the sender's computer?
- ✓ Ensures agreement at both ends about error recovery procedures, data integrity and privacy.
- ✓ Determines protocol and data syntax rules at the application level.
- ✓ Presents the data on the receiving end to the user application.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.

There' is an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

On the other hand, when we use a Web Browser, which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network. HTTP is Application Layer protocol.

Another example is File Transfer Protocol, which helps a user to transfer text based or binary files across the network. A user can use this protocol in either GUI based software like FileZilla or CuteFTP and the same user can use FTP in Command Line mode.

Hence, irrespective of which software you use, it is the protocol which is considered at Application Layer used by that software. DNS is a protocol which helps user application protocols such as HTTP to accomplish its work (Callaway, Jason 2020).

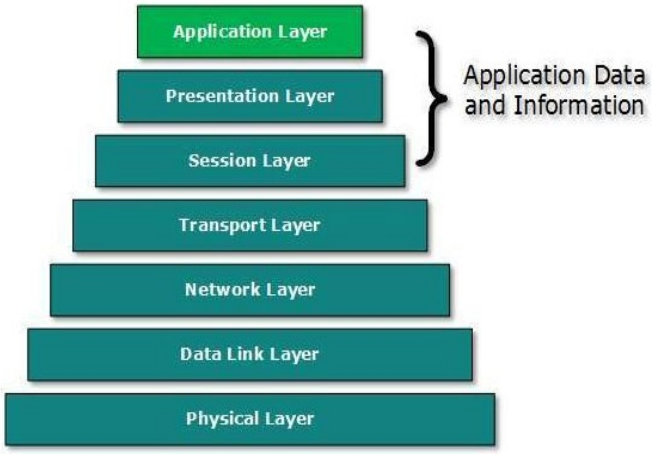


Figure 8.2.The OSI Model: Application

Source:https://www.tutorialspoint.com/data_communication_computer_network/application_layer_introduction.htm

Lesson 1. Client Server Model

The client-server model describes how a server provides resources and services to one or more clients. Examples of servers include web servers, mail servers, and file servers. Each of these servers provide resources to client devices, such as desktop computers, laptops, tablets, and smartphones (Callaway, Jason 2020).

Client-server denotes a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service.

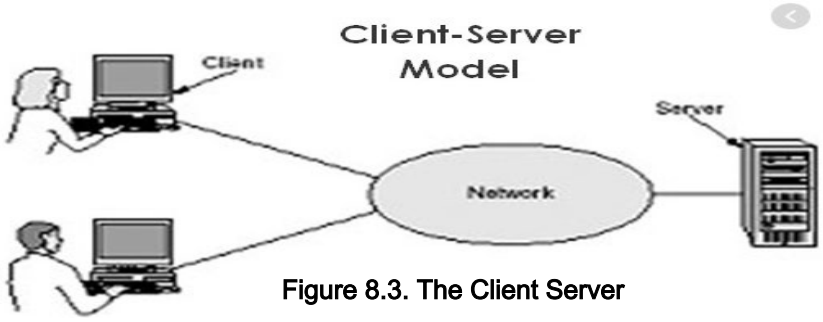


Figure 8.3. The Client Server

Source:https://www.javatpoint.com/osi-model

The way the client and server communicate is known as the client/server stack. In the OSI model, communication between separate computers occurs in a stack-like fashion with information passing from one node to the other through several layers of code, including: Physical layer. Data link layer (Callaway, Jason 2020).

Lesson 1.1 Peer to Peer

Protocol layers may be defined in such a way that the communications within a layer is independent of the operation of the layer being used. This is known as "peer-to-peer" communication and is an important goal of the OSI Reference Model (Callaway, Jason 2020).

Each layer provides a protocol to communicate with its peer. When a packet is transmitted by a layer, a header consisting of Protocol Control Information (PCI) is added to the data to be sent. In OSI terminology, the packet data (also known as the Payload) is called a Protocol Data Unit (PDU). The packet so-formed, called a Service Data Unit (SDU) is passed via a service access point to the layer below. This is sent using the service of the next lower protocol layer (Callaway, Jason 2020).

In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function. - Dividing the network into seven layers provides the following advantages:

- ✓ It breaks network communication into smaller, more manageable parts.
- ✓ It standardizes network components to allow multiple vendor development and support.
- ✓ It allows different types of network hardware and software to communicate with each other.
- ✓ It prevents changes in one layer from affecting other layers.

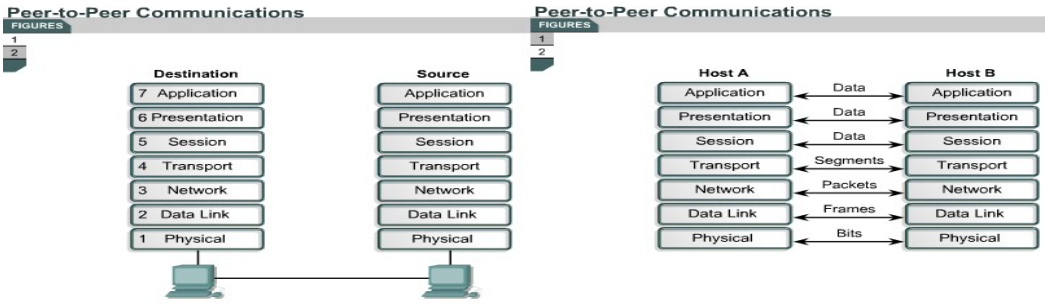


Figure 8.4. Peer to Peer Communications
Source: https://www.javatpoint.com/peer-topeer

Two remote application processes can communicate mainly in two different fashions:

- ✓ **Peer-to-peer:** Both remote processes are executing at same level and they exchange data using some shared resource.
- ✓ **Client-Server:** One remote process acts as a Client and requests some resource from another application process acting as Server.

In client-server model, any process can act as Server or Client. It is not the type of machine, size of the machine, or its computing power which makes it server; it is the ability of serving request that makes a machine a server.

A system can act as Server and Client simultaneously. That is, one process is acting as Server and another is acting as a client. This may also happen that both client and server processes reside on the same machine (Callaway, Jason 2020).

Lesson 1.2 Client – Server

Client-server denotes a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service. The client-server model, or client-server architecture, is a distributed application framework dividing tasks between servers and clients, which either reside in the

Figure 8.5. Client Server

Source: https://www.javatpoint.com/peer-topeer

same system or communicate through a computer network or the Internet. The client relies on sending a request to another program in order to access a service made available by a server. The server runs one or more programs that share resources with and distribute work among clients (Callaway, Jason 2020).

The client server relationship communicates in a request–response messaging pattern and must adhere to a common communications protocol, which formally defines the rules, language, and dialog patterns to be used. Client-server communication typically adheres to the TCP/IP protocol suite (Callaway, Jason 2020).

TCP protocol maintains a connection until the client and server have completed the message exchange. TCP protocol determines the best way to distribute application data into packets that networks can deliver, transfers packets to and receives packets from the network, and manages flow control and retransmission of dropped or garbled packets. IP is a connectionless protocol in which each packet traveling through the Internet is an independent unit of data unrelated to any other data units (Callaway, Jason 2020).

Client requests are organized and prioritized in a scheduling system, which helps servers cope in the instance of receiving requests from many distinct clients in a short space of time. The client-server approach enables any general-purpose computer to expand its capabilities by utilizing the shared resources of other hosts. Popular client-server applications include email, the World Wide Web, and network printing (Callaway, Jason 2020).

Categories of Client-Server Computing

There are four main categories of client-server computing (Callaway, Jason 2020):

- ✓ **One-Tier architecture:** consists of a simple program running on a single computer without requiring access to the network. User requests don't manage any network protocols, therefore the code is simple and the network is relieved of the extra traffic.
- ✓ **Two-Tier architecture:** consists of the client, the server, and the protocol that links the two tiers. The Graphical User Interface code resides on the client host and the domain logic resides on the server host. The client-server GUI is written in high-level languages such as C++ and Java.
- ✓ **Three-Tier architecture** : consists of a presentation tier, which is the User Interface layer, the application tier, which is the service layer that performs detailed processing, and the data tier, which consists of a database server that stores information.
- ✓ **N-Tier architecture:** divides an application into logical layers, which separate responsibilities and manage dependencies, and physical tiers, which run on separate machines, improve scalability, and add latency from the additional network communication. N-Tier architecture can be closed-layer, in which a layer can only communicate with the next layer down, or open-layer, in which a layer can communicate with any layers below it (Callaway, Jason 2020).

What is a Client -Server Network?

A client-server network is the medium through which clients access resources and services from a central computer, via either a local area network (LAN) or a wide-area network (WAN), such as the Internet. A unique server called a daemon may be employed for the sole purpose of awaiting client requests, at which point the network connection is initiated until the client request has been fulfilled (Callaway, Jason 2020).

Network traffic is categorized as client-to-server (north-south traffic) or server-to-server (east-west traffic). Popular network services include e-mail, file sharing, printing, and the World Wide Web. A major advantage of the client-server network is the central management of applications and data (Callaway, Jason 2020).

Benefits of Client -Server Computing

There are numerous advantages of the client server architecture model (Callaway, Jason 2020):

- ✓ A single server hosting all the required data in a single place facilitates easy protection of data and management of user authorization and authentication.
- ✓ Resources such as network segments, servers, and computers can be added to a client-server network without any significant interruptions.
- ✓ Data can be accessed efficiently without requiring clients and the server to be in close proximity.
- ✓ All nodes in the client-server system are independent, requesting data only from the server, which facilitates easy upgrades, replacements, and relocation of the nodes.
- ✓ Data that is transferred through client-server protocols are platform-agnostic.

Difference Between Client and Server

Clients, also known as service requesters, are pieces of computer hardware or server software that request resources and services made available by a server. Client computing is classified as Thick, Thin, or Hybrid (Callaway, Jason 2020).

- ✓ **Thick Client:** a client that provides rich functionality, performs the majority of data processing itself, and relies very lightly upon the server.
- ✓ **Thin Client** : a thin-client server is a lightweight computer that relies heavily on the resources of the host computer -- an application server performs the majority of any required data processing.
- ✓ **Hybrid Client:** possessing a combination of thin client and thick client characteristics, a hybrid client relies on the server to store persistent data, but is capable of local processing.

A server is a device or computer program that provides functionality for other devices or programs. Any computerized process that can be used or called upon by a client to share resources and distribute work is a server. Some common examples of servers include (Callaway, Jason 2020):

- ✓ **Application Server:** hosts web applications that users in the network can use without needing their own copy.
- ✓ **Computing Server:** shares an enormous amount of computer resources with networked computers that require more CPU power and RAM than is typically available for a personal computer.
- ✓ **Database Server:** maintains and shares databases for any computer program that ingests well-organized data, such as accounting software and spreadsheets.
- ✓ Web Server: hosts web pages and facilitates the existence of the World Wide Web.

Client-Server VS Peer-to-Peer

Peer-to-peer (P2P) is a decentralized communications model in which all nodes in the network have equivalent capability and can function as both a client and server. Nodes in peer-to-peer computing collectively use their resources and communicate with each other directly on-demand (Callaway, Jason 2020).

An algorithm in the peer-to-peer communications protocol balances load, making other peers available to compensate for any resource downtime, and rerouting requests as the load capacity and availability of peers changes. A major advantage of peer-to-peer networking is the ability to expand the network to manage a large number of clients (Callaway, Jason 2020).

In client-server computing, a centralized communications model, the server is the central node that communicates with other client nodes. A major advantage that the client-server relationship has over the peer-to-peer relationship is the ability to manage data and applications in one, centralized server (Callaway, Jason 2020).

Lesson 2. Application Protocol

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their

respective highest level layer, the detailed definitions and purposes are different (Callaway, Jason 2020).

It is the top most layer of OSI Model. Manipulation of data(information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc(Callaway, Jason 2020).

The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.Other Application protocols that are used are: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol(SMTP), TELNET, Domain Name System(DNS) etc(Callaway, Jason 2020).

Functions of Application Layer

- ✓ **Mail Services** : This layer provides the basis for E-mail forwarding and storage.
- ✓ **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.

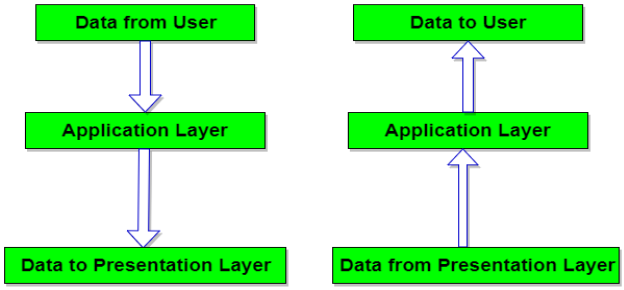


Figure 8.6. Function of Application

- ✓ **Directory Services:** This layer provides access for global information about various services.
- ✓ **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

Lesson 2.1 Domain Name Server (DNS)

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

A DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53 (Callaway, Jason 2020).

Domain Name Service (DNS) is an application layer protocol used to resolve hostnames to IP addresses. Although a host can be accessed by using only its IP address, DNS makes your life easier by using domain names. For example, you can access the Google website by typing http://208.117.229.214 in your browser, but it is much easier to type http://www.google.com.

Each host that wants to use DNS needs to have a DNS server configured. When you type a URL in your browser (e.g. http://www.google.com), your host will query the DNS server for the IP address of www.google.com. The DNS server will resolve the query and send the answer back to the host. The host will then be able to establish a connection to http://www.google.com (Callaway, Jason 2020).

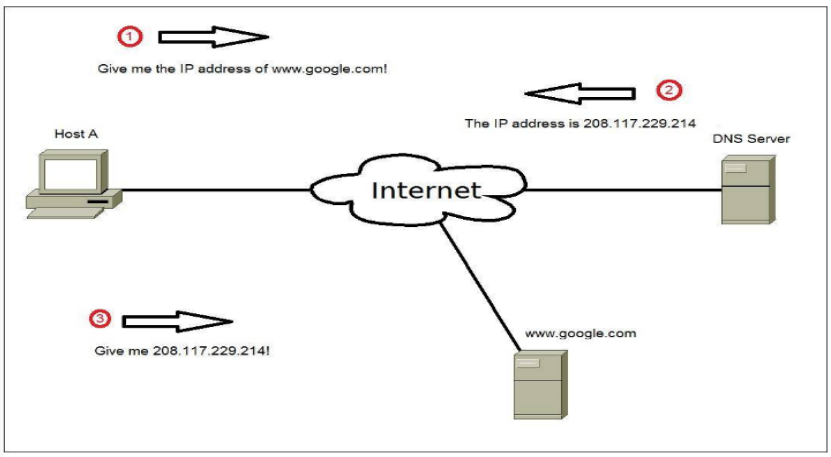


Figure 8.7. Domain Name Server

Source: https://www.javatpoint.com/peer-topeer

Lesson 2.2 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software (Callaway, Jason 2020).

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587 (Callaway, Jason 2020)..

Client software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

What is SMTP?

SMTP (Simple mail Transfer Protocol) is a network protocol (a set of rules employed in sending messages over a network) used for the sending and receiving of text -based messages or email messages between one server and another. If you have used an email sy stem before, then SMTP has facilitated the transmission and delivery of your messages. But it must be noted that SMTP only serves to get the messages to their destination recipient servers that is why it is an end to end service. In order for you to downlo ad or access these messages, an email client such as Outlook Yahoo or Gmail Protocols is used. An email client is a form of email reader that allows the user to access and manage their messages. The SMTP can be likened to the mailman who gets your mail fro m the post office to your home/office mailbox. The postman has no capability to receive, read, respond to or throw your mails away. In other words the postman

cannot manage your emails. He delivers and that's it. You need an email client to do that (Callaway, Jason 2020).

How Does it all work?

SMTP functions as a delivery system from one SMTP server to the destination SMTP server. This is illustrated in Figure 1. There are different layers in the network protocols employed in internet messaging. SMTP, however, is an application layer protocol (function over the application layer) that manages its messages over the TCP/IP (Transmission Control Protocol/Internet Protocol) Port 25. TCP/IP is a collection of communication protocols that are employed in the interconnection of communication devices over the internet or over a private network (Callaway, Jason 2020).

SMTP Server Contact Initialized

Claire's mail client through her corresponding SMTP server sends a message to Ben's SMTP Server. The server respond acknowledging request with a 220 READY FOR MAIL message Claire's mail client receives the 220 message and responds with a HELLO command. Ben 's server responds with '250 requested mail action OK'. The process now begins.

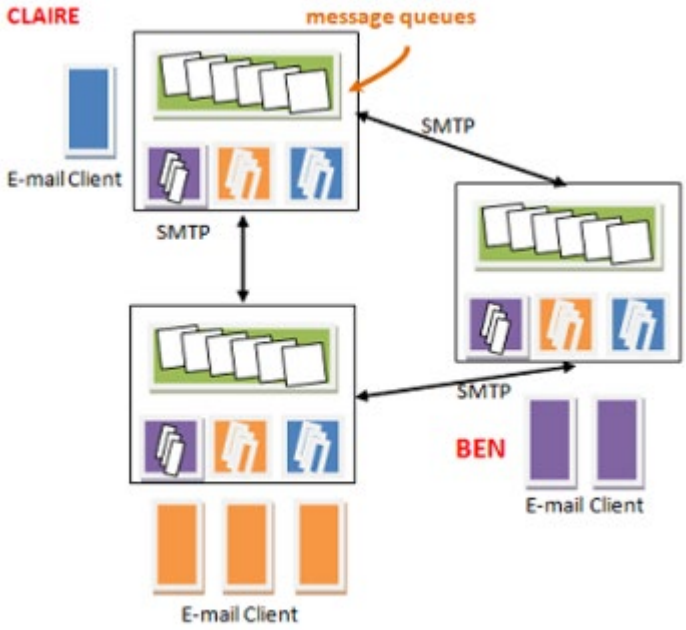


Figure 8.8. SMTP

Source:https://www.javatpoint.com/simple-mail-transfer-protocol

Mail Identification Details Transmitted

With the MAIL command, sender and identification details are sent as a well as details of an address, in case there is an error in transmission. When the Mail command completes successfully the sender transmits a number of RCPT (receipt) commands identifyi ng email recipients. The receiving server responds with 250 OK acknowledging details or in the event there is an error responds with 550 NO such users here (Callaway, Jason 2020).

Lesson 2.3 File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.

The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection (Callaway, Jason 2020).

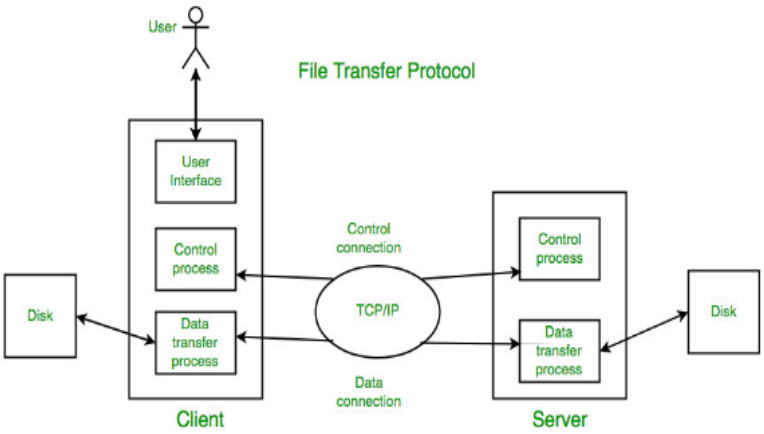


Figure 8.9. File Transfer Protocol

Source:https://www.javatpoint.com/computer-network-ftp

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

What is control connection?

- ✓ For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.

What is data connection?

For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20. FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples (Callaway, Jason 2020).

Lesson 2.4 Post Office Protocol (POP)

The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server.

When a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer. POP3 works in two modes.

Figure 8.10. Post Office Protocol

Source: https://www.javatpoint.com/pop-protocol

The most common mode the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server (Callaway, Jason 2020).

- ✓ POP is also called as POP3 protocol
- ✓ This is a protocol used by e-mail server in conjunction with SMTP to receive and holds mail for host.
- ✓ POP3 mail server receives e-mail and filters them into the appropriate user folder. When a user connects to the mail server to retrieve his mail, the message are downloaded from server to the user's hard disk.

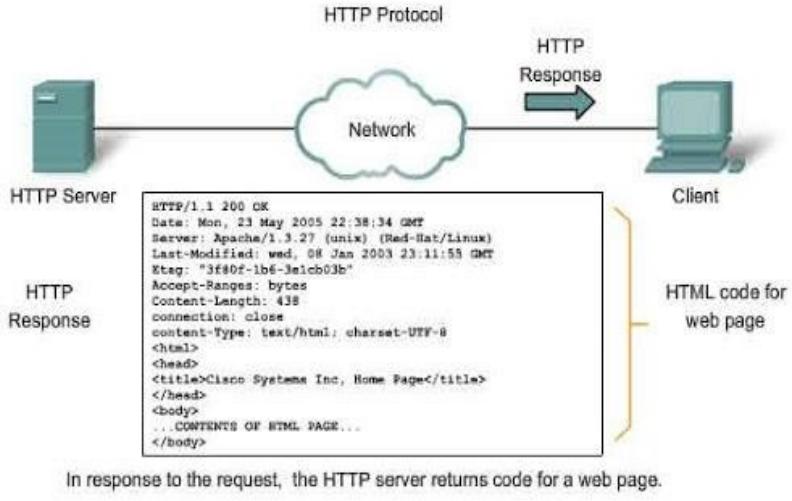
Lesson 2.5 Hypertext Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP versions

- ✓ HTTP 1.0 uses non persistent HTTP. At most one object can be sent over a single TCP connection.
- ✓ HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection (Callaway, Jason 2020).



In response to the request, the HTTP server returns code for a web page.

Hypertext Transfer Protocol (HTTP) is an application layer protocol used by web browsers and web servers to transfer files, such as text and graphic files. It is a client-server protocol; a client (usually a web browser) requests a resource (a web page) from a web server. The web server responds with the requested web page (Callaway, Jason 2020).

Lesson 3. Network Services

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine (Callaway, Jason 2020).

Clients and servers will often have a user interface, and sometimes other hardware associated with it. Computer systems and computerized systems help human beings to work efficiently and explore the unthinkable. When these devices are connected together to form a network, the capabilities are enhanced multiple-times. Some basic services computer network can offer are (Callaway, Jason 2020).

Lesson 3.1 Directory Services

These services are mapping between name and its value, which can be variable value or fixed. This software system helps to store the information, organize it, and provides various means of accessing it (Callaway, Jason 2020).

Accounting

In an organization, a number of users have their user names and passwords mapped to them. Directory Services provide means of storing this information in cryptic form and make available when requested (Callaway, Jason 2020).

Authentication and Authorization

User credentials are checked to authenticate a user at the time of login and/or periodically. User accounts can be set into hierarchical structure and their access to resources can be controlled using authorization schemes (Callaway, Jason 2020).

Domain Name Services

DNS is widely used and one of the essential services on which internet works. This system maps IP addresses to domain names, which are easier to remember and recall than IP addresses. Because network operates with the help of IP addresses and humans tend to remember website names, the DNS provides website's IP address which is mapped to its name from the back -end on the request of a website name from the user (Callaway, Jason 2020).

File Services

File services include sharing and transferring files over the network.

File Sharing

One of the reason which gave birth to networking was file sharing. File sharing enables its users to share their data with other users. User can upload the file to a specific server, which is accessible by all intended users. As an alternative, user can ma ke its file shared on its own computer and provides access to intended users (Callaway, Jason 2020).

File Transfer

This is an activity to copy or move file from one computer to another computer or to multiple computers, with help of underlying network. Network enables its user to locate other users in the network and transfers files (Callaway, Jason 2020).

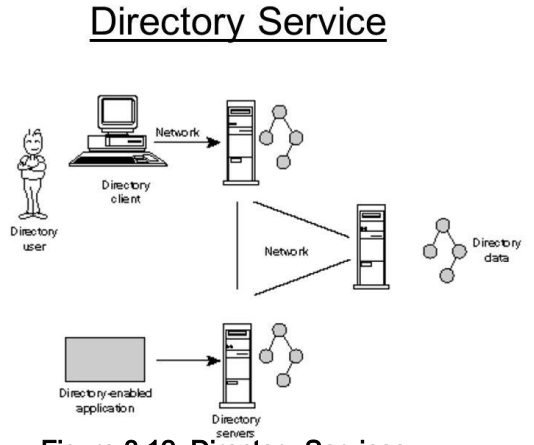


Figure 8.12. Directory Services [3]

Source:https://www.javatpoint.com/computer-network-ftp

Lesson 3.2 Communication Services

A communications service provider is a service provider that transports information electronically for example, a telecommunications service provider. The term encompasses public and private companies in the telecom, Internet, cable, satellite, and managed services businesses (Callaway, Jason 2020).

Email

Electronic mail is a communication method and something a computer user cannot work without. This is the basis of today's internet features. Email system has one or more email servers. All its

users are provided with unique IDs. When a user sends email to other user, it is actually transferred between users with help of email server (Callaway, Jason 2020).

Social Networking

Recent technologies have made technical life social. The computer savvy peoples, can find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos (Callaway, Jason 2020).

Internet Chat

Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with each other using text based Internet Relay Chat services. These days, voice chat and video chat are very common (Callaway, Jason 2020).

Discussion Boards

Discussion boards provide a mechanism to connect multiple peoples with same interests. It enables the users to put queries, questions, suggestions etc. which can be seen by all other users. Other may respond as well.

Remote Access

This service enables user to access the data residing on the remote computer. This feature is known as Remote desktop. This can be done via some remote device, e.g. mobile phone or home computer.

Lesson 3.3 Application Services

These are nothing but providing network based services to the users such as web services, database managing, and resource sharing (Callaway, Jason 2020).

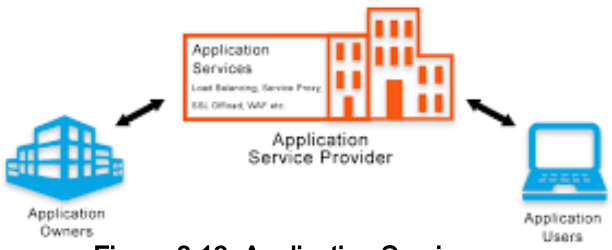


Figure 8.13. Application Services

Source:https://images.app.goo.gl/usdf8NYA9WBWHqj46

Resource Sharing

To use resources efficiently and economically, network provides a mean to share them. This may include Servers, Printers, and Storage Media etc. (Callaway, Jason 2020)

Databases

This application service is one of the most important services. It stores data and information, processes it, and enables the users to retrieve it efficiently by using queries. Databases help organizations to make decisions based on statistics (Callaway, Jason 2020).

Web Services

World Wide Web has become the synonym for internet. It is used to connect to the internet, and access files and information services provided by the internet servers (Callaway, Jason 2020).

Lesson 4. Transport Layer

Next Layer in OSI Model is recognized as Transport Layer (Layer-4). All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host.

Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery (Callaway, Jason 2020).

Layer 4 of the OSI Model: Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation and desegmentation, and error control. It provides logical

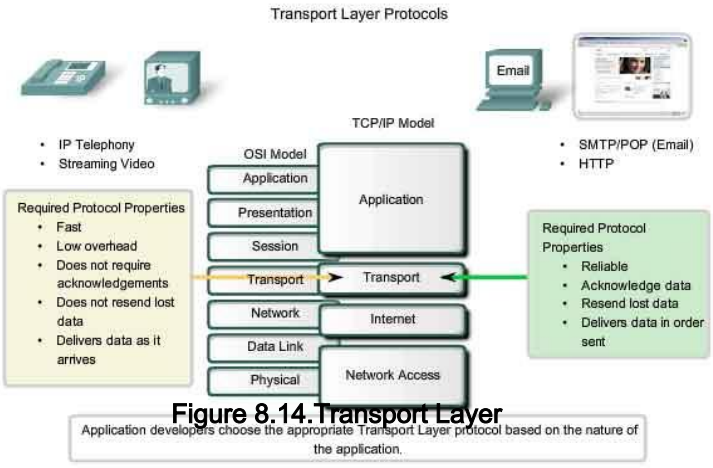


Figure 8.14.Transport Layer

Source: https://images.app.goo.gl/58VSjQjWgqdz5DkNA

communication between application processes running on different hosts within a layered architecture of protocols and other network components.

In a nutshell, the transport layer collects message segments from applications, and transmits them into the network (Layer 3). Here the segments are reassembled into fully-fledged messages, and passed on to Layer 7. The transport layer is also responsible for the management of error correction, providing quality and reliability to the end user. This layer enables the host to send and receive error corrected data, packets or messages over a network and is the network component that allows multiplexing (Callaway, Jason 2020).

Functions of the Transport Layer

- ✓ This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- ✓ This layer ensures that data must be received in the same sequence in which it was sent.

- ✓ This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.
- ✓ All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also known as port numbers.

End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.

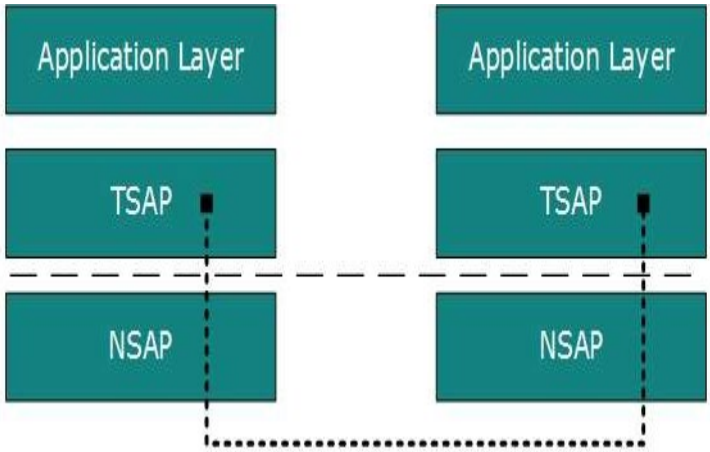


Figure 8.16. End to end Communication
Source:https://www.tutorialspoint.com/data_communication_computer_network/application_layer_introduction.htm

For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

The two main Transport layer protocols are:

Transmission Control Protocol

It provides reliable communication between two hosts.

User Datagram Protocol

It provides unreliable communication between two hosts.

Lesson 4.1 Transmission Control Protocol

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet (Callaway, Jason 2020).

Transmission Control Protocol (TCP) – a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network. It is the most common protocol in networks that use the Internet Protocol (IP); together they are sometimes referred to as TCP/IP (Callaway, Jason 2020).

TCP takes messages from an application/server and divides them into packets, which can then be forwarded by the devices in the network – switches, routers, security gateways – to the destination. TCP numbers each packet and reassembles them prior to handing them off to the application/server recipient. Because it is connection-oriented, it ensures a connection is established and maintained until the exchange between the application/servers sending and receiving the message is complete (Callaway, Jason 2020).

For example, when an email (using the simple mail transfer protocol – SMTP) is sent from an email server, the TCP layer in that server will divide the message up into multiple packets, number them and then forward them to the IP layer for transport. At the IP layer, each packet will be transported to the destination email server. While each packet is going to the same place, the route they take to get there may be different. When it arrives, the IP layer hands it back to the TCP layer, which reassembles the packets into the message and hands it to the email application, where it shows up in the Inbox (Callaway, Jason 2020).

Features of Transmission Control Protocol

TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it (Callaway, Jason 2020).

- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.

- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.

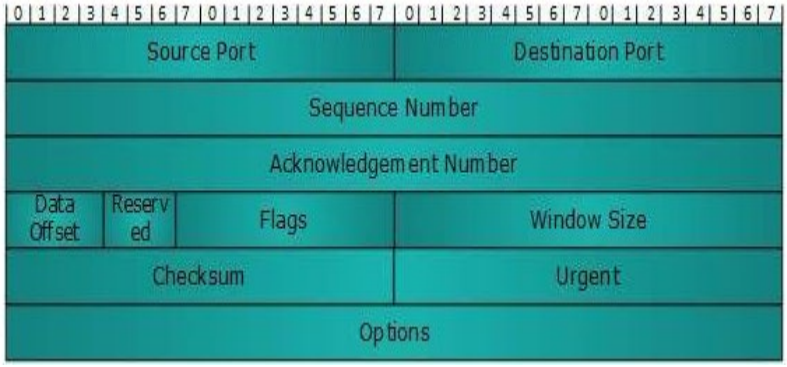


Figure 8.17. Header of transport Layer
Source:https://www.tutorialspoint.com/data_communication_computer_network/transport_layer_introduction.htm

Source Port (16 -bits) - It identifies source port of the application process on the sending device.

Destination Port (16 -bits) - It identifies destination port of the application process on the receiving device.

Sequence Number (32 -bits) - Sequence number of data bytes of a segment in a session.

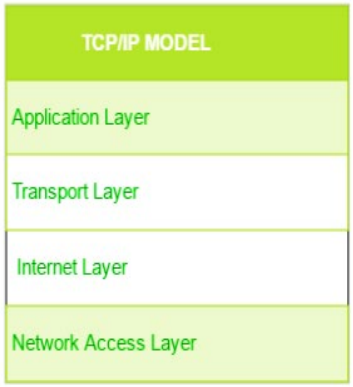
Acknowledgement Number (32 -bits) - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.

Data Offset (4 -bits) - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.

Reserved (3 -bits) - Reserved for future use and all are set zero by default.

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer



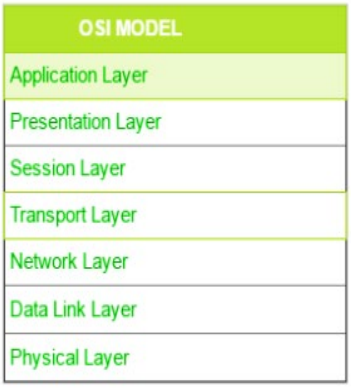


Figure 8.18. The diagrammatic comparison of TCP/IP
Source: https://www.javatpoint.com/computer-network-tcp-ip-model

Difference between TCP/IP and OSI Model:

TCP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

Network Access Layer

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

Internet Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are (Callaway, Jason 2020):

- **IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
- **ICMP** – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP** – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

Host-to-Host Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

- **Transmission Control Protocol (TCP)** – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
- **User Datagram Protocol (UDP)** – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

Application Layer

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are (Callaway, Jason 2020):

- **HTTP and HTTPS** – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

- **SSH** – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync (Callaway, Jason 2020).

Lesson 4.2 Addressing

According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating (Javapoint, n.d).

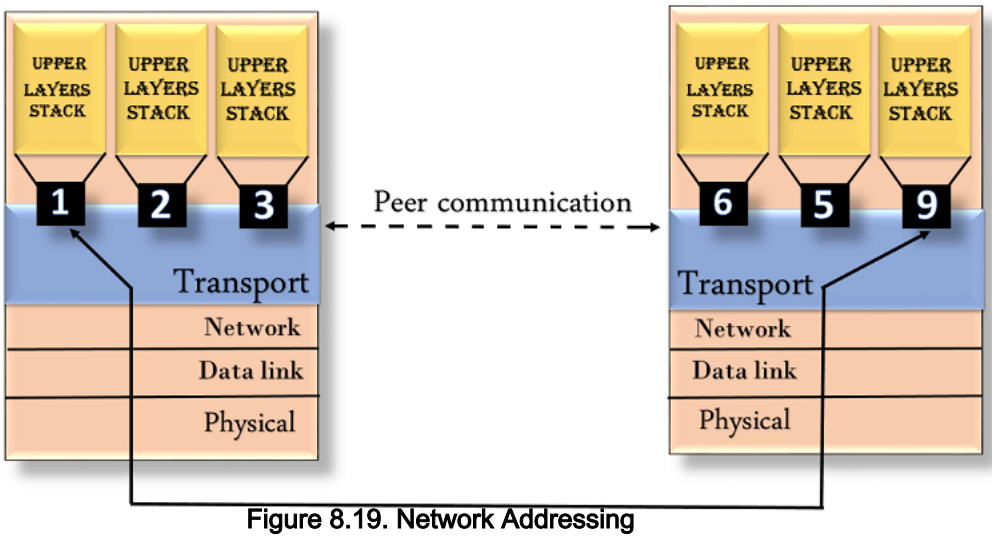


Figure 8.19. Network Addressing
Source: https://www.javatpoint.com/computer-network-tcp-ip-model

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- ✓ System Ports (0 – 1023)
- ✓ User Ports (1024 – 49151)
- ✓ Private/Dynamic Ports (49152 – 65535)

Lesson 4.3 Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.

Connection management includes establishing, maintaining, and terminating the links between networked systems. This layer provides for full-duplex, half-duplex, and simplex communications (i.e., two-way simultaneous, two-way one-way-at-a-time, and one direction only).

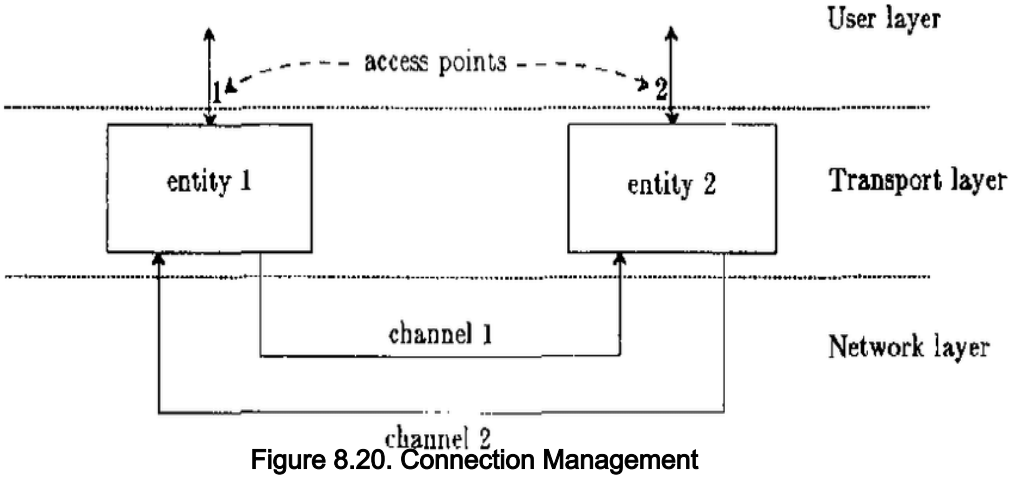


Figure 8.20. Connection Management
Source: https://www.javatpoint.com/computer-network-tcp-ip-model

Lesson 4.4 Bandwidth Management

Bandwidth management refers to the process of optimizing the bandwidth that carries traffic over networks. Bandwidth the amount of data transferred over a communication channel in a specific amount of time can be controlled by bandwidth management tools, which often are referred to as traffic or packet shapers.

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4 -byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again (Callaway, Jason 2020).

Error Control & and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender kn ows which last

data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision (Javapoint, n.d).

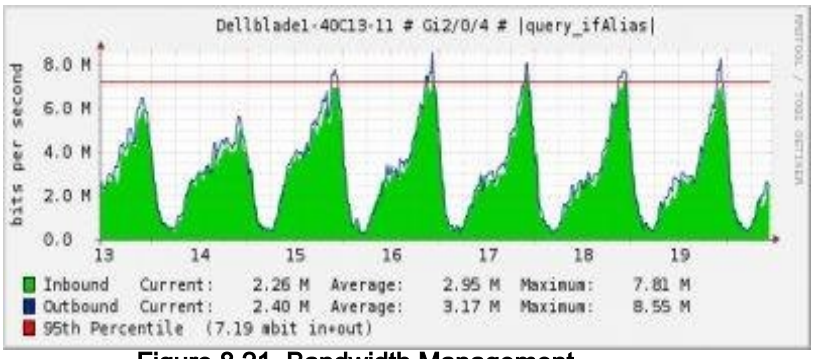


Figure 8.21. Bandwidth Management

Source: https://www.javatpoint.com/computer-network-tcp-ip-model

How is Bandwidth measured?

Bandwidth is measured in bits per second, as shown above on the left hand side of the graph – 8.0m at the largest amount. It is important to know that there is a very big difference between mega "bits" and mega "bytes" – the physical connection of your net work hardware (i.e. switch, server or router) would be measured in mega "bits" always, but traffic could be measured in megabits or megabytes per second.

Since the megabytes figure will be larger than the megabits figure (equation to follow shortly) most industry service providers like to give a total transfer based on this figure – however most bandwidth providers use megabits.

To translate bits to bytes is quite easy – there are 8 bits in a byte. In order to convert Mb (bits) into MB (bytes) divide by 8. Conversely, to convert MB into Mb multiply by 8 (Callaway, Jason 2020).

So for the example above, we see that the maximum outbound figure of 8.55 Mbs actually equates to a transfer rate of 8.55*8 = 68.4 MB per second – luckily the above server is on a giga bit connection – otherwise you would be thinking about upgrading your server network hardware.

Lesson 5. User Datagram Protocol

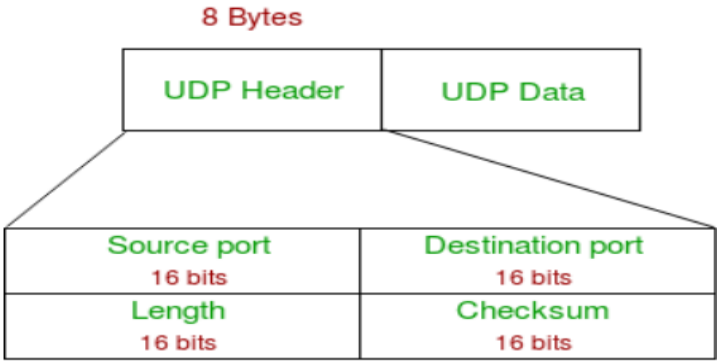
The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

UDP (User Datagram Protocol) is a connectionless protocol of the internet protocol family that operates at the transport layer and was specified in 1980 in RFC (Request for Comments) 768. As a lean and almost delay-free alternative to TCP, UDP is used for the fast transmission of data packets in IP networks (Callaway, Jason 2020).

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth (Callaway, Jason 2020).



UDP Header

UDP header is 8-bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers h elp to distinguish different user

requests or process (Callaway, Jason 2020).

- ✓ **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
- ✓ **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
- ✓ **Length :** Length is the length of UDP including header and the data. It is 16-bits field.

Checksum : Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP

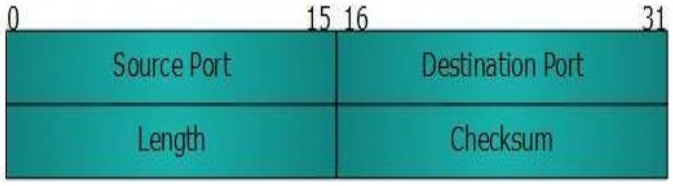


Figure 8.23. User Datagram Protocol
https://www.javatpoint.com/udp-protocol

header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets (Callaway, Jason 2020).

Applications of UDP (Callaway, Jason 2020):

- ✓ Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.

- ✓ It is suitable protocol for multicasting as UDP supports packet switching.
- ✓ UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- ✓ Normally used for real time applications which can not tolerate uneven delays between sections of a received message.
- ✓ Domain Name Services
- ✓ Simple Network Management Protocol
- ✓ Trivial File Transfer Protocol
- ✓ Routing Information Protocol
- ✓ Kerberos

Following implementations uses UDP as a transport layer protocol:

- ✓ NTP (Network Time Protocol)
- ✓ DNS (Domain Name Service)
- ✓ BOOTP, DHCP.
- ✓ NNP (Network News Protocol)
- ✓ Quote of the day protocol
- ✓ TFTP, RTSP, RIP.

Application layer can do some of the tasks through UDP (Callaway, Jason 2020)-

- ✓ Trace Route
- ✓ Record Route
- ✓ Time stamp
- UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.
- Actually UDP is null protocol if you remove checksum field.
- ✓ Reduce the requirement of computer resources.
- ✓ When using the Multicast or Broadcast to transfer.
- ✓ The transmission of Real-time packets, mainly in multimedia applications

Lesson 5.1 User Datagram Protocol Application

- ✓ The transport layer is represented by two protocols: TCP and UDP.
- ✓ The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- ✓ Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- ✓ An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- ✓ Each port is defined by a positive integer address, and it is of 16 bits (Javapoint, n.d).

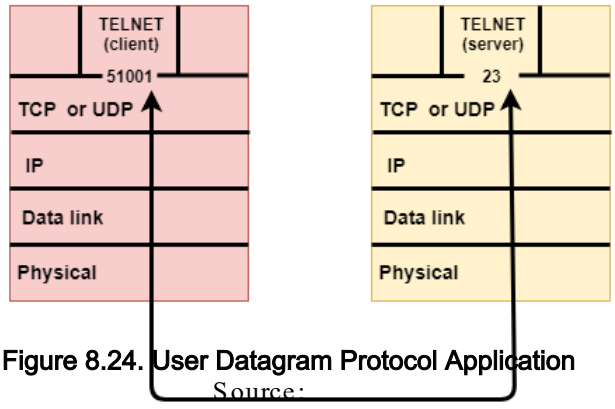


Figure 8.24. User Datagram Protocol Application

Source: https://www.javatpoint.com/udp-protocol

UDP

- UDP stands for User Datagram Protocol.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte

header which is shown below:

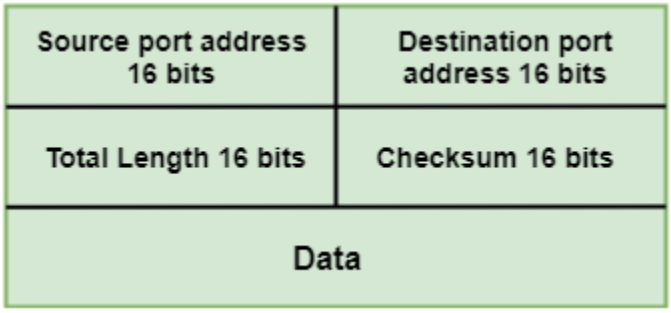


Figure 8.25. User Datagram format

Source: https://www.javatpoint.com/udp-protocol

Where,

- ✓ Source port address: It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- ✓ Destination port address: It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- ✓ Total length: It defines the total length of the user datagram in bytes. It is a 16-bit field.
- ✓ Checksum: The checksum is a 16-bit field which is used in error detection (Javapoint, n.d).

Disadvantages of UDP protocol

- ✓ UDP provides basic functions needed for the end-to-end delivery of a transmission.

- ✓ It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- ✓ UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

Assessment Task

Activity No. 1

Note that multiple computer were used to complete this activity so the addresses will not be the same for all questions.

1. Complete the following table using CMD.

	IP Address
Your computer	134.68.62.108
Your subnet mask	255.255.255.0
Your gateway	134.6862.100
Your DNS	134.68.1.9 134.68.1.2 129.79.1.1 129.79.5.100

2. When does your IP “lease” expire?
3. Which transport/network layer protocols are used by your computer?
4. What computers are used for packets traveling between the Ball State Web server (http://www.bsu.edu) and your computer? (tracert)
5. Display your computer's routing table. How many unique gateways are listed? Which of these gateway addresses also appear in our configuration data?

Activity No. 2

Objective

Internet Protocols are the core of the Internet and it is necessary to understand how these protocols work together.

1. Host IP configuration

This exercise focuses on basic IP configurations of a single host. Use the “ipconfig” utility to observe and list: Physical address (MAC address), IP address, Subnet Mask, Default Gateway, IP address of the DHCP server, when was the lease for the IP address obtained, when will the lease expire. Open a command window and type:

2. >ipconfig /all

Do it again on a different host on different subnets and fill out Table 1. Familiarize yourself with the topology of the lab network and draw a picture of the lab network; show how it is connected and what IP addresses are assigned to the network interfaces.

	Host on LAN 1	Host on LAN 2	Host on LAN 3
MAC Address			
IP Address			
Subnet Mask			
Default Gateway IP Address			
DHCP Server IP Address			
Lease obtained			
Lease expires			

3. Domain Name System (DNS)

The “nslookup” utility allows you to query DNS servers and display the mapping from IP addresses to hostnames. Before using this tool, you should be familiar with how DNS works. Nslookup works in interactive or non-interactive mode.

Determine the local hostname of your machine by typing the following:

>hostname

Write down your local hostname here: _____

4. You can run nslookup in interactive mode by typing:

>nslookup

To query the DNS server, type the hostname on the **nslookup** command prompt.

Use **nslookup** to query different hosts and fill Table

DNS Server name	Address

5.Address Resolution Protocol (ARP)

ARP is a protocol for determining the physical address (or MAC address) of a node on a local area network when only the IP address (or logical address) is known. An ARP request is sent to the network, and the node that has the IP address responds with its physical address. Although ARP technically refers only to finding the hardware address, and Reverse ARP (RARP) refers to the reverse procedure, the acronym ARP is commonly used to describe both. ARP is limited to physical network systems that support broadcast packets.

Ping some hosts on your network, the network picture will be showed on the whiteboard, to populate your ARP table. Then use the arp utility to observe the current table. Find out the hosts corresponding to the entries. On a command window type:

Delete current entries in the ARP table and start the windump utility by typing
>arp –d

>windump -n

Ping some hosts on your network and watch for the ARP Request and ARP Reply messages in the windump output and give explanation.

>arp –a

local interface IP address _____

MAC Address	IP Address	Type

Summary

The application layer is the topmost layer of the protocol hierarchy. It is the layer where actual communication is initiated. It uses the services of the transport layer, the network layer, the data link layer, and the physical layer to transfer data to a remote host. This chapter discusses some of the application layer protocols in greater detail. These application layer protocols are as follows: Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), File transfer protocol (FTP), Hypertext transfer protocol (HTTP), Simple mail transfer protocol (SMTP), and Simple network management protocol (SNMP). DHCP is defined in RFC 1541 and updated in RFC 2131. It was designed to provide a centralized approach to configuring and maintaining IP addresses. The DNS is a distributed, hierarchical database where authority flows from the top of the hierarchy downward. FTP is a standard network protocol used to transfer computer files between two hosts on a computer network. (Callaway, Jason 2020).

References

Data Communication and Computer Network Tutorial. (n.d.). https://www.tutorialspoint.com/data_communication_computer_network/index.htm

https://www.omnisci.com/technical-glossary/client-server

http://basicitnetworking.blogspot.com/2009/11/osi-layers-peer-to-peer-communications.html

https://searchnetworking.techtarget.com/definition/client-server#:~:text=Client%2Dserver%20protocols,-Clients%20typically%20communicate&text=It%20determines%20how%20to%20break,of%20all%20packets%20that%20arrive.

https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/

Computer networking and cybersecurity: a guide to understanding communications systems, internet connections, and network security along with protection from hacking and cyber security threats Author: Kiser, Quinn Copyright Date: 2020

Computer networking: a top-down approach Author: Kurose, James F. & Ross, Keith W. 2020

Computer networking for beginners: a complete guide. Callaway, Jason 2020

Computer networking: the complete beginner's guide to learning the basics of network. Author: Walker, Benjamin

2019.

MODULE 9
THE NETWORK LAYER

Introduction

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may b e operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols (Callaway, Jason 2020).

Learning Outcomes

At the end of this lesson, the student should be able to:

- ✓ Identify some of the factors driving the need for network layer
- ✓ Identify and classify particular examples of attacks
- ✓ define the terms vulnerability, threat and attack
- ✓ Identify physical points of vulnerability in simple networks
- ✓ Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

Lesson 1. What is Network Layer?

The network layer is a portion of online communications that allows for the connection transfer of data packets between different devices or networks.

The network layer is the third level (Layer 3) of the Open Systems Interconnection Model (OSI Model) and the layer that provides data routing paths for network communication. Data is transferred to the receiving device in the form of packets via logical network paths in an ordered format controlled by the network layer.

Logical connection setup, data forwarding, routing and delivery error reporting are the network layer's primary responsibilities. Layer 3 can be either able to support connection-oriented or connectionless networks (but not both of them at the same time) (Callaway, Jason 2020).

Network Layer

- ✓ The Network Layer is the third layer of the OSI model.
- ✓ It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- ✓ The network layer translates the logical addresses into physical addresses
- ✓ It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- ✓ The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are (Callaway, Jason 2020):

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.

- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Forwarding & Routing

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded (Javapoint, n.d).

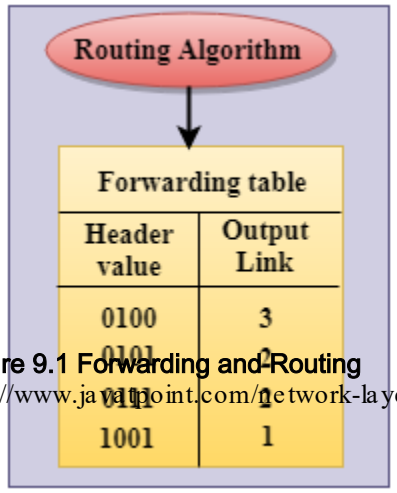
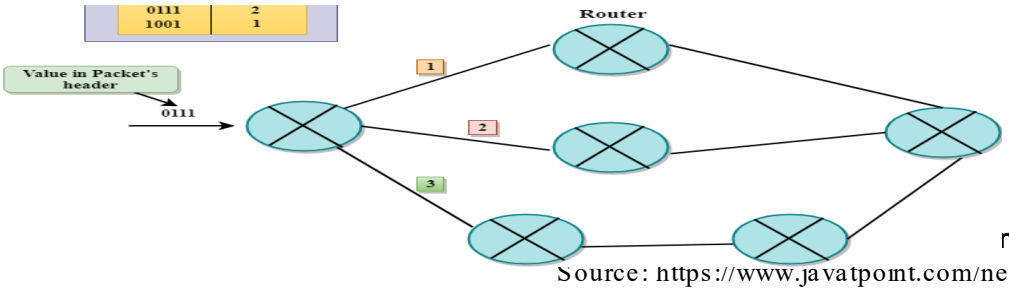


Figure 9.1 Forwarding and Routing
Source: https://www.javatpoint.com/network-layer



ng table
Source: https://www.javatpoint.com/network-layer

Figure 9.1 Forwarding and Routing
Source: https://www.javatpoint.com/network-layer

example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.

Services Provided by the Network Layer

✓ **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.

- ✓ **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- ✓ **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- ✓ **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- ✓ **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services (Javatpoint, n.d).

Lesson 1.1 Network Addressing

A network address is any logical or physical address that uniquely distinguishes a network node or device over a computer or telecommunications network. It is a numeric/symbolic number or address that is assigned to any device that seeks access to or is part of a network (Callaway, Jason 2020).

- ✓ Network Addressing is one of the major responsibilities of the network layer.
- ✓ Network addresses are always logical, i.e., software-based addresses.
- ✓ A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- ✓ A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- ✓ Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

There are different kinds of network addresses in existence (Callaway, Jason 2020):

- ✓ IP

- ✓ IPX
- ✓ AppleTalk

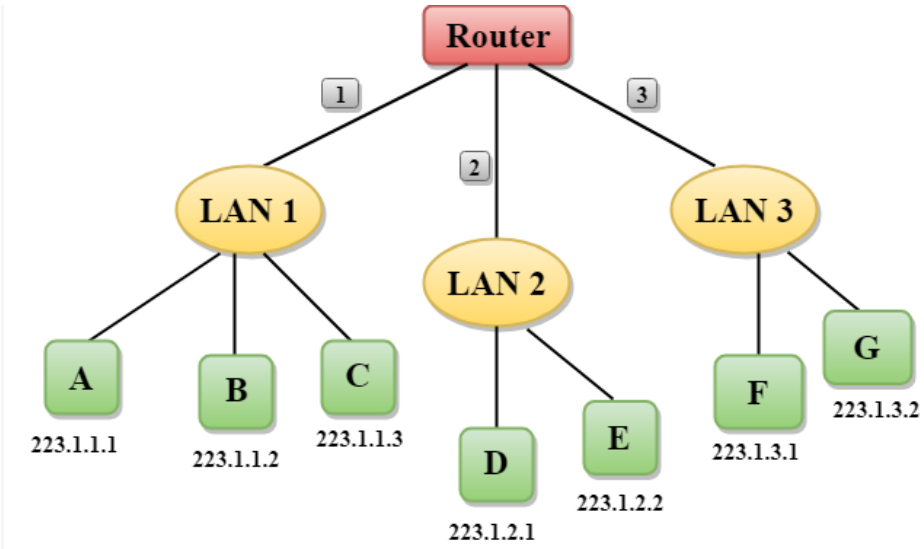


Figure 9.3 The network addressing
Source: https://www.javatpoint.com/network-layer

- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network (Javatpoint, n.d).

Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes (Callaway, Jason 2020):

- ✓ Class A
- ✓ Class B
- ✓ Class C
- ✓ Class D
- ✓ Class E

IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network.The host which needs to communicate outside its subnet, needs to know dest ination network address, where the packet/data is to be sent (Callaway, Jason 2020).

Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all

its packet to its gateway. A gateway is a router equipped with all the information which leads to route packets to the destination host (Callaway, Jason 2020).

An ip address is divided into two parts (Callaway, Jason 2020):

- ✓ **Network ID:** It represents the number of networks.
- ✓ **Host ID:** It represents the number of hosts.

In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class (Callaway, Jason 2020).

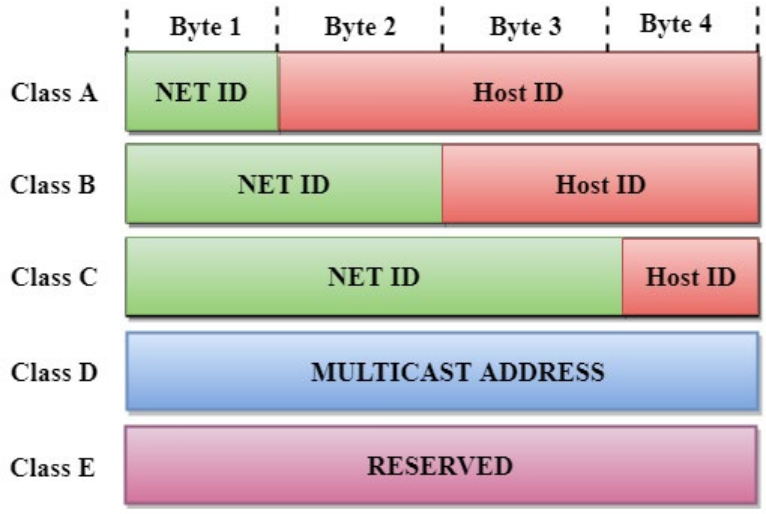


Figure 9.4 The network addressing category
Source: https://www.javatpoint.com/network-layer

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts (Javatpoint, n.d).

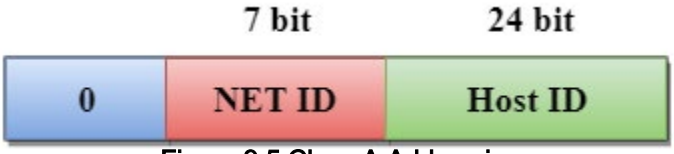


Figure 9.5 Class A Addressing

- ✓ The network ID is 8 bits long.
- ✓ The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

- ✓ The total number of networks in Class A = 2^7 = 128 network address
- ✓ The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small -sized to large-sized networks (Javatpoint, n.d).

- ✓ The Network ID is 16 bits long.
- ✓ The Host ID is 16 bits long.

Figure 9.6 Class B Addressing
Source: javatpoint.com/network-addressing

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

- ✓ The total number of networks in Class B = 2^{14} = 16384 network address

- ✓ The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks (Javatpoint, n.d).

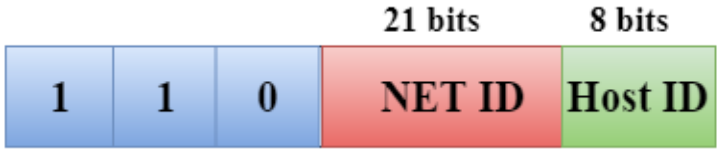


Figure 9.7 Class C Addressing
Source: javatpoint.com/network-addressing

- ✓ The Network ID is 24 bits long.
- ✓ The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

- ✓ The total number of networks = 2^{21} = 2097152 network address
- ✓ The total number of hosts = 2^{8} - 2 = 254 host address

Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network (Javatpoint, n.d).

Figure 9.8 Class D Addressing
Source: javatpoint.com/network-addressing

Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network (Javatpoint, n.d).

Figure 9.9 Class D Addressing
Source: javatpoint.com/network-addressing

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- ✓ The Host ID must be unique within any network.
- ✓ The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.

- ✓ The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- ✓ The network ID cannot start with 127 as 127 is used by Class A.
- ✓ The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- ✓ The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Figure 9.10 Classful Network Architecture
Source: javatpoint.com/network-addressing

Lesson 1.2 Network Routing

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes.The software based routers have limited functionality and limited scope (Tutorialpoint, n.d).

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information (Tutorialpoint, n.d):

- ✓ Hop Count

- ✓ Bandwidth
- ✓ Metric
- ✓ Prefix-length
- ✓ Delay

Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator (Javatpoint, n.d).

- ✓ **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- ✓ **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- ✓ **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.

- ✓ **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- ✓ **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator (Javatpoint, n.d).

Types of Routing

Routing can be classified into three categories (Javatpoint, n.d):

- Static Routing
- Default Routing
- Dynamic Routing

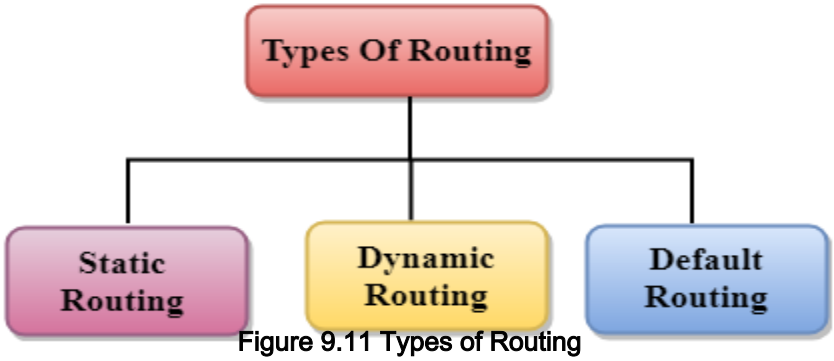


Figure 9.11 Types of Routing
Source: https://www.javatpoint.com/computer-network-routing

Static Routing

- ✓ Static Routing is also known as Nonadaptive Routing.
- ✓ It is a technique in which the administrator manually adds the routes in a routing table.
- ✓ A Router can send the packets for the destination along the route defined by the administrator.
- ✓ In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages of Static Routing

Following are the advantages of Static Routing:

- ✓ **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- ✓ **Bandwidth** : It has not bandwidth usage between the routers.
- ✓ **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing (Javatpoint, n.d):

- ✓ For a large network, it becomes a very difficult task to add each route manually to the routing table.
- ✓ The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing (Javatpoint, n.d.)

- ✓ Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- ✓ Default Routing is used when networks deal with the single exit point.
- ✓ It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- ✓ When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing (Javatpoint, n.d.)

- ✓ It is also known as Adaptive Routing.
- ✓ It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- ✓ Dynamic protocols are used to discover the new routes to reach the destination.
- ✓ In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- ✓ If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features (Javatpoint, n.d.):

- ✓ All the routers must have the same dynamic routing protocol in order to exchange the routes.
- ✓ If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing (Javatpoint, n.d.):

- ✓ It is easier to configure.
- ✓ It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing (Javatpoint, n.d.):

- ✓ It is more expensive in terms of CPU and bandwidth usage.
- ✓ It is less secure as compared to default and static routing.

Lesson 1.3 Unicast Routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It

is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

Unicast Routing Protocols

There are two kinds of routing protocols available to route unicast packets:

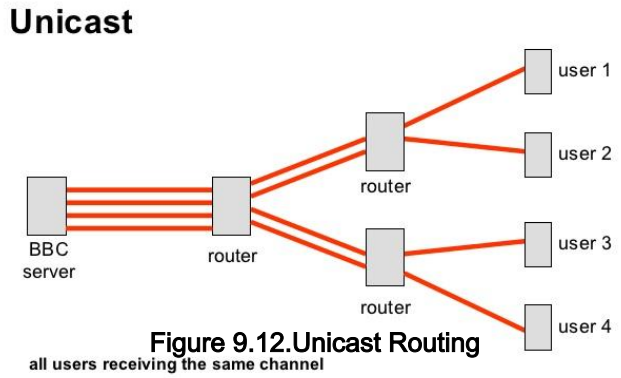


Figure 9.12.Unicast Routing

https://www.javatpoint.com/computer-network-routing

Distance Vector Routing Protocol

Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ul timately, all routers build up their network topology based on the advertisements of their peer routers,

For example Routing Information Protocol (RIP).

Link State Routing Protocol

Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then calculate their best path for routing purposes. For example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS) (Callaway, Jason 2020).

Lesson 1.4 Broadcast Routing

In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicastrouting, the data is sent to only nodes which wants to receive the packets. The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward (Javatpoint, n.d).

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be

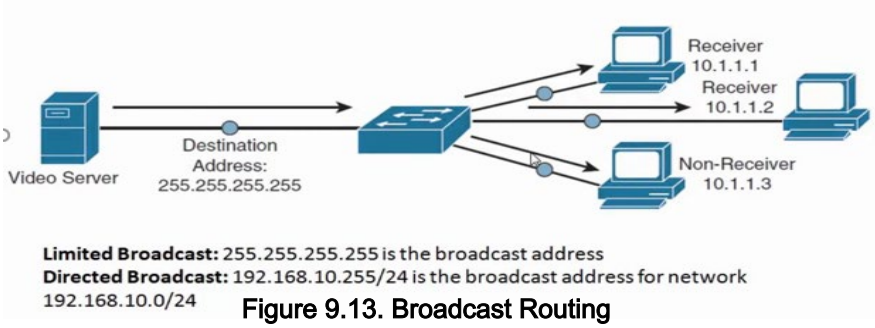


Figure 9.13. Broadcast Routing

https://
images.

configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- ✓ A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

This method consumes lots of bandwidth and router must destination address of each node.

- ✓ Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.

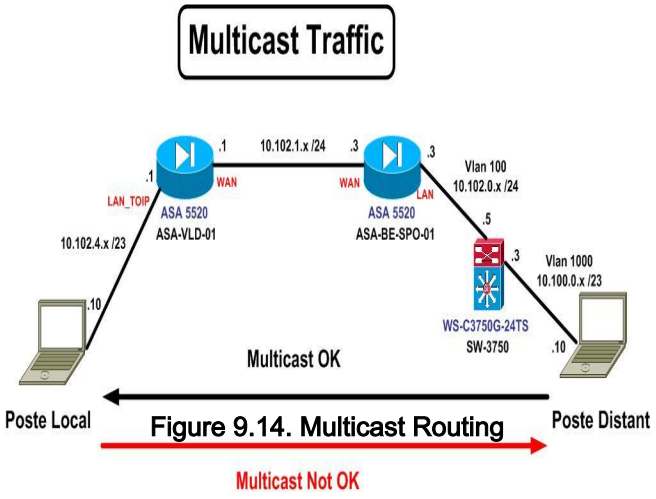


Figure 9.14. Multicast Routing

Lesson 1.5 Multicast Routing

Multicast routing is a networking method for efficient distribution of one-to-many traffic. A multicast source, such as a live video conference, sends traffic in one stream to a multicast group. The multicast group contains receivers such as computers, devices, and IP phones. Multicast routing is special case of broadcast routing with significance difference and challenges.

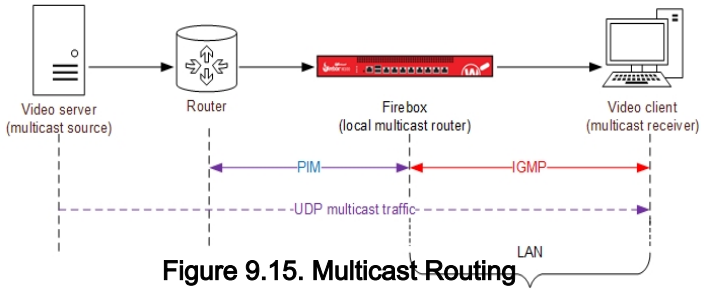


Figure 9.15. Multicast Routing

https://images.app.goo.gl/TrTAP5uFNfQaCP6EA

In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets (Callaway, Jason 2020).

How It Works?

Multicast routing uses the Protocol -Independent Multicast (PIM) protocol. There are different variants of this protocol. Your Firebox supports PIM Sparse Mode (PIM -SM) which is used when only a few devices subscribe to the multicast. These devices are multicast receivers (Javatpoint, n.d).

Receivers can be located anywhere in the world, on any network, and compose the multicast group logical group.

In this diagram, a server sends multicast traffic through a router and the Firebox. The Firebox forwards the multicast traffic to the multicast group on the local network.

In PIM-SM mode, the central point in the multicast domain is the Rendezvous Point (RP). The RP is a router that receives multicast traffic destined for the multicast group. All multicast traffic must pass through the RP.

You must enable all Firebox interfaces as RP candidates that are involved in multicast routing, except those exposed to the multicast source or the receivers. When you enable the Firebox as an RP candidate, the Firebox periodically communicates its RP candidacy to the PIM -SM network. RP elections on the Firebox occur dynamically.

After you enable multicast routing, the aliasAny-Multicast and two new policies are added to your configuration:

- ✓ MR-PIM-Allow
- ✓ MR-IGMP-Allow

In a multicast policy, you can specify only these options:

- Incoming interfaces
- Source IP addresses
- Destination IP addresses
- Protocols and ports

Interfaces

Multicast routing is supported for these Firebox interface types:

- Physical
- VLAN
- Bridge
- Link aggregation
- Wireless
- BOVPN virtual interface

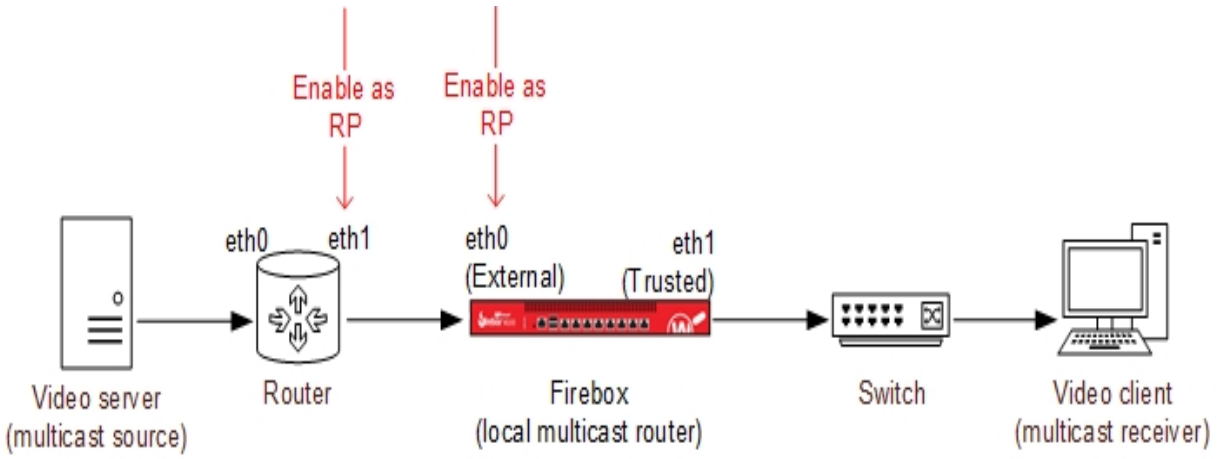


Figure 9.16. Multicast Routing

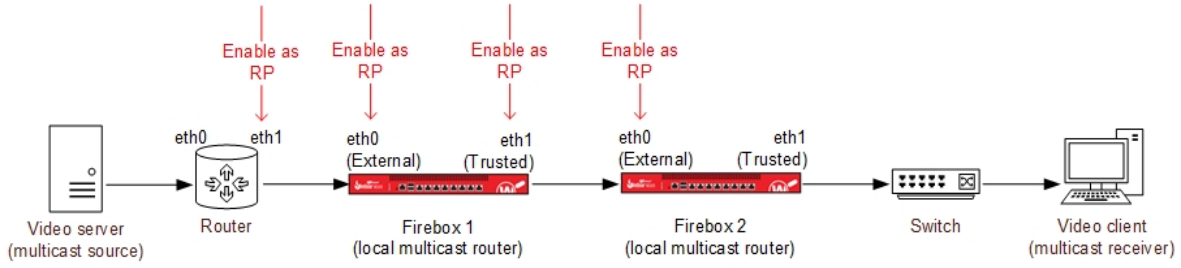
https://images.app.goo.gl/xoJYHv6iPorm4qEp7

Example 1

In this example, the local network has one Firebox configured for multicast routing. The external interface, eth0, is enabled as an RP candidate. On the router, the interface connected to the Firebox, eth1, is also enabled as an RP candidate.

Example 2

In this example, the local network has two Fireboxes configured for multicast routing. The external interfaces on both Fireboxes, eth0, are enabled as RP candidates. The trusted



https://images.app.goo.gl/xoJYHv6iPorm4qEp7

Figure 9.17. Multicast Routing

interface on Firebox 1 is also enabled as an RPcandidate. On the router, the interface connected to the Firebox, eth1, is also enabled as an RP candidate.

The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops (Javatpoint, n.d).

Lesson 1.6 Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology. Anycast is a network addressing and routing methodology in which a single destination address has multiple routing paths to two or more endpoint destinations. Routers will select the

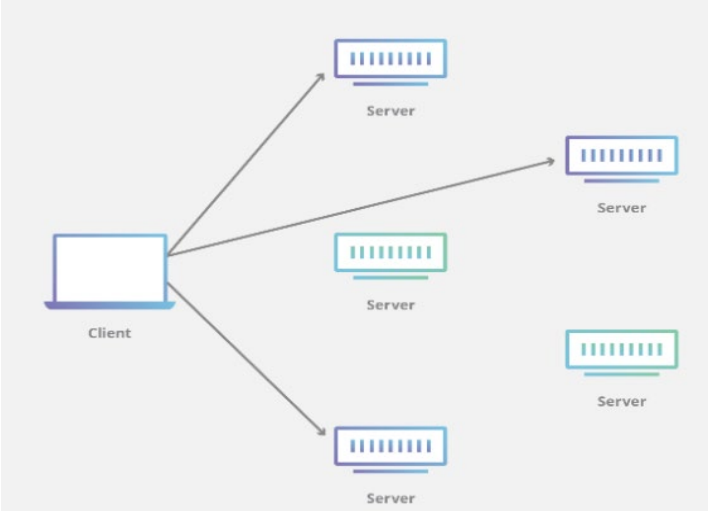


Figure 9.18. Anycast Routing

https://images.app.goo.gl/2AiCpxDTAYrmu8q38

desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route (Javatpoint, n.d).

How does Anycast Work?

Anycast network routing is able to route incoming connection requests across multiple data centers. When requests come into a single IP address associated with the Anycast network, the network distributes the data based on some prioritization methodology.The selection process behind choosing a particular data center will typically be optimized to reduce latency by selecting the data center with the shortest distance from the requester. Anycast is characterized by a 1-to-1 of many association, and is one of the 5 main network protocol methods used in the Internet protocol.

Why Use an Anycast Network?

If many requests are made simultaneously to the same origin server , the server may become overwhelmed with traffic and be unable to respond efficiently to additional incoming requests. With an Anycast network, instead of one origin server taking the brunt of the traffic, the

load can also be spread across other available data centers, each of which will have servers capable of processing and responding to the incoming request. This routing method can prevent an origin server from extending capacity and avoids service interruptions to clients requesting content from the origin server (Javatpoint, n.d).

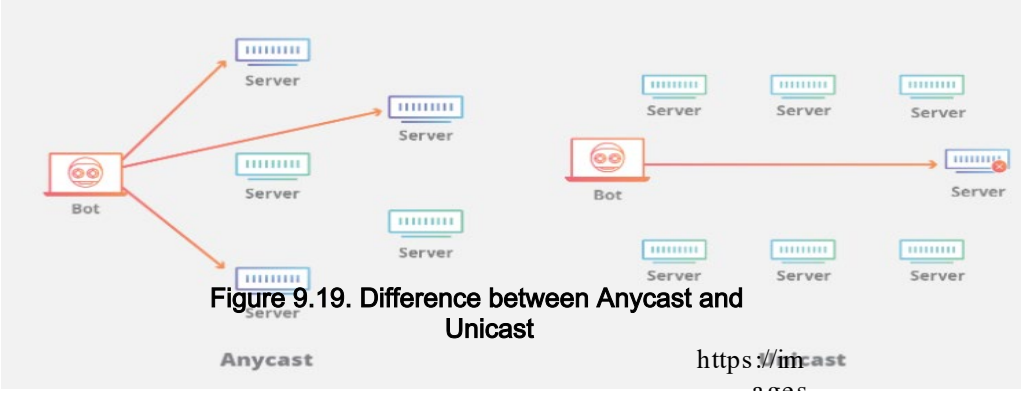


Figure 9.19. Difference between Anycast and Unicast

https://im ages

What is the Difference between Anycast and Unicast?

Most of the Internet works via a routing scheme called Unicast. Under Unicast, every node on the network gets a unique IP address. Home and office networks use Unicast; when a computer is connected to a wireless network and gets a message saying the IP address is already in use, an IP address conflict has occurred because another computer on the same Unicast network is already using the same IP. In most cases, that isn't allowed.

Lesson 2. Internetworking

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking. Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme. In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol (Javatpoint, n.d).

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that functions as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internetworks (Javatpoint, n.d).

To enable communication, every individual network node or phase is designed with similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP).

Once a network communicates with another network having constant communication procedures, it's called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is associate degree example of Internetworking. Internetworking is enforced in Layer three (Network Layer) of OSI-ISO model. The foremost notable example of internetworking is that the Internet (Javatpoint, n.d).

There are chiefly 3 unit of Internetworking:

- Extranet
- Intranet
- Internet

✓ **Extranet** – It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one refer ence to associate degree external network.

✓ **Intranet** – This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP -based tools akin to web browsers and FTP tools, that's underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browseable data.

✓ **Internet** – A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that management assignments (Javatpoint, n.d).

Lesson 2.1 Tunneling

In computer networks, a tunneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communications to be sent across a public network (such as the Internet) through a process called encapsulation. Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through

unnoticed. A technique of internetworking called Tunneling is used when source and destination networks of same type are to be connected through a network of different type. For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:

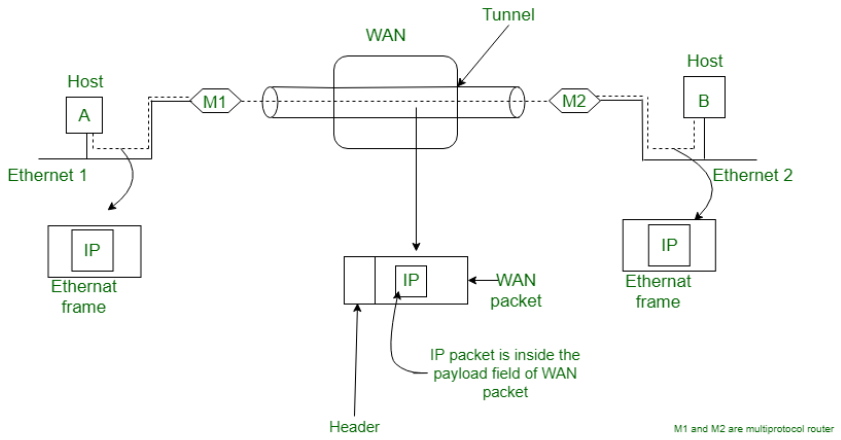


Figure 9.20. The Tunneling

Tunneling

https://images.app.goo.gl/95xWCjSDRr7M5Lj4A

When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

The task is sent on an IP packet from host A of Ethernet-1 to the host B of ethernet-2 via a WAN.

Sequence of events:

- ✓ Host A construct a packet which contains the IP address of Host B.
- ✓ It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1
- ✓ Host A then puts this frame on Ethernet.
- ✓ When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and send it to host B in an Ethernet frame (Javatpoint, n.d).

Why is this Technique called Tunneling?

In this particular example, the IP packet does not have to deal with WAN. The host A and B also do not have to deal with the WAN. The multiprotocol routers M1 and M2 will have to understand about IP and WAN packets. Therefore, the WAN can be imagined to beequivalent to a big tunnel extending between multiprotocol routers M1 and M2 and the technique is called Tunneling.

Lesson 2.2 Packet Fragmentation

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

If a packet with DF (don't fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time (Javatpoint, n.d).

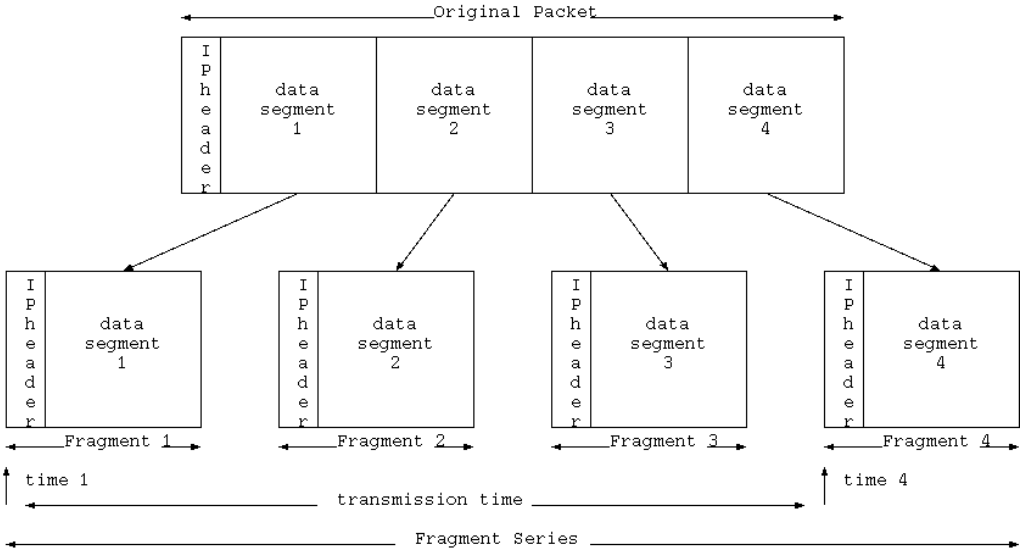


Figure 9.21. The Fragmentation
https://images.app.goo.gl/9ywGufDn1HtZFBAC6

Lesson 3. Network Layer Protocol

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network:

access method, allowed physical topologies, types of cabling, and speed of data transfer. Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the Open Systems Interface (OSI) model proposed by ISO.

Lesson 3.1 Address Resolution Protocol ARP

TCP/IP supports the following protocols:

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

- ✓ ARP stands for Address Resolution Protocol.
- ✓ It is used to associate an IP address with the MAC address.
- ✓ Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

How ARP works

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the i ntended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender (Javatpoint, n.d).

Steps taken by ARP protocol

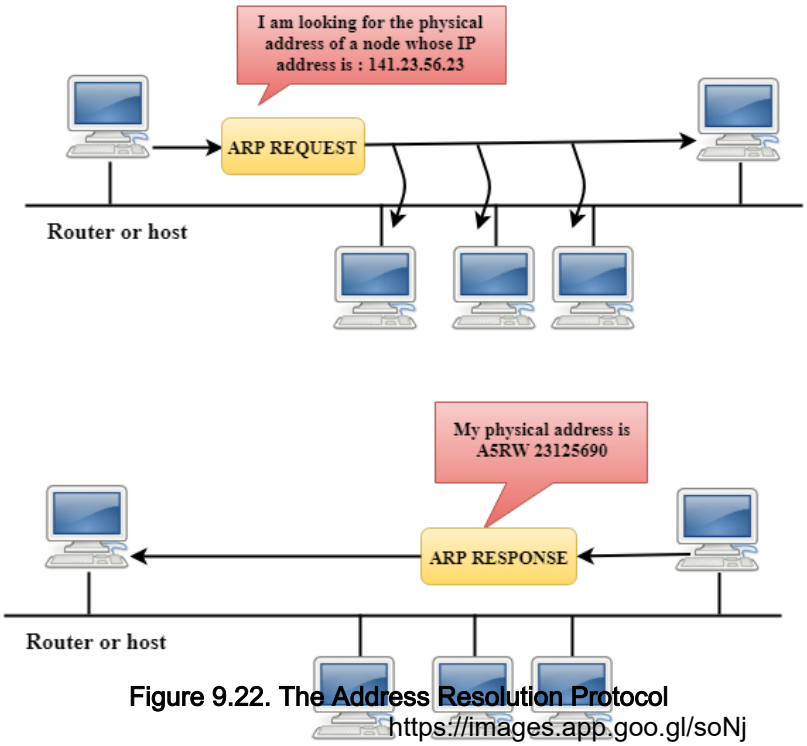
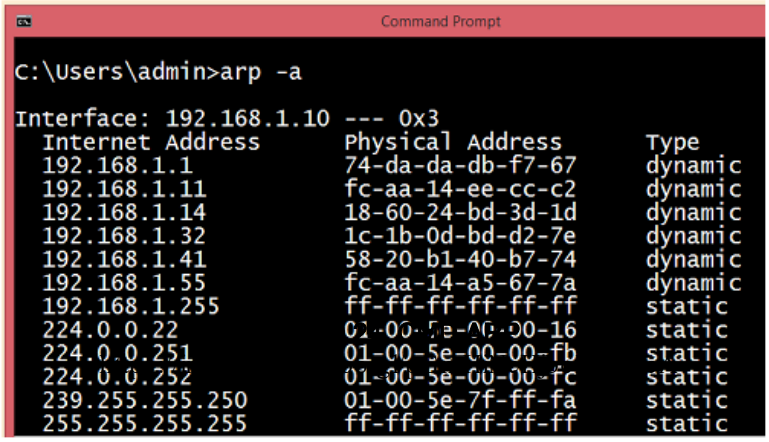


Figure 9.22. The Address Resolution Protocol
https://images.app.goo.gl/soNjX1Q6tXhbKKYn8

- ✓ If a device wants to communicate with another device, the following steps are taken by the device:
- ✓ The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.

- ✓ If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
- ✓ The device that has the matching IP address will then respond back to the sender with its MAC address
- ✓ Once the MAC address is received by the device, then the communication can take place between two devices.
- ✓ If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.



There are two entries types of ARP (Javatpoint, n.d):

Dynamic entry: It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.

Static entry: It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility (Javatpoint, n.d).

Lesson 3.2 Internet Control Message – ICM

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP (Javatpoint, n.d).

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages (Javatpoint, n.d).

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem (Javatpoint, n.d).

- ✓ ICMP stands for Internet Control Message Protocol.
- ✓ The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ✓ ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ✓ ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- ✓ An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ✓ ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ✓ ICMP messages are transmitted within IP datagram.

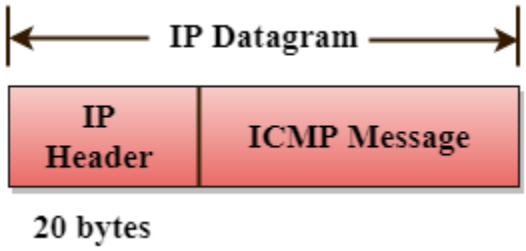


Figure 9.25. ICM Message
https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

The Format of an ICMP message

- ✓ The first field specifies the type of the message.
- ✓ The second field specifies the reason for a particular message type.
- ✓ The checksum field covers the entire ICMP message.

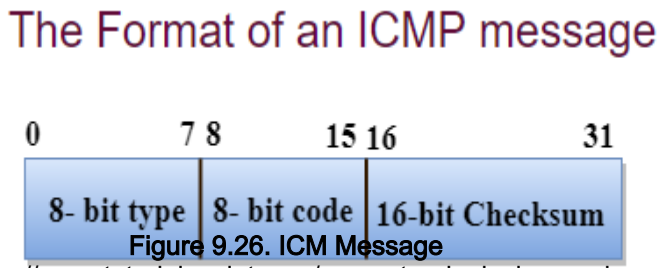


Figure 9.26. ICM Message
https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Error Reporting

ICMP protocol reports the error messages to the sender.

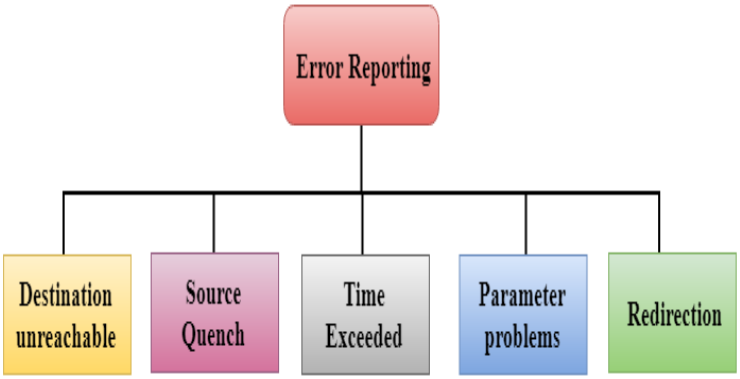


Figure 9.27. Error Reporting Message

Five types of errors are handled by the ICMP protocol:

- ✓ Destination unreachable
- ✓ Source Quench
- ✓ Time Exceeded
- ✓ Parameter problems
- ✓ Redirection

Destination unreachable: The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.

Source Quench: The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.

Time Exceeded: Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

Parameter problems: When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.

Redirection: Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table (Javatpoint, n.d).

Lesson 3.3 Internet Protocol Version 4 – Ipv4

Pv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

Class A - it uses first octet for network addresses and last three octets for host addressing

Class B - it uses first two octets for network addresses and last two for host addressing

Class C - it uses first three octets for network addresses and last one for host addressing

Class D - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.

Class E - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Lesson 3.4 Internet Protocol Version 4 – Ipv6

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other (Javatpoint, n.d).

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- ✓ Dual stack implementation
- ✓ Tunneling
- ✓ NAT-PT

Lesson 4. Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link (Javatpoint, n.d).

Following services are provided by the Data Link Layer (Javatpoint, n.d)**:**

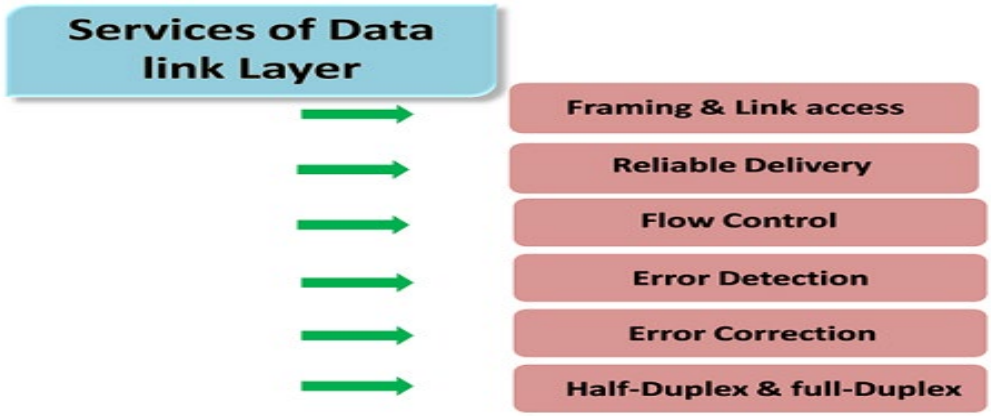


Figure 9.29. Data Link Layer Services

https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Framing & Link access : Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structu re of the frame as well as a channel access protocol by which frame is to be transmitted over the link.

Reliable delivery: Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable deliver y service over the

links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.

Flow control: A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the s ending node on one side of the link from overwhelming the receiving node on another side of the link.

Error detection: Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.

Error correction: Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.

Half-Duplex & Full -Duplex: In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half -Duplex mode, only one node can transmit the data at the same time (Javatpoint, n.d).

Lesson 4.1 Functionality of Data Link Layer

Data link layer does many tasks on behalf of upper layer. These are (Javatpoint, n.d):

Framing

Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

Addressing

Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

Synchronization

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Error Control

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

Flow Control

Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

Multi -Access

When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems (Javatpoint, n.d).

Lesson 4.2 Error Detection and Correction

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted (Javatpoint, n.d).

Lesson 4.3 Types of Errors

Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

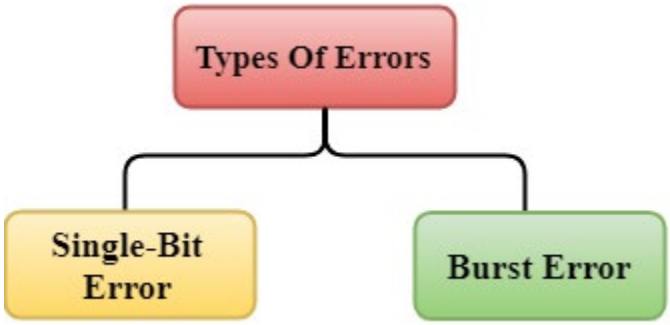


Figure 9.30. Types of Errors
https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Single -Bit Error:

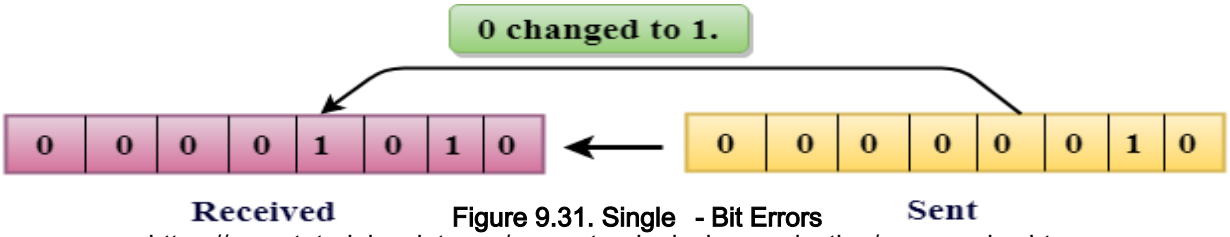


Figure 9.31. Single - Bit Errors
https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1 (Javatpoint, n.d).

- In the above figure, the message which is sent is corrupted as single -bit, i.e., 0 bit is changed to 1.
- Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

- Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte (Javatpoint, n.d).

Burst Error (Javatpoint, n.d):

- The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.
- The Burst Error is determined from the first corrupted bit to the last corrupted bit.

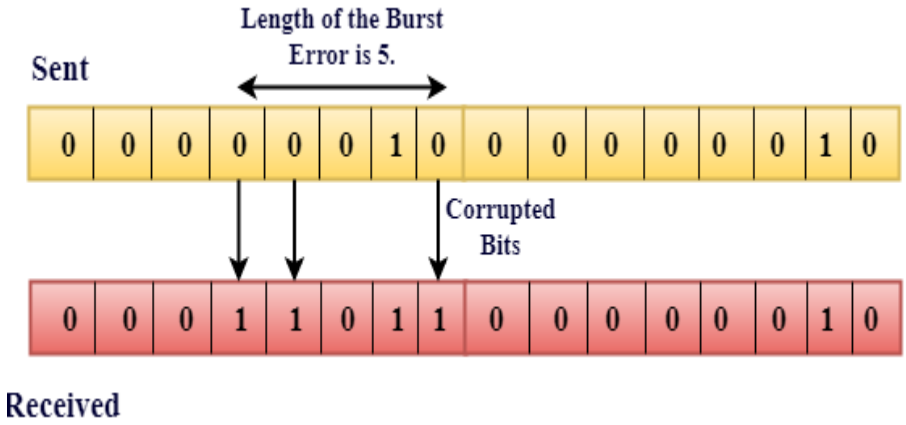


Figure 9.32. Burst Errors

https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

- The duration of noise in Burst Error is more than the duration of noise in Single-Bit.
- Burst Errors are most likely to occur in Serial Data Transmission.
- The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques (Javatpoint, n.d):

- The most popular Error Detecting Techniques are:
- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Lesson 4.4 Error Detection

Error detection is the process of detecting the errors that are present in the data transmitted from transmitter to receiver, in a communication system. We use some redundancy codes to detect these errors, by adding to the data while it is transmitted from source (transmitter) (Javatpoint, n.d).

A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message. Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors (Javatpoint, n.d).

Some popular techniques for error detection are (Javatpoint, n.d):

- Simple Parity check
- Two-dimensional Parity check
- Checksum
- Cyclic redundancy check

Lesson 4.5 Error Correction

Error correction is the process of detecting errors in transmitted messages and reconstructing the original error-free data. Error correction ensures that corrected and error-free messages are obtained at the receiver side.

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver (Javatpoint, n.d).

Error Correction can be handled in two ways (Javatpoint, n.d):

- Backward error correction : Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- Forward error correction: In this case, the receiver uses the error-correcting code which automatically corrects the errors. A single additional bit can detect the error, but cannot correct it. For correcting the errors, one has to know the exact position of the error. For example, if we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits (Javatpoint, n.d).

Lesson 5. Data Link Control and Protocol

A data link control protocol must prevent data loss caused by mismatched sending/receiving capacities. A flow control procedure, usually a simple sliding window mechanism, provides this function. Data link control protocols must provide transparent data transfer.

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half -duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs (Javatpoint, n.d).

The Data link layer provides three functions:

- ✓ Line discipline
- ✓ Flow Control
- ✓ Error Control

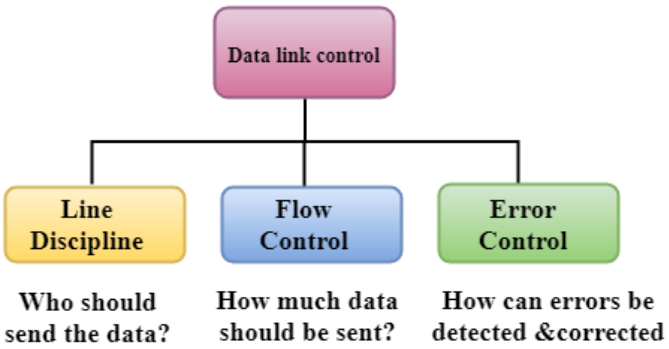


Figure 9.33. Data Control Protocol
https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Line Discipline

Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways (Javatpoint, n.d):

- ✓ ENQ/ACK
- ✓ Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one (Javatpoint, n.d).

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiveris unable to accept the transmission.

Following are the responses of the

receiver (Javatpoint, n.d) :

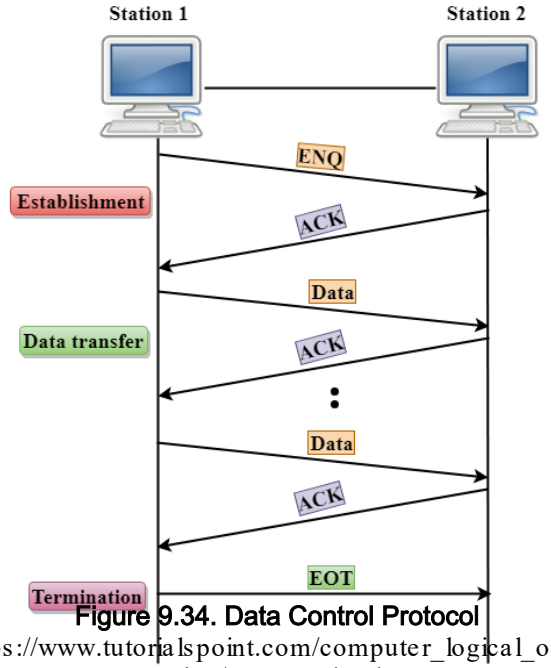


Figure 9.34. Data Control Protocol

https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

- ✓ If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame. If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- ✓ If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.

Lesson 5.1 Flow Control (Javatpoint, n.d)

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data (Javatpoint, n.d):

- ✓ Stop-and-wait
- ✓ Sliding window

Stop-and-wait

- ✓ In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.

- ✓ When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop -and-wait

- The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop -and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link (Javatpoint, n.d).

Sliding Window (Javatpoint, n.d)

- ✓ The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- ✓ In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- ✓ A single ACK acknowledge multiple frames.
- ✓ Sliding Window refers to imaginary boxes at both the sender and receiver end.
- ✓ The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- ✓ Frames can be acknowledged even when the window is not completely filled.
- ✓ The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- ✓ The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- ✓ When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window (Javatpoint, n.d)

- ✓ At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- ✓ Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

✓ For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).

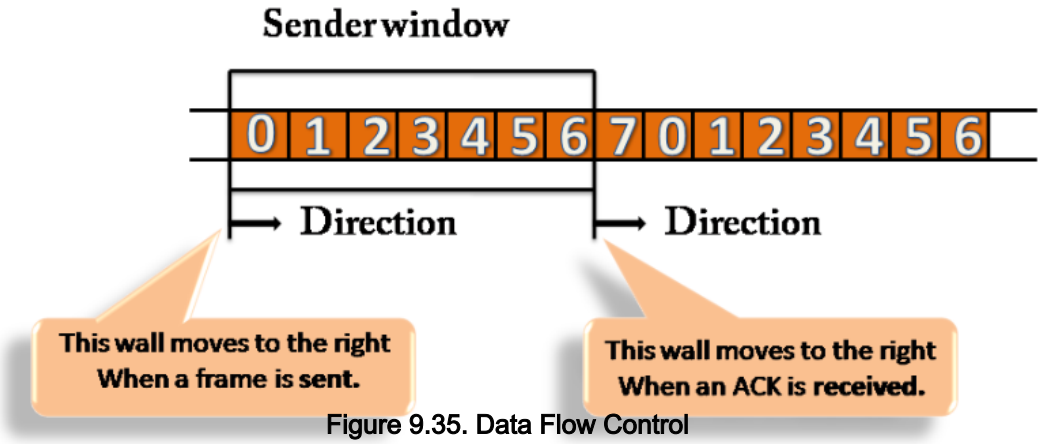


Figure 9.35. Data Flow Control

https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Lesson 5.2 Error Control

Error Control is a technique of error detection and retransmission (Javatpoint, n.d).

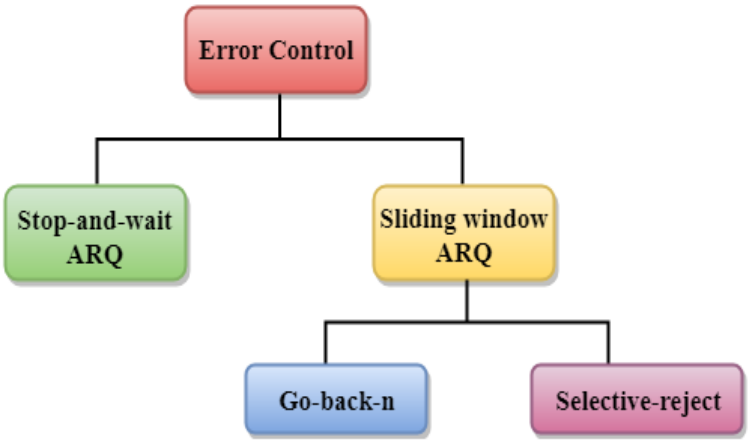


Figure 9.36. Categories of Error Control

Stop-and-wait ARQ (Javatpoint, n.d)

- ✓ Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.
- ✓ This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission (Javatpoint, n.d):

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission (Javatpoint, n.d):

- Damaged Frame: When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- Lost Frame: Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ (Javatpoint, n.d)

- ✓ SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission (Javatpoint, n.d):

- ✓ In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- ✓ The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

✓ The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

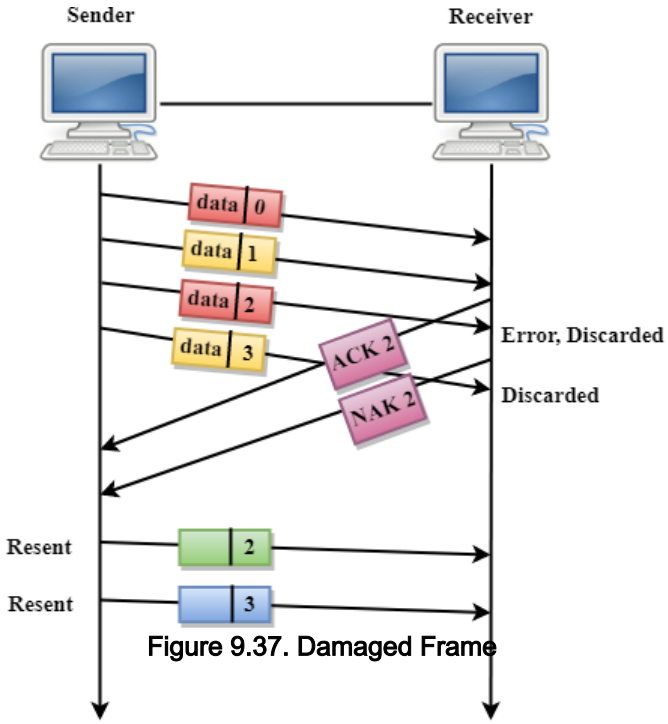


Figure 9.37. Damaged Frame

Two protocols used in sliding window ARQ:

- Go-Back-n ARQ: In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

Damaged Frame: When the frame is damaged, then the receiver sends a NAK frame.

In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

Lost Data Frame: In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.

Lost Acknowledgement: The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective -Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.

- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

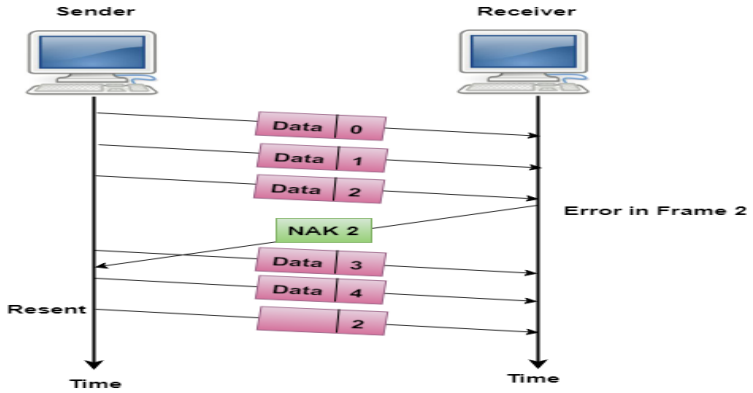


Figure 9.38. Selective – Reject ARQ

https://www.tutorialspoint.com/computer_logical_organization/error_codes.htm

Assessment Task

Activity No. 1

Explain each.

1. What is the data link address of your computer? (ipconfig /all)

_____
_____
_____
_____
_____
_____

2. List other data link addresses known to your computer? (arp -a)

_____
_____
_____
_____
_____
_____

3. Which data link layer protocols are in use on your computer? (Control Panel)

4. Approximately how many bytes have been transferred by your computer this session? (netstat -e)

5. How many errors has you computer encountered this session? (netstat -e)

6. How many broadcast (i.e., non-unicast) messages has your computer processed this session? (netstat -e)

7. Compare the functions of a MAC level bridge with an IP router. In what circumstances is it more appropriate to use one than the other?

8. Discuss the tables inside both bridges and routers used to control the acceptance and forwarding of packets. Indicate both how these tables are used and how information is put in the tables. How quickly can the tables be searched in each case?

_____
_____
_____
_____
_____
_____
_____

9. What features might be added to a router or bridge to improve some aspects of network security?

_____
_____
_____
_____
_____
_____

Activity No. 2 IPv4 and IPv6

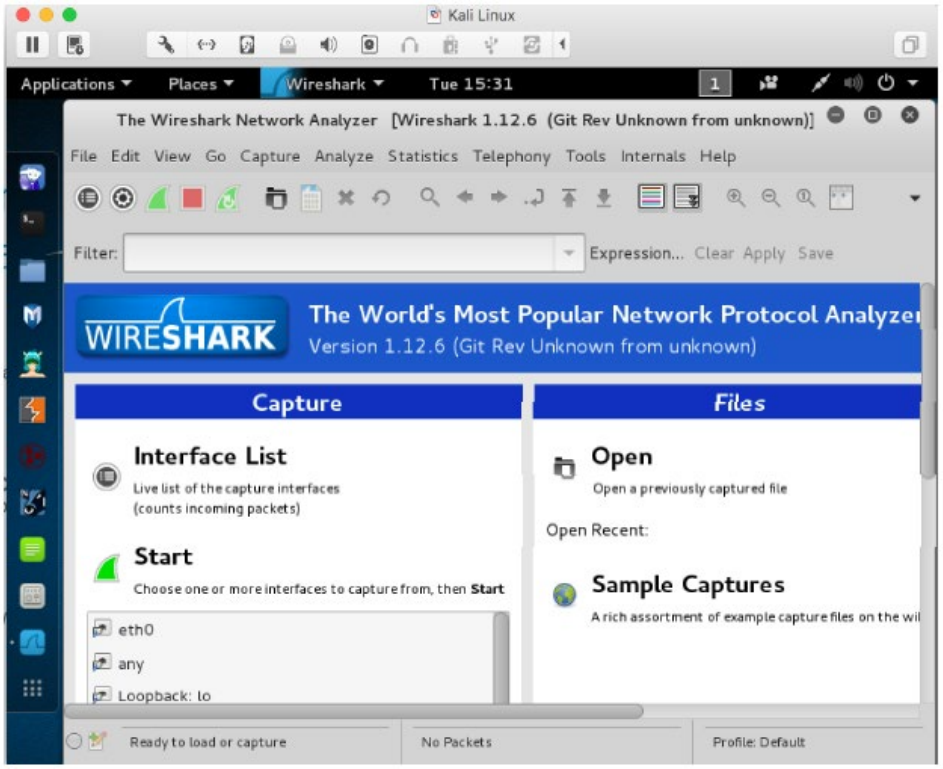
1. Draw the structure of an IPv4 packet and an IPv6 packet. Briefly describe the purpose of each IP header field. (You might want to make use of Wireshark to examine some real-life IP headers.)

https://www.wireshark.org/download.html

Introduction

The first part of the lab introduces packet sniffer, Wireshark. Wireshark is a free opensource

network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture andoffline analysis, three-pane packet browser, coloring rules for analysis. This document uses Wireshark for the experiments, and it covers Wireshark installation, packet capturing, and protocol analysis.



2. Where in this structure would you look to find a link-layer header (e.g. Ethernet) and a transport-layer header (e.g. TCP)?

_____
_____
_____
_____
_____
_____
_____

3. Automatic configuration is the process by which a host obtains an IP address and other details necessary to communicate at the network layer.

_____
_____
_____
_____
_____
_____
_____

4. Explain the protocol used for IPv4 autoconfiguration.

_____
_____
_____
_____
_____
_____
_____

5. List the two mechanisms which could be used for IPv6 autoconfiguration, and explain the differences and motivations behind each. [3 marks] (This may go beyond the course material, but you should do a little research!)

_____
_____
_____
_____
_____
_____
_____

6. In each case make sure to state the configuration details which are likely to be managed by these mechanisms.

_____
_____
_____
_____
_____
_____
_____

Activity No. 3 Part 1

1. Determine the correct class of the following IP addresses:

Address	Class?
191.107.10	
172.16.16.15	
200.200.5.2	
3.3.57.0	
131.107.2.89	

2. Which address class (es) will allow you to have more than 1000 hosts per network?

_____
_____
_____
_____
_____

_____

3. Which address class (es) will allow only 254 hosts per network?

_____
_____
_____
_____
_____
_____
_____

Part 2

Circle the portion of the IP address that would be invalid if it were assigned to a host, and then explain why it is invalid:

- 131.107.256.80
- 222.222.255.222
- 0.127.4.100
- 190.7.2.0
- 127.1.1.1
- 198.121.254.255
- 255.255.255.255

Part 3

Determine the Network ID, First Valid Host, Last Valid Host, and Broadcast ID of the following network address/mask pairs:

- 192.168.1.134/27
- 160.150.140.130/18

Summary

In this chapter, you learned:

- The network layer, or OSI Layer 3, provides service to allow end devices to exchange data across the network.
- The network layer uses four basic process: IP addressing for end devices, encapsulation, routing and de – encapsulation.
- The internet largely based on IPv4, which is still be the most widely – used network layer protocol.
- An IPv4 packet contains the IP header on the payload.

- The IPv6 simplified header offers several advantages over IPv4, including better routing efficiency, simplified extension headers, capabilities and capability for per – flow processing.
- Network layer protocols like IP, IPX and DDP provide data encapsulation, logical addressing, fragmentation and reassembly.
- There are three classes of IP address, Class A. Class B and Class C

References

- *Data Communication and Computer Network Tutorial*. (n.d.). https://www.tutorialspoint.com/data_communication_computer_network/index.htm
- https://www.omnisci.com/technical-glossary/client-server
- http://basicitnetworking.blogspot.com/2009/11/osi-layers-peer-to-peer-communications.html
- https://searchnetworking.techtarget.com/definition/client-server#:~:text=Client%2Dserver%20protocols,-Clients%20typically%20communicate&text=It%20determines%20how%20to%20break,of%20all%20packets%20that%20arrive.
- https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/
- Computer networking and cybersecurity: a guide to understanding communications systems, internet connections, and network security along with protection from hacking and cyber security threats Author: Kiser, Quinn Copyright Date: 2020
-
- Computer networking: a top-down approach Author: Kurose, James F. & Ross, Keith W. 2020
-
- Computer networking for beginners: a complete guide. Callaway, Jason 2020
-
- Computer networking: the complete beginner's guide to learning the basics of network. Author: Walker, Benjamin 2019.

MODULE 10
GETTING STARTED WITH CLIENT – SERVER MODEL

Introduction

Client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server host runs one or more server programs, which share their resources with clients. A client does not share any of its resources, but it requests content or service from a server. Clients, therefore, initiate communication sessions with servers, which await incoming requests. Examples of computer

applications that use the client-server model are email, network printing, and the World Wide Web (Callaway, Jason 2020).

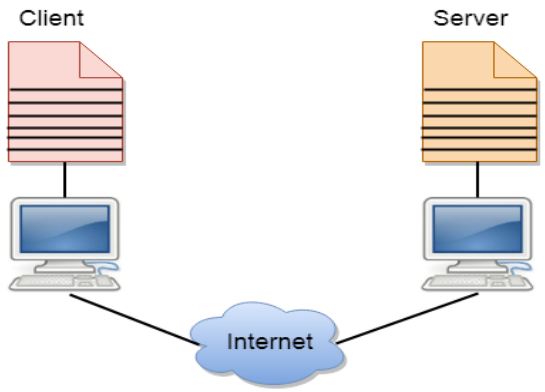
Learning Outcomes

At the end of this lesson, the student should be able to:

- Explain the client-server model of networked computers.
- Give examples of applications which use the client-server model.
- Describe what is meant by the World Wide Web (WWW) and the Internet Explain how hardware is used to support the Internet: networks, routers, gateways, servers.
- Explain how communication systems are used to support the Internet: The Public Service Telephone Network (PSTN), dedicated lines, cell phone network Explain the benefits and drawbacks of using copper cable, fibre- optic cabling, radio waves, microwaves, satellites.

Lesson 1. Client and Server Model

- Client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:



https://www.wireshark.org/download.html

- An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

Client

✓ A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

✓ A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

Advantages of Client -server networks:

Centralized: Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.

Security: These networks are more secure as all the shared resources are centrally administered.

Performance: The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.

Scalability: We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

Disadvantages of Client -Server network:

✓ Traffic Congestion is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.

✓ It does not have a robustness of a network, i.e., when the server is down, then the client requests cannot be met.

- ✓ A client/server network is very decisive. Sometimes, regular computer hardware does not serve a certain number of clients. In such situations, specific hardware is required at the server side to complete the work.
- ✓ Sometimes the resources exist in the server but may not exist in the client. For example, If the application is web, then we cannot take the print out directly on printers without taking out the print view window on the web.

Lesson 1.1 Building a Client Server

When you have finished installing Microsoft Windows Server 2008 R2, a window titled Initial Configuration Tasks may come up:

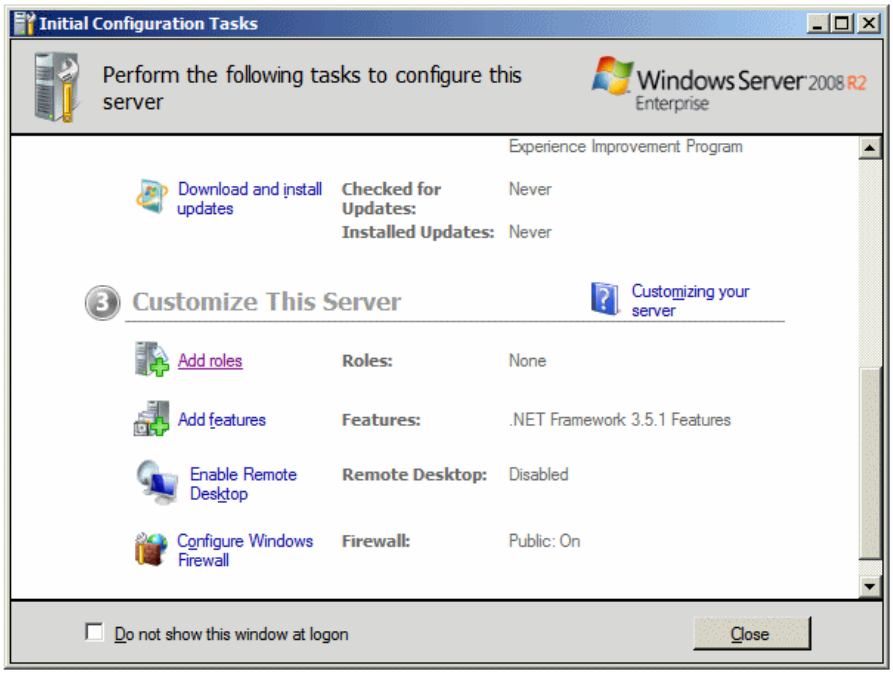


Figure 10.2. Client Server Configurations

The Initial Configuration Tasks window is used to perform the most fundamental or routine operations of Microsoft Windows Server 2008 R2. This window displays when the computer starts. If you don't want to come up like that, click the bottom check box. If it doesn't come up when the computer starts, to restore this window,**click Start -> Run**, type **oobe** and **press Enter** .

After installing the operating system, there are a few things you should (must) do before continuing:

- ✓ You must make sure the computer is connected to the Internet
- ✓ If this is the first computer, you must make it a domain controller (this is not a requirement if the computer will not be a domain controller; if you don't (yet) know what a domain controller is, don't worry about that now)

Lesson 1.2 Configurations Client Server

The Server name

Every computer in the network must have a name. The installation gives a default name that you can accept or change. Some installations, such as Small Business Server, prompt you to accept or specify the name of the server. After installing Microsoft Windows Server 2008, to check and/or change the name of the server:

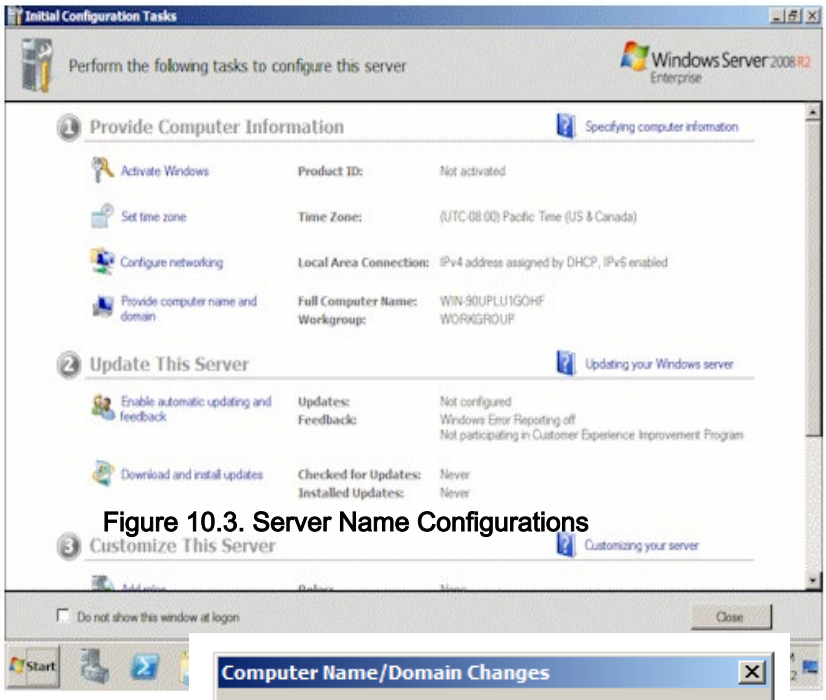


Figure 10.3. Server Name Configurations

- ✓ In the Initial Configuration Tasks window, click Provide Computer Name and Domain:
- ✓ In the Computer Name property page, click Change
- ✓ Accept or change the name of the server
- ✓ Click OK
- ✓ A dialog box will ask you to restart your computer. Click OK

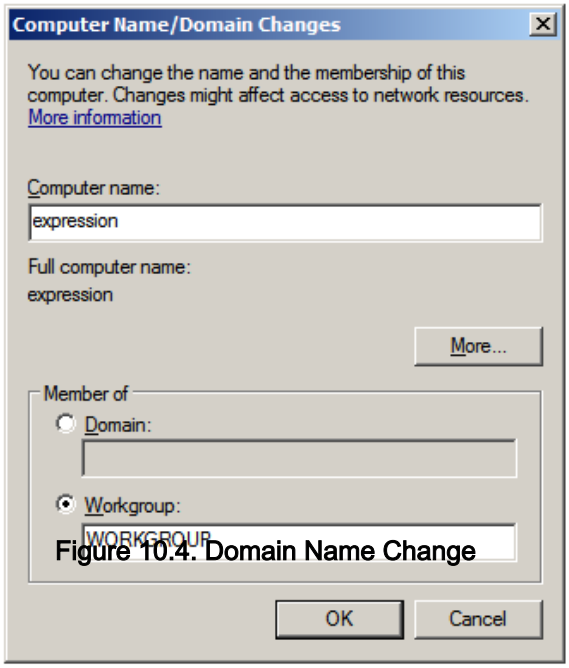


Figure 10.4. Domain Name Change

- ✓ Click Close
- ✓ Click Restart Now

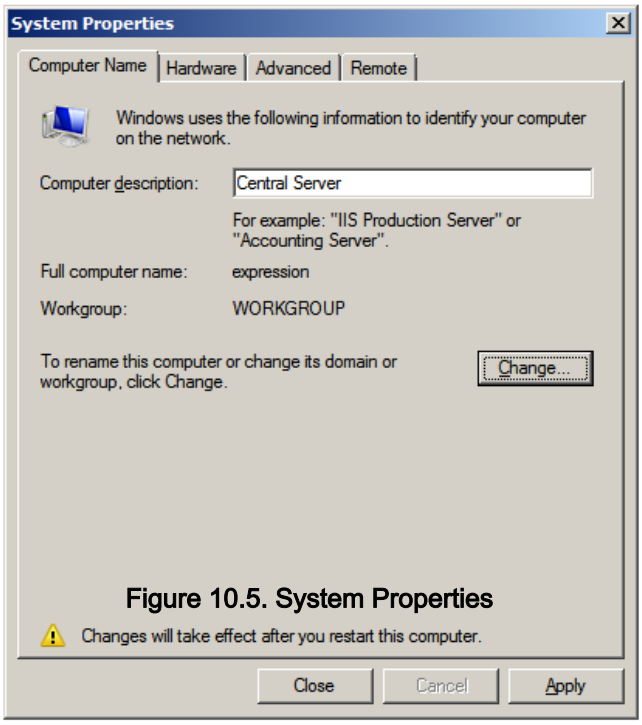


Figure 10.5. System Properties

Lesson 1.3 File Sharing

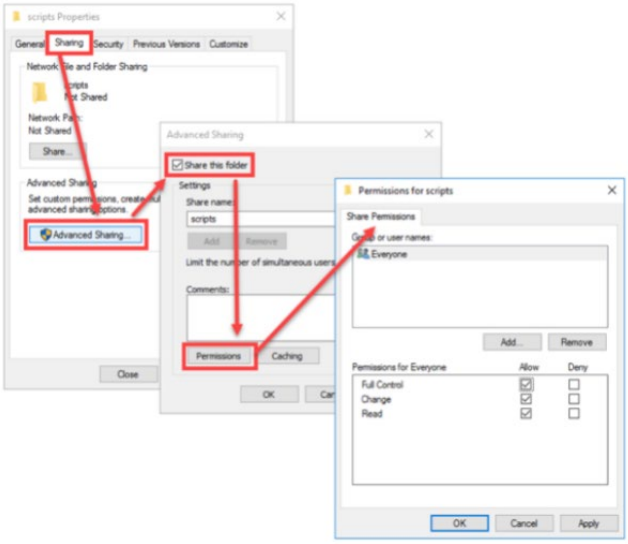
File sharing is the practice of distributing or providing access to digital media, such as computer programs, multimedia (audio, images and video), documents or electronic books. File sharing may be achieved in a number of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers on computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking.

The term "file share" in Windows Server is a bit of a misnomer. After all, you can't share individual files, but only folders or disk volumes. Windows Server uses the Server Message Block (SMB) file-sharing protocol and the File and Printer Sharing for Microsoft Networks component (also known as the Server service) to perform file sharing.

Let's review some ways to get the job done in Windows Server 2016. Recall that Windows has two types of permissions available for file system resources:

- ✓ **Shared folder permissions:** These permissions control network access to a folder or disk volume
- ✓ **NTFS permissions:** These permissions apply to local or remote access, and can be applied to individual files as well as folders or disk volumes

File Explorer



https://www.wireshark.org/download.html

The method that's familiar to most Windows systems administrators is to right -click the target folder, select Properties from the shortcut menu, and navigate to the Sharing tab. You then click Advanced Sharing, enable Share this folder, and click Permissio ns to adjust the folder's access control list (ACL).

Figure 10.6. File Sharing

Lesson 1.4 Restrictions

Under a client-server model, the main drawback is the chance of a system overload due to not having sufficient supplies to serve all the clients. If too many distinct clients try to reach the shared network at the same time, there may be a crash or a slowing down of the connection. Moreover, if the network is down, this impairs access to the information from any site or client wherever. This can be harmful to important businesses that are incapable to reach their appropriate data.

Network and Server Security

Security is usually considered only in terms of preserving software. But, any security plan should be hierarchical at each level. Servers must be placed in secure, access-controlled surroundings. Only authorized staff should be permitted to manage and control it.

Typically, server security is the supervising of the path to the database server itself. The server must be connected to a constant power supply that gives alternate power if there's a difficulty with the supply. This allows the server to shut down in a way that preserves data and creates the slightest amount of harm. They should comply with market standards in password policy to guard database access.

Encryption also preserves data through superior DES (Data Encryption Standard) mechanisms or cryptograms. The degree of encryption depends on state standards. Database servers should not be noticeable to the world.

For security and performance concerns, the database backend should not be on the same machine as the web server with its open links. To secure the database, the server should be configured to allow only granted IP addresses. If the database is a backend for a web server, the IP address of the web server should be the only one that can reach the database server. Another security gap in servers arises from more dynamic applications that permit online upgrades and can infiltrate the database server.

Networks are exposed to trespassers watch networks that can hold delicate business information, passwords, and other likely company flaws. Secure networks should adhere to four principles that form a 'trusted computing base' (TCB). These are:

- Identification, authorization,
- Discretionary control
- Audit, and
- Object re-utilization

Here's a tutorial video link from YouTube:

https://study.com/academy/lesson/what-is-a-client-server-network-definition-advantages-disadvantages.html

Assessment Task

Activity No. 1:

1. RMI stands for?

a. Remote Mail Invocation
b. Remote Message Invocation
c. Remaining Method Invocation
d. Remote Method Invocation

2. A remote object is an object whose method can be invoked from another virtual environment.
   a. True
   b. False
3. A typical _____ program creates some remote objects, makes references to these objects accessible, and waits for clients to invoke methods on these objects.
   a. Server
   b. Client
   c. Thread
   d. Concurrent
4. A typical _____ program obtains a remote reference to one or more remote objects on a server and then invokes methods on them.

a. Server
b. Client
c. Thread
d. Concurrent

5. The _____ layer, which provides the interface that client and server application objects use to interact with each other.

a. Increasing
b. Count
c. Bit
d. Stub/Skeleton

6. A layer which is the binary data protocol layer.

a. Stub layer
b. Skeleton layer
c. Remote layer
d. Transport protocol

7. A middleware layer between the stub skeleton and transport.

a. Remote layer
b. Instruction layer
c. Reference layer
d. Remote reference layer

8. An object acting as a gateway for the client side.

a. Skeleton
b. Stub
c. Remote
d. Server

9. A gateway for the server side object.

a. Skeleton
b. Stub
c. Remote
d. Server

10. RMI uses stub and skeleton for communication with the _____ object.

a. Client
b. Remote
c. Server
d. Any

Activity No. 2:

Explain each.

1. How to validate MAC address using regular expression?

2. What is basic network attacks in computer network?

3. What is Computer network?

4. What is the difference between the block filter devices and add simple security for router configuration?

5. What are the advantage and disadvantage of secret key encryption?

Summary

The client-server model describes how a server provides resources and services to one or more clients. Examples of servers include web servers, mail servers, and file servers. Most servers have a one -to-many relationship with clients, meaning a single server can provide resources to multiple clients at one time.

References

- https://www.geeksforgeeks.org/mac-filtering-in-computer-network/
- *DCN - Computer Network Types - Tutorialspoint*. (n.d.). Retrieved August 25, 2020, from
- https://www.tutorialspoint.com/data_communication_computer_network/computer_network_types.htm
- https://apachebooster.com/blog/what-is-client-server-network-advantages-and-limitations/#:~:text=Limitations%20of%20Client%2DServer%20Network,slowing%20down%20of%20the%20connection.
- https://www.javatpoint.com/computer-network-client-and-server-model
- Computer networking and cybersecurity: a guide to understanding communications systems, internet connections, and network security along with protection from hacking and cyber security threats Author: Kiser, Quinn Copyright Date: 2020
-
- Computer networking: a top-down approach Author: Kurose, James F. & Ross, Keith W. 2020
-
- Computer networking for beginners: a complete guide. Callaway, Jason 2020
-
- Computer networking: the complete beginner's guide to learning the basics of network. Author: Walker, Benjamin
- 2019.

- END OF THE FINAL TERM MODULE -

CHECK YOUR EXAM SCHEDULE FOR THIS COURSE.

DO NOT FORGET TO TAKE THE EXAM AS SCHEDULED.

THANK YOU AND GOD BLESS