
# Open University *of* Mauritius

# Network

# Technologies

# Contents

## 1.1 Introduction

For anyone who wants to be well-versed in computer networks, it is imperative for him/her to understand the 7-Layer Open Systems Interconnections Reference Model (for short, OSI RM). A reference model is a conceptual blueprint of how communications should take place. It addresses all the processes required for effective communications and divides these processes into logical groupings called layers. Vendors design network products based on the specifications of the OSI model. It provides a description of how network hardware and software work together in a layered fashion to make communications possible. It also helps with troubleshooting by providing a frame of reference that describes how components are supposed to function.

## 1.2 Unit Objectives

- Recognise the history of OSI reference model,
- Be able to distinguish among reference model, protocol and layers,
- Explore the principles in designing the OSI model,
- Differentiate between client and peer-to-peer model,
- Describe the various layers of making up the OSI reference model,
- Understand various tasks and functions of the layers in the OSI layer,
- Explain the need for data encapsulation and de-encapsulation,
- Explore the difference between frame check sequence and cyclic redundancy check,
- Outline the difference between connection-oriented and connectionless network services,
- Derive the requirements needed for the implementation of connectionless services.

## 1.3 Principles needed for the OSI model

The OSI version has seven layers. The standards that have been implemented to reach on the seven layers may be in brief summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Most networks are arranged as a stack of layers or levels, each one constructed on top of the one before it, to reduce design complexity. From network to network, the number of layers, the names of each layer, the contents of each layer, and the function of each layer varies. Each layer's objective is to provide certain services to upper layers while hiding them from the intricacies of how the services are really implemented. A dialogue takes place between layer n on one machine and layer n on another machine. The layer n protocol refers to the set of rules and conventions employed in this communication. A protocol, in its simplest form, is an agreement between communicating parties about how communication should proceed. In practice, no data is transported directly from layer n on one system to layer n on another. Instead, until the lowest layer (physical layer) is reached, each layer transfers data and control information to the layer immediately below it.

Below layer 1 is the physical medium through which actual communication occurs. In Figure 1.1, virtual communication is shown by dotted lines and physical communication by solid lines.

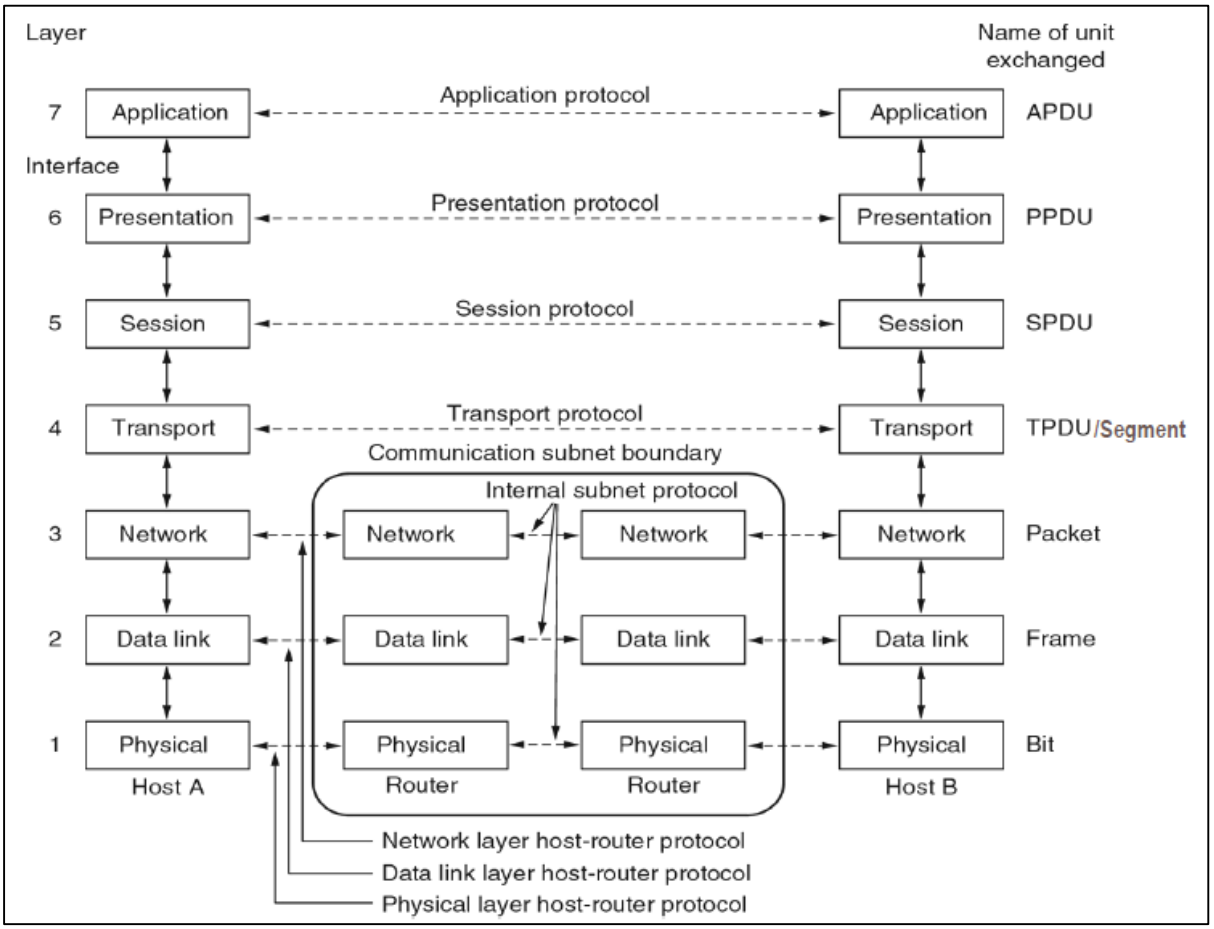



**Figure 1.1 – Virtual communication in OSI model**

The OSI Reference Model (RM) is a collection of rules that application developers can utilize to construct and implement network applications. It also serves as a foundation for developing and deploying networking standards, devices, and internetworking schemes. The OSI RM is made up of seven levels that are separated into two groups. The top three layers (Application, Presentation, and Session) establish how end-station programs interact with one another (and with users). They are in charge of apps that communicate between hosts. None of these layers have any knowledge of networking or network addresses, for example. These are the four bottom levels' responsibilities. The bottom four layers (Transport, Network, Data Link, and Physical) determine how data is sent from point A to point B.

## 1.4 The Physical Layer

Raw bits are transmitted via a communication channel by the physical layer. The electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating networking systems are defined by the physical layer.

Voltage levels, voltage change timing, physical data speeds, maximum transmission distances, and physical connectors are all defined by physical layer requirements. Physical-layer implementations fall into one of two categories: LAN or WAN.

Functions of the physical layer:

- Moves bits between devices
- Specifies voltage, wire speed and pin-out cables.
- Determine how many pins the network connector has and what each pin is used for.

To recall the layers (from top to bottom): **All People Seem To Need Data Processing.**

## 1.5 The Data Link Layer

The data link layer's major job is to take a raw transmission facility (a medium) and turn it into a line that looks to the network layer to be free of undetected transmission defects. In order to achieve this, the incoming data is divided into frames (typically a few hundred or a few thousand bytes). The frames are then sent out in order, with the receiver sending back acknowledgment frames. The data connection layer ensures that data is transported reliably via a physical network link.

Physical addressing, network topology, error warning, frame sequencing, and flow control are among the network and protocol characteristics defined by different data link layer specifications.

- **Physical addressing** (as opposed to networking addressing) defines how devices are addressed at the data link layer.
- **Network topology** consists of the data-link layer specifications that often define how devices are to be physically connected, such as in a bus, star or a ring topology.
- **Error notification** alerts upper-layer protocols that a transmission error has occurred.
- **Sequencing of data frames** reorders frames that are transmitted out of sequence.
- **Flow control** moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

### 1.5.1 Functions of the data link layer:

- Combines packets into bytes and then bytes into frames.
- Create and to recognize frame boundaries - typically by attaching special bit patterns to the beginning and end of the frame.
- Provides access to media using **MAC address***.
- Performs error detection (not correction!).

#### 1.5.1.1 MAC Address (Hardware address/Ethernet address/Physical address)

- MAC is short for Media Access Control. The MAC address is the hardware address that uniquely identifies a network device or a node (normally a Network Interface Card, called NIC) on the network. Every NIC has a UNIQUE MAC address.
- Note: A MAC Address is not the same thing as an IP address! The address currently has the format: xx-xx-xx-xx-xx-xx. The first 3 octets of the address is the manufacturer's Organizationally Unique Identifier (OUI).

## 1.6 The Network Layer

The network layer's primary responsibility is to determine how data can be transferred from source to destination, as well as to provide routing and related operations that allow many data lines to be merged into an internetwork. The logical addressing (IP address as opposed to physical addressing - MAC address) of devices does this. From higher-layer protocols, the network layer allows both connection-oriented and connectionless services. Routing protocols are commonly implemented at the network layer, although other protocols can also be implemented there.

### 1.6.1 Functions of the network layer:

- Provides logical addressing, which routers use for path determination.
- To control congestion.
- To do accounting.
- To allow interconnection of heterogeneous networks.

## 1.7 The Transport Layer

This is in charge of packet processing. Ensures that the delivery is error-free. Messages are repackaged, divided into smaller packets (data is fragmented and reassembled), and error management is handled. It also ensures appropriate sequencing and avoids duplication and loss. In the event of faulty transmissions, takes corrective action and recognizes that data has been successfully received.

### 1.7.1 Functions of the transport layer:

- **Flow control -** manages data management between devices so that the transmitting device does not send more data than the receiving device can process.
- **Multiplexing -** enables data from several applications to be transmitted onto a single physical link.
- **Virtual circuit management -** are established, maintained, and terminated by the transport layer.
- **Error checking and recovery -** involves creating various mechanisms for detecting transmission errors, while **error recovery** involves taking an action, such as requesting that data be retransmitted, to resolve any errors

## 1.8 The Session Layer

Users on various machines can establish sessions with each other via the session layer. In some apps, a session allows for better services. The session layer creates, manages, and ends communication sessions between entities in the presentation layer. Service requests and replies are exchanged between apps on separate network devices during communication sessions. Protocols deployed at the session layer coordinate these requests and responses.

### 1.8.1 Functions of the session layer:

- Dialog control - session can allow traffic to go in both directions at the same time or in only one direction at a time. If traffic can go only in one way at a time, the session layer can help to keep track of whose turn it is.
- Token management - for some protocols it is essential that both sides do not attempt the same operation at the same time. The session layer provides tokens that can be exchanged. Only the side holding the token may perform the critical action.
- Synchronization - by inserting checkpoints into the data stream the layer eliminates problems with potential crashes at long operations. After a crash, only the data transferred after the last checkpoint have to be repeated.

## 1.9 The Presentation Layer

Application layer data is subjected to a range of coding and conversion functions provided by the presentation layer. These functions ensure that information provided from one system's application is readable by another system's application. Common data representation formats, conversion of character representation formats, common data compression methods, and common data encryption schemes are all examples of presentation layer coding and conversion systems.

- Common/standard data representation formats or the use of standard image, sound and video formats enable the interchange of application data between different types of computer systems.
- Conversion of character schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII.
- Common/standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination.
- Common/Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

### 1.9.1 Functions of the presentation layer:

- It is concerned with the syntax and semantics of the information transmitted.
- Presents data.
- Handles processing such as encryption etc.

## 1.10 The Application Layer

The application layer is the OSI layer nearest to the end user, which means that both the OSI applications layer and the user interact with the software program directly. This layer communicates with software programs that use a communication component. The OSI model does not apply to such application programs. Identifying communication partners, evaluating resource availability, and synchronizing communication are all common application-layer operations. A piece of software must be built to map the functions of the network virtual terminal onto the real terminal for each terminal type. The application layer contains all of the virtual terminal software. File transfer is another application layer function. It must deal with a variety of file system incompatibilities on various PCs. Electronic mail, remote job entry, and directory lookup are just a few of the application layer's features.

## 1.11 Summary of the OSI RM

| LAYERS | FUNCTIONS | CORRESPONDING PROCOTOLS |
|---|---|---|
| Application | Provide services to applications | HTTP, SMTP, FTP, NFS, Telnet, SMB |
| Presentation | Formatting, Compression, Encryption | JPEG, MIDI, MPEG etc etc |
| Session | Data transfer, class of service, control data exchange | Network File System (NFS), SQL, RPC |
| Transport | Quality and reliability, ensures data received, segments | TCP, UDP, SPX, NetBEUI |
| Network | Path selection, logical addressing, routing | IP, IPX, RIP, ICMP, ARP, RARP, OSPF, NetBEUI, DLC, DecNET |
| Data Link | Reliable data transfer across media; physical addressing | HDLC, SLIP, PPP |
| Physical | Transmit data on media | NONE |

**Figure 1.2 – Summary of the OSI RM**

## 1.12 Data Encapsulation

When a car is manufactured in a factory, one person does not finish all of the tasks; instead, it is placed on a production line, where each individual adds different parts to the car as it progresses, until it reaches the end of the line, when it is complete and ready to be transported to the dealer. Any data that needs to be sent from one computer to another follows the same approach. Because the OSI model assures that these principles are followed (much like the manufacturing line above), any computer will be able to connect with every other computer, regardless of whether one is a Macintosh, Linux, or a PC. One thing to remember is that data travels in the OSI model in two directions: DOWN (from top layers to bottom layers – data encapsulation) and UP (from physical to above layers – data de-encapsulation).

Figure 1.3 is an example of a simple data transfer between 2 computers and shows how the data is encapsulated and de-encapsulated.

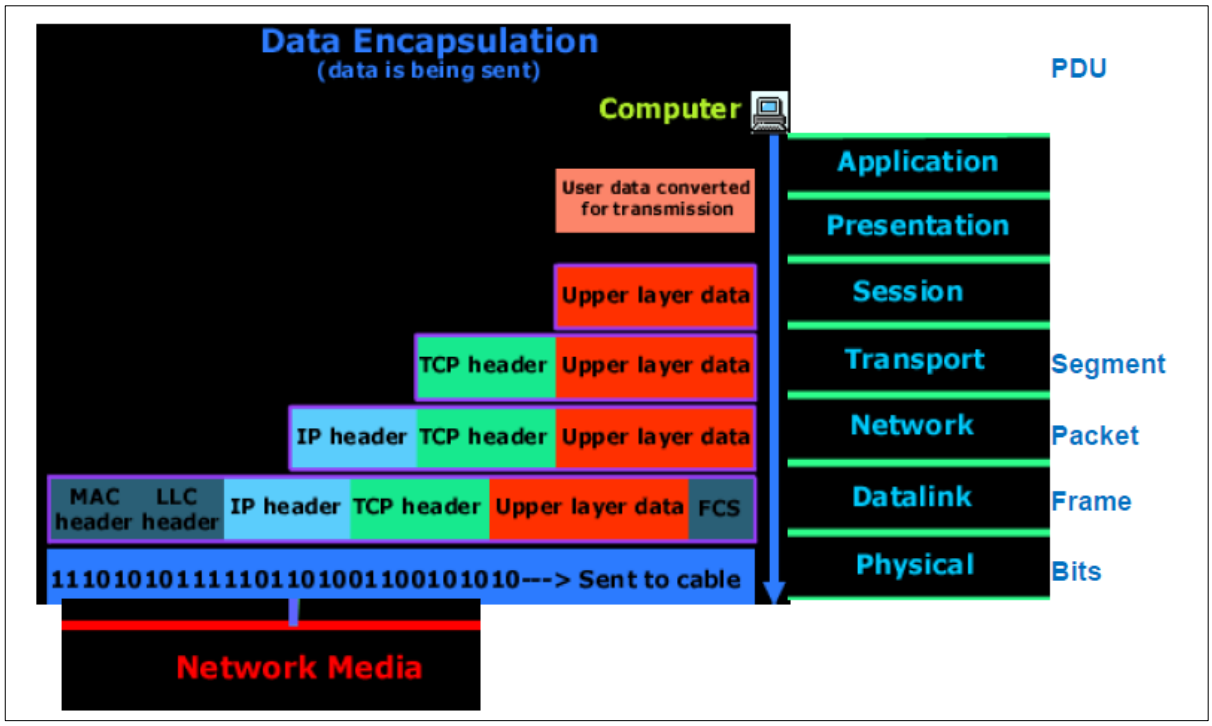



**Figure 1.3 – Simple Data Transfer – Encapsulation & De-encapsulation**

A computer in the illustration above needs to communicate data to another computer. The user interface is created at the Application layer, where the user interacts with the application. This data is then sent to the Presentation layer, and finally to the Session layer. These three layers provide some more information to the user's original data before passing it on to the Transport layer. The data is broken down into smaller chunks (sent one at a time) and the TCP header is inserted. The data at the Transport layer is referred to as a segment at this stage. Each segment is sequenced such that the data stream may be reassembled exactly as it was sent on the receiving end. The Network layer then handles network addressing (logical addressing) and routing over the internet network for each segment. The data (which includes the transport header and upper layer information at this point) is referred to as a packet at the Network layer.

The IP header is added by the Network layer, which then transfers it to the Datalink layer. A frame is the name given to the data (which contains the Network layer header, Transport layer header, and higher layer content). The Datalink layer is in charge of transferring packets from the Network layer to the network media (cable).

The Datalink layer encapsulates each packet in a frame that includes the source and destination computer's (host) MAC addresses, as well as LLC information that specifies which protocol in the preceding tier (Network layer) the packet should be forwarded to when it reaches at its destination. Finally, there is the FCS field, which stands for Frame Check Sequence. FCS is used for error checking/detecting within transmitted packets and is added at the end by the Datalink layer.

## 1.13 Frame Check Sequence

FCS is a protocol that checks and detects errors in transmitted packets. Crosstalk between the wires of a cable, as well as external interference such as Radio Frequency and Electromagnetic Interference, can create mistakes in all frames on a network. Thankfully, the Data Link layer employs a Frame Check Sequence (FCS) to detect mistakes during transmission. A FCS field exists in each frame and is used to keep a value that is calculated for each frame. Before the frame is transferred, the destination Data Link layer compares this field value to the same calculation made by the source Data Link layer. If the frame's FCS number does not match the recalculated number, a transmission error has occurred; the frame is dropped, and the destination host requests that it be resent.
The Frame Check Sequence can use a number of different methods; however, these are the most popular:

- CRC – Cyclic redundancy Check – Polynomial calculations are performed on the data
- Two Dimensional Parity – Uses a parity bit to make sure the data has not been corrupted.
- Checksum – Sums the data to arrive at a total

If the destination computer is located on a different network, the frame is transmitted to the router or gateway to be routed to it. This frame must be converted to a digital signal before being sent across the network. Because a frame is essentially a logical collection of 1s and 0s, the Physical layer is in charge of encoding these numbers into a digital signal that can be read by devices on the same local network. A few 1s and 0s are also placed at the start of the frame to allow the receiving end to synchronize with the digital signal it will be receiving.

The data is received at the target computer, as shown in Figure 1.4. The receiving computer will initially synchronize with the digital signal by reading the aforementioned few extra 1's and 0's. Once the synchronization is complete, it receives the entire frame and passes it on to the Datalink layer above it.

The frame will be subjected to a Cyclic Redundancy Check (CRC) by the Datalink layer. This is a calculation that the computer performs, and if the result equals the value in the FCS field, it is assumed that the frame was received correctly.

Once that's done, the Datalink layer will strip off any data or headers added by the remote system's Datalink layer and transfer the rest (now that we've moved from the Datalink layer to the Network layer, we'll refer to the data as a packet) to the Network layer above it.

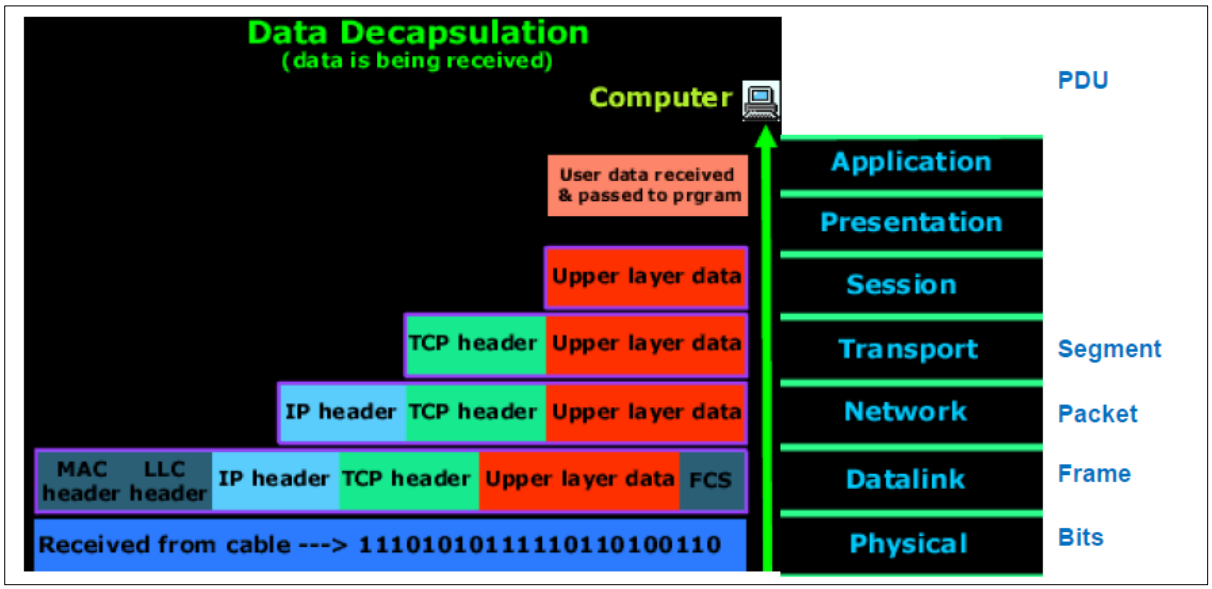



**Figure 1.4 – Synchronization between computers in FCS**

The IP address is checked at the Network layer, and if it matches (with the machine's own IP address), the Network layer header, or IP header, is stripped from the packet, and the rest is transmitted to the Transport layer above. The rest of the data is now referred to as a segment.

The segment is processed at the Transport layer, which rebuilds the data stream (which was originally divided into pieces on the sender's computer so it could be sent) and recognizes that each piece has been received by the transmitting computer. We are obviously utilizing TCP (rather than UDP!) because we are sending an ACK back to the sender from this tier.

After then, the data stream is handed over to the upper-layer application. Most people never investigate any layers above the Transport layer in detail when analysing how data gets from one machine to another. This is because, depending on the type of data, the entire process of moving data from one computer to another usually involves layers 1 to 4, or the Physical layer to the Transport layer and vice versa (or layer 5 (Session) at the most).

## 1.14 Connection-oriented Network Services

Networking protocols and the data traffic they allow can be classified as connection-oriented or connectionless in general. The sender (a node) first alerts the network that it desires to initiate a discussion with another node in connection-oriented service. The network transmits its request to the destination, which either accepts or rejects it.

Connection fails if the destination refuses; otherwise, connection is established. The use of a specific path that is established for the length of a connection is called connection-oriented data handling. As a result, connection-oriented data processing entails sending data across a persistent connection. There are three steps to a connection-oriented service: connection formation, data transfer, and connection termination. A single path between the source and destination systems is determined during the connection-establishment phase. To provide a consistent level of service, such as a specified throughput rate, network resources are often reserved at the time.

Data is delivered successively via the defined path during the data transmission phase. Data is always delivered in the sequence in which it was sent to the target system. A connection that is no longer needed is ended during the connection-termination phase. A new link between the source and destination systems is required for further communication.

### 1.14.1 Goal of Connection-oriented Network Services:

- data transfer between end systems. - Handshaking of Connection-oriented Network Services. Setup (prepare for) data transfer ahead of time: sets up "state" in two communicating hosts.
- Transport Control Protocol (TCP): Is the Internet's connection-oriented service. TCP is reliable, in-order byte-stream data transfer. Loss: means no acknowledgement from receiver and entails a retransmission. Flow Control: A fast sender won't overwhelm a slow receiver. Congestion Control: Senders "slow down sending rate" when network congested.
- Applications using connection-oriented TCP: HTTP (WWW), FTP (file transfer), Telnet (remote login), SMTP (email) etc.
- Connection-Oriented Service – Points to retain: The network guarantees that all packets will be delivered in order, without loss or duplication of data. Only a single path is established for the call and all the data follow that path. The network guarantees a minimal amount of bandwidth and this bandwidth is reserved for the duration of the call.

Future call requests will be denied if the network becomes overburdened. Before any data packets can be transferred using connection-oriented service, a path from the source router to the destination router must be created. In analogy to the real circuits put up by the telephone system, this connection is referred to as a VC (virtual circuit) (the subnet is called a virtual-circuit subnet).

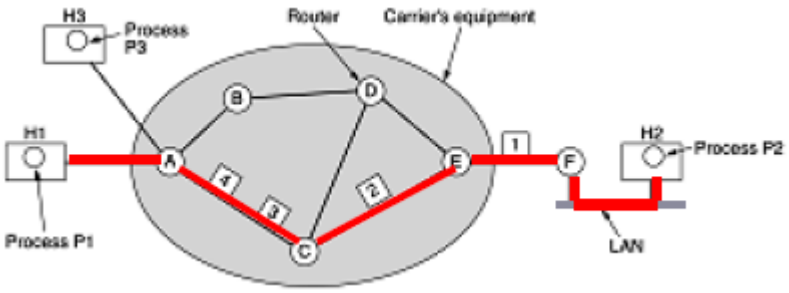



**Figure 1.5 – Virtual Circuit**

A connectionless network service is one that allows subscribers to share information without the requirement for end-to-end setup processes (i.e., no advance setup is required). In a connectionless service, the sender (a node) sends the address of the recipient to whom the data should be delivered with each piece of data. Because each packet of data is routed individually, the network cannot guarantee that all packets will arrive at their destination in the same sending order in which they were sent, because packets can be sent by multiple paths.

Because each packet of data is routed individually, the network cannot guarantee that all packets will arrive at their destination in the same sending order in which they were sent, because packets can be sent by multiple paths (for e.g., routers). The router will make a NEW decision of which among its output lines it would send any NEWLY arriving packet. Hence the goals are to make data transfer between end systems, for the UDP (User Datagram Protocol) is Internet's connectionless service – make unreliable data transfer, there is no flow control and no congestion control. Applications using UDP are the streaming media, teleconferencing, Internet telephony, Resolver querying a DNS server to fetch an IP address.

## 1.15 Implementation of connectionless services

If a connectionless service is available, packets are injected into the subnet one by one and routed separately. There is no need to prepare ahead of time. As shown in Figure 1.6, the packets are commonly referred to as datagrams (in analogy with telegrams) and the subnet is referred to as a datagram subnet.

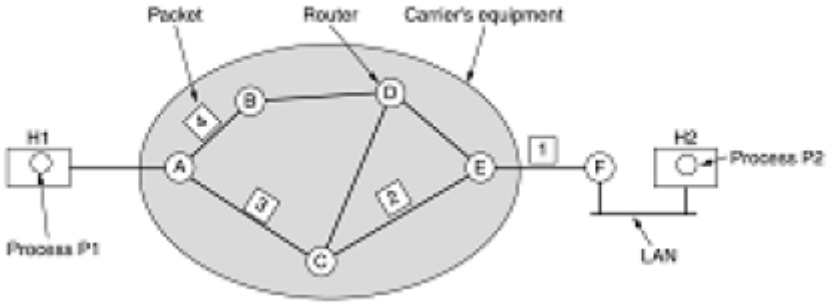



**Figure 1.6 – Implementation of connectionless services**

However, when compared to connection-oriented services, connectionless services have two significant advantages: dynamic path selection and dynamic bandwidth distribution. Because paths are chosen on a packet-by-packet basis, dynamic path selection allows traffic to be routed around network faults. Because network resources are not assigned bandwidth that they will not utilize, bandwidth is used more efficiently with dynamic-bandwidth allocation. Connection-oriented network services have two major drawbacks over connectionless network services: static path selection and static network resource reservation. Because all traffic must travel along the same static path, static-path selection might be problematic. The connection will fail if there is a failure anywhere along the path. Static network resource reservation is problematic because it necessitates a certain rate of throughput and, as a result, a commitment of resources that other network users are unable to share. Unless the connection uses full, uninterrupted throughput, bandwidth is not used efficiently

## 1.7 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 1.8 Activities

- Describe the different layers in the OSI model,
- Explain the various advantages of using the OSI model,
- Describe how data encapsulation and de-encapsulation occurs in the OSI model,
- Differentiate between a MAC Address and a Port,
- Elaborate on how the Frame Check Sequence works,
- Describe how connection oriented network services can be implemented.

## 2.1 Introduction

An IP address consists of four bytes/octets (32 bits in binary) separated by periods (dots) that uniquely identify a computer accessible over a TCP/IP-based LAN or on the public Internet. An IP address is typically (normally) represented in dotted-decimal form/notation, with the decimal value of each octet (each octet being converted to decimal) separated by a period (dot). For example, 1.160.10.240 could be an IP address. Is there any limit on the decimal values??? Could an IP address be 2568.967783.370129.96102? This chapter provides a more in-depth of the IP addressing schemes.

## 2.2 Unit Objectives

- Recognise the different classes of IP addressing schemes,
- Be able to distinguish among IEEE standard project 802 and ISO,
- Explore the various formats of a frame,
- Differentiate between the different types of addressing,
- Describe various types of Ethernet,
- Understand the need for CSMA/CD,
- Explain the various networking communications media,
- Explore the difference between hub, router, switch, bridge and repeater.

## 2.3 IP address – The classes

In classful addressing, the IP address space is divided into five **classes: A, B, C, D,** and **E.** Each class occupies some part of the whole address space. Figure 8.1 shows the class occupation of the address space.

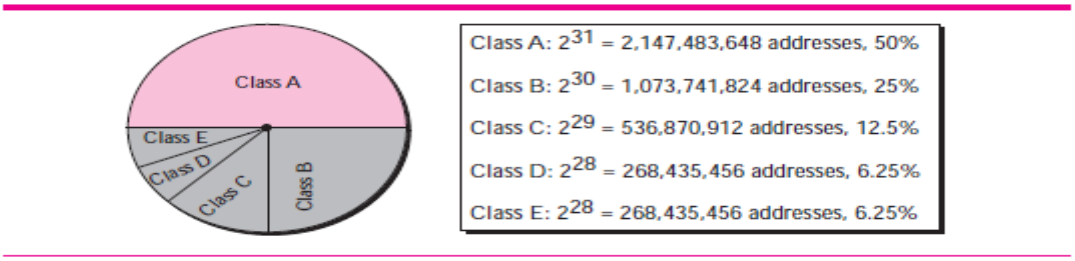



*Figure 2.1 – Classes occupation of the address space*

*Recognizing Classes*

he class of an address when the address is given either in binary or dotted decimal notation. In the binary notation, the first few bits can immediately tell us the class of the address; in the dotted-decimal notation, the value of the first byte can give the class of an address (Figure 2.2).

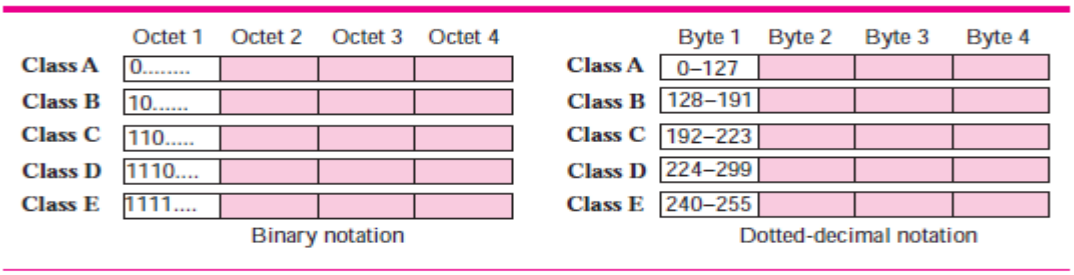



*Figure 2.2 – Different Classes*

Note that some special addresses fall in class A or E. Emphasis is made to these special addresses which are exceptions to the classification. Computers often store IPv4 addresses in binary notation. In this case, it is very convenient to write an algorithm to use a continuous checking process for finding the address as shown in Figure 2.3.

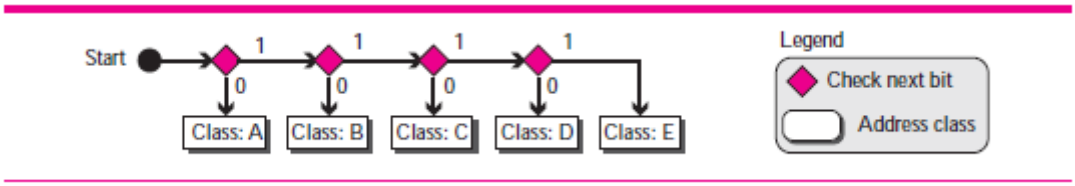



*Figure 2.3 – Finding Addresses*

In classful addressing, an IP address in classes A, B, and C is divided into **netid** and **hostid.** These parts are of varying lengths, depending on the class of the address. Figure 2.4 shows the netid and hostid bytes.

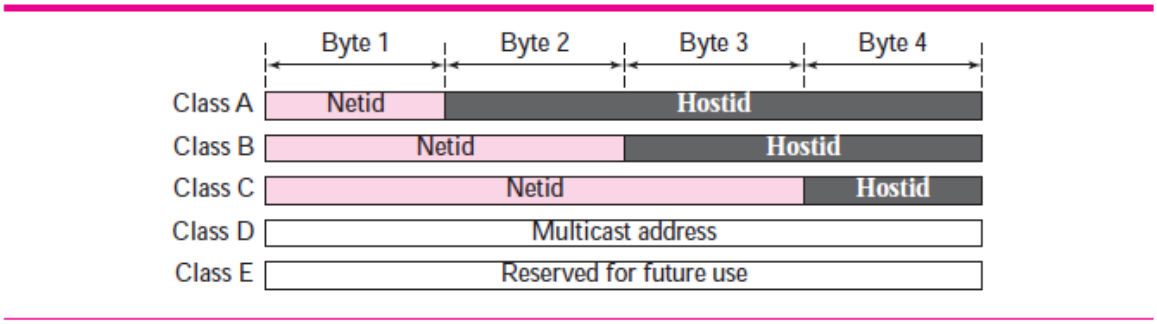



*Figure 2.4 – Netid and Hostid*

In classful addressing, the IP address space is divided into five **classes: A, B, C, D,** and **E.** Each class occupies some part of the whole address space. Figure 2.5 shows the class occupation of the address space

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size. The following scenarios shows what happens in each classes and blocks. For instance in class A, since only 1 byte in class A defines the netid and the leftmost bit should be 0, the next 7 bits can be changed to find the number of blocks in this class. Therefore, class A is divided into 27 = 128 blocks that can be assigned to 128 organizations. However, each block in this class contains 16,777,216 addresses, which means the organization should be a really large one to use all these addresses. Many addresses are wasted in this class. Figure 2.5 shows the block in class *A*.

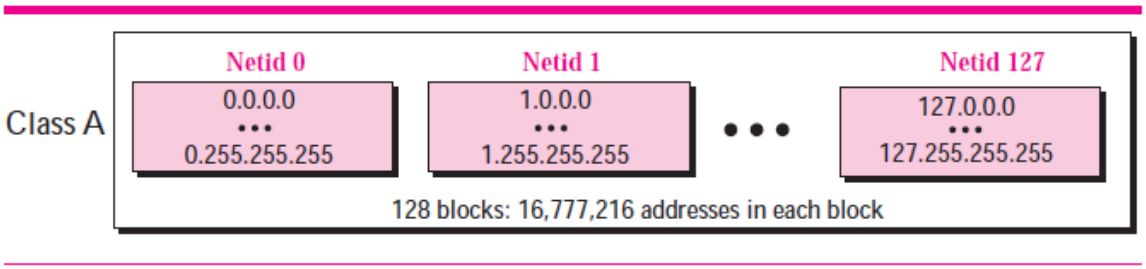



*Figure 2.5 – Block in class A*

For Class B, since 2 bytes in class B define the class and the two leftmost bit should be 10 (fixed), the next 14 bits can be changed to find the number of blocks in this class. Therefore, class B is divided into 214 = 16,384 blocks that can be assigned to 16,384 organizations. However, each block in this class contains 65,536 addresses. Not so many organizations can use so many addresses. Many addresses are wasted in this class. Figure 2.6 shows the blocks in class B.

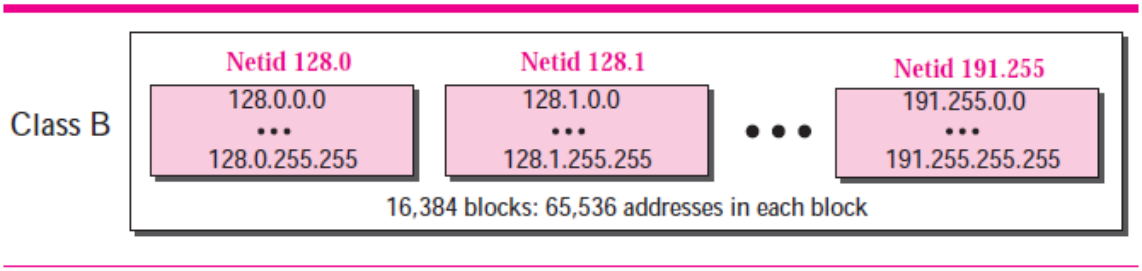



*Figure 2.6 – Block in class B*

In a class C, since 3 bytes in class C define the class and the three leftmost bits should be 110 (fixed), the next 21 bits can be changed to find the number of blocks in this class. Therefore, class C is divided into 221 = 2,097,152 blocks, in which each block contains 256 addresses, that can be assigned to 2,097,152 organizations. Each block contains 256 addresses. However, not so many organizations were so small as to be satisfied with a class C block. Figure 2.7 shows the blocks in class C.

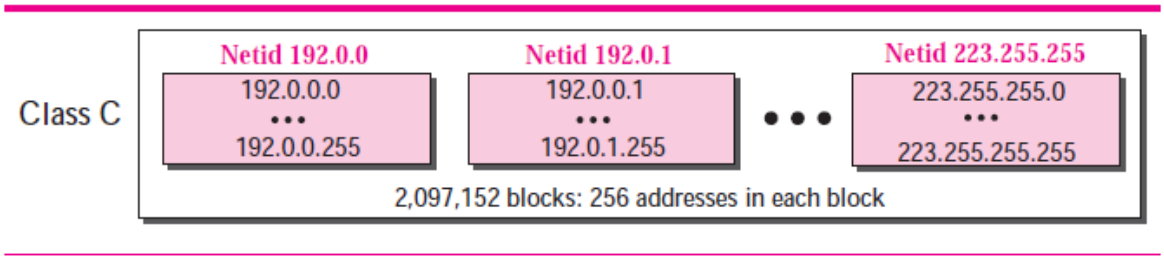



*Figure 2.7 – Block in class C*

On the other hand, for a class D, there is just one block of class D addresses. It is designed for multicasting. Each address in this class is used to define one group of hosts on the Internet. When a group is assigned an address in this class, every host that is a member of this group will have a multicast address in addition to its normal (unicast) address. Figure 2.8 shows the block.

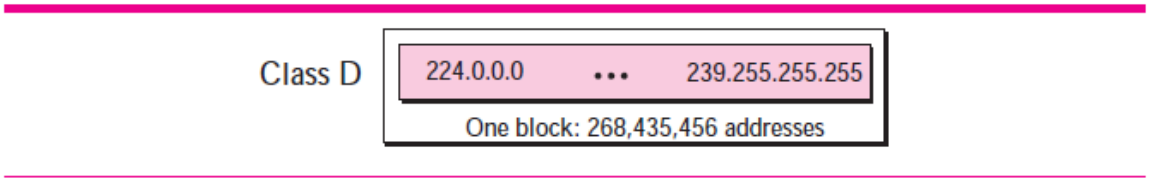



*Figure 2.8 – Block of class D*

In a class E, there is just one block of class E addresses. It was designed for use as reserved addresses, as shown in Figure 2.9.

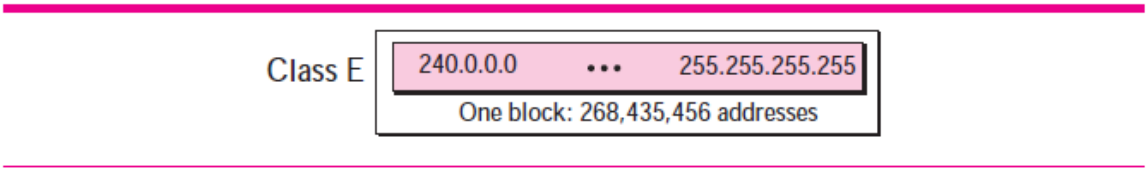



*Figure 2.9 – Block of class E*

The class networks are described as follows: - Class A comprises networks 1.0.0.0 through 126.0.0.0. The network number is contained in the first octet. This class provides for a 24-bit host part, allowing roughly 1.6 million hosts per network. Class B contains networks 128.0.0.0 through 191.255.0.0; the network number is in the first two octets. This class allows for 16,320 nets with 65,024 hosts each. Class C networks range from 192.0.0.0 through 223.255.255.0, with the network number contained in the first three octets. This class allows for nearly 2 million networks with up to 254 hosts. Classes D, E, and F Addresses falling into the range of 224.0.0.0 through 254.0.0.0 are either experimental or are reserved for special purpose use and don't specify any network. IP Multicast, which is a service that allows material to be transmitted to many points on an internet at one time, has been assigned addresses from within this range.

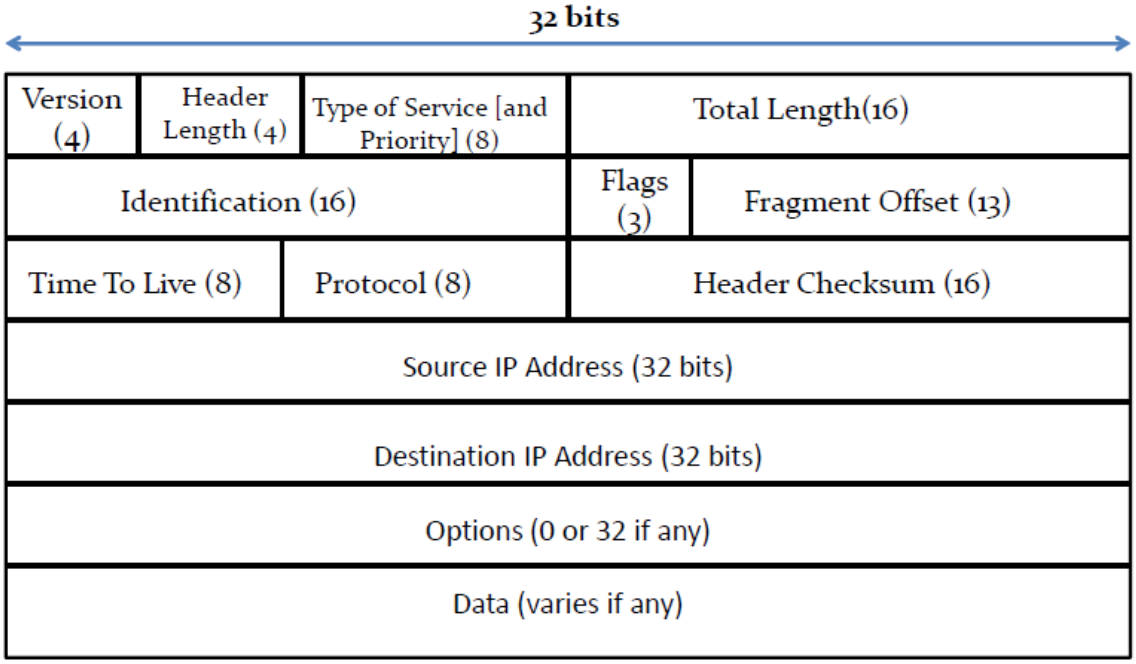
You may have observed that for each octet in the host part, not all of the potential values from the previous list were allowed. Because the octets 0 and 255 are designated for particular purposes, this is the case. A network address is one in which all host part bits are 0, while a broadcast address is one in which all host part bits are 1.

This refers to all hosts on a certain network at the same time. As a result, 149.76.255.255 is not a valid host address; instead, it refers to all hosts on the 149.76.0.0 network. A set of network addresses has been set aside for certain uses. Two examples are 0.0.0.0 and 127.0.0.0. The default route is the first, and the loopback address is the second. The default route refers to how IP datagrams are routed. Your host's IP traffic is routed through network 127.0.0.0. 127.0.0.1 is usually assigned to a particular interface on your host called the loopback interface, which serves as a closed circuit. Any TCP or UDP IP packet handed to this interface will be returned to them as if it had just arrived from some network.

This enables you to create and test networking applications without ever having to connect to a "real" network. You can also utilize networking software on a solitary host using the loopback network. This isn't as rare as it sounds; many UUCP sites, for example, don't have any IP connectivity but nevertheless want to operate the INN news system. INN requires the loopback interface to function properly on Linux. Some address ranges from each of the network classes have been set aside and labeled as "reserved" or "private." These addresses are just for private networks and are not routed through the Internet. They're most typically utilized by companies creating their own intranets, although they're also useful for tiny networks.

## 2.4 IPv4 Protocol (revisited)

The format of IP datagrams as shown in Figure 2.10 is a good location to start our investigation of the network layer on the Internet. A header part and a text part make up an IP datagram. A 20-byte fixed part and a variable-length optional part make up the header. The format of the header is given in the diagram below. It's sent in big-endian order, from left to right, starting with the version's high-order bit.




**The IPv4 (Internet Protocol) Header**

**Figure 2.10 – The IPv4 – IP Header**

The **Version field -** keeps track of the protocol version to which the datagram belongs. It becomes feasible to move between old versions operating on some machines and newer versions running on others by including the version in each datagram.

**HLEN -** The **Header LENgth field** is not a constant, therefore, a field in the header, IHL, is provided to tell how long the header is. The minimum value is 5, which applies when no options are present. The maximum value of this 4-bit field is 15.

The **Type of Service** (and Priority) **field** is one of the few fields that has changed its meaning (slightly) over the years. It was and is still intended to distinguish between different **Classes of Service**. Various combinations of reliability and speed are possible. For digitized voice, fast delivery beats accurate delivery. For file transfer, error-free transmission is more important than fast transmission.

The **Total Length field** - length of the packet/datagram including both header and data. The maximum length is 65,535 bytes. At present, this upper limit is tolerable, but with future gigabit networks, larger datagrams might be needed.

The **Identification field is** a unique IP-packet value needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments/datagrams belonging to the same flow contains the same identification value.

**Flags field:** consists of 2 sub-fields DF and MF and specifies whether fragmentation should occur. **DF** stands for Don't Fragment. It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again. **MF** stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.

**Fragment Offset field** - If the packet is too large to fit in a frame, it is fragmented and reassembled. The Fragment offset also indicates where this fragment belongs in the current datagram. Except for the last fragment in a datagram, all fragments must be multiples of 8 bytes, the elementary fragment unit.

The **Time To Live field** is a counter used to limit packet lifetimes. TTL is set into a packet when it is originally generated. It gives it a time…to live! If the packet does not get where it wants to go before the TTL expires, it is cast off. This stops IP packets from continuously cycling the network looking for a destination. TTL is counts time in seconds and allows a maximum lifetime of 255 sec. It is decremented at each hop and *is supposed to be decremented multiple times when queued for a long time in a router*. In practice, TTL just counts hops. When it hits zero, the packet is discarded and a warning packet is sent back to the source host. This feature prevents datagrams from wandering around forever, something that otherwise might happen if the routing tables ever become corrupted.

The **Protocol field** - The network layer must know what to do with a complete datagram after it has been built. The Protocol field specifies which transport protocol to use - for example, TCP, UDP, or some other transport protocol. The numbering of protocols is consistent throughout the Internet. Protocols and other given numbers are stored in a database that can be accessed online (located at www.iana.org). The Protocol field, in summary, refers to the port number of upper-layer protocols (for example, TCP port 6 (hex) and UDP port 17 (hex)).

The **Header checksum field -** Only checks the header. This checksum can be used to detect faults caused by faulty memory words in a router. The algorithm consists of adding up all the 16-bit half-words as they come using one's complement arithmetic, then taking the one's complement of the result. The Header checksum is assumed to be zero upon arrival for the purposes of this technique. In a nutshell, the header checksum is nothing more than a Cyclic Redundancy Check (CRC) on the header only.

**Source address field**: 32-bit IP address of sending host.

**Destination address field**: 32-bit IP address of the station the packet is destined for.

The **(IP) Options field** allows future versions of the protocol to contain information that was not there in the initial design, allowing experimenters to test out new ideas and avoiding allocating header bits to information that is rarely used. The Options field is used for a variety of purposes, including network testing, debugging, and security.

**Data field**: It's the upper-layer data.

## 2.5 Network Address Translation (NAT) & IP Masquerading

There is a scarcity of IP addresses. An ISP can be assigned a class B address, which gives it 65,534 host numbers. If it has more customers than that, it will have a problem. For home users with dial-up connections, one approach is to assign a computer a dynamic IP address when it calls up and logs in, and then delete the IP address after the session is done.

A single class B address may accommodate up to 65,534 active users using this method, which is more than enough for a big ISP with hundreds of thousands of customers. After the connection is terminated, the IP address is assigned to another caller. This strategy works well for ISPs that serve a significant number of home users, but it falls short for ISPs that primarily serve commercial customers. To make matters worse, more and more home customers are choosing for ADSL or cable Internet. There are two benefits to using these services: the user gets a permanent IP address and there is no connection fee (just a monthly flat rate charge). As a result, many ADSL and cable clients remain connected at all times. This trend merely adds to the scarcity of IP addresses.

Assigning IP numbers on the fly, as is done with dial-up users, is futile because the number of IP addresses in use at any given time may be many times the number possessed by the ISP. The entire Internet should migrate to IPv6, which utilizes 128-bit addresses, in the long run. This transition will take years to accomplish. As a result, several individuals believed that a temporary solution was required. The solution to this problem was Network Address Translation (NAT). The basic idea behind NAT is to provide each company with a single (or a small number of) IP addresses for Internet traffic. Internal traffic is routed using a unique IP address allocated to each machine in the organization. However, when a packet leaves the company and travels to the ISP, it undergoes an address translation. To make this technique possible, three IP address ranges have been declared as private (reserved).

Companies may use them internally as they wish. The only rule is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges of Private/Reserved IP addresses are: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255. This is depicted in Figure 2.1

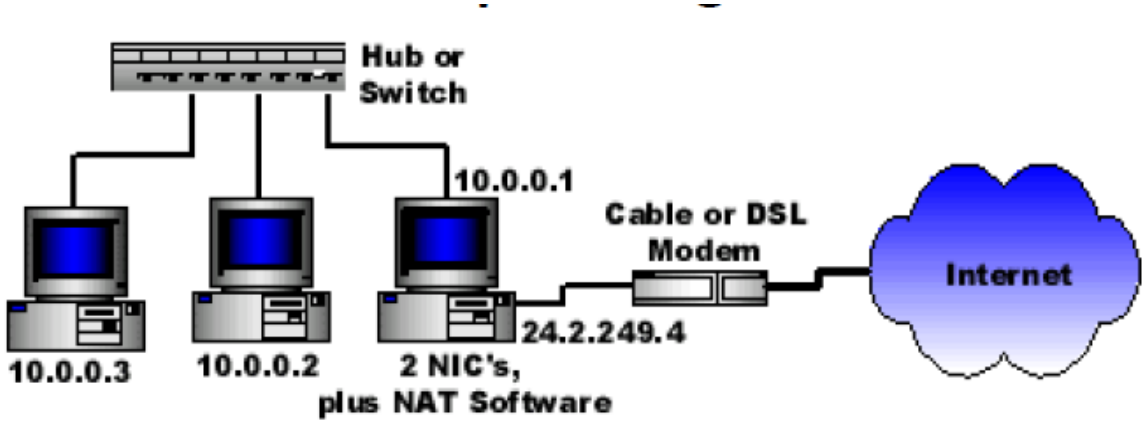



Figure 2.11 – Operation of the NAT

**Operation of NAT** - Within the company premises, every machine has a unique address of the form 10.x.y.z. as shown in Figure 2.11. However, when a packet leaves the company premises, it passes through a NAT box that converts the internal IP source address, 10.0.0.1 in the figure, to the company's true IP address, 24.2.249.4. NOTE: It is also possible to integrate the NAT box into a router. Suppose there are many requests to the Internet (using 24.2.249.4). How does the NAT box know how to redirect these requests to their respective PCs? This can be shown in Figure 2.12

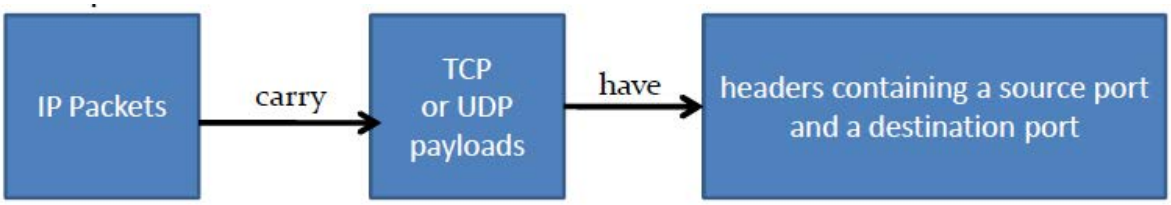



**Figure 2.12 – The NAT box**

Ports = 16-bit integers which indicates where TCP connections begin and ends. Ports provide the field needed to make NAT work. There are 65535 ports out of which only 1024 (0 – 1023) are used/reserved for well-known services. Suppose there are many requests to the Internet (using 24.2.249.4). How does the NAT box know how to redirect these requests to their respective PCs?

RECAP: When a process wants to connect to another process through TCP, it connects to an unused TCP port on its own machine. This is known as the source port, and it instructs the TCP code where to deliver incoming packets for this connection. The process also provides a destination port, which indicates to whom the packets should be sent on the remote network. A source port and a destination port are included in every outgoing TCP communication. These ports work together to identify the processes on both sides of the connection.

Whenever an outgoing packet enters the NAT box, the 10.x.y.z source address is replaced by the NAT's box true IP address. In addition, the TCP Source port field is replaced by an index into the NAT box's 65,536-entry translation table. This table entry contains the original IP address and the original source port. Finally, both the IP and TCP header checksums are recomputed and inserted into the packet. It is necessary to replace the Source port because connections from machines 10.0.0.1 and 10.0.0.2 may both happen to use, for e.g., port 5000. So, the Source port alone is not enough to identify the sending process. When a packet arrives at the NAT box from the ISP, the Source port in the TCP header is extracted and used as an index into the NAT box's mapping table. From the entry located, the internal IP address and original TCP Source port are extracted and inserted into the packet. Then both the IP and TCP checksums are recomputed and inserted into the packet. The packet is then passed to the company router for normal delivery using the 10.x.y.z address.

### 2.5.1 Objections to NAT

For starters, NAT goes against the IP architectural paradigm, which asserts that each IP address uniquely identifies a particular machine on the Internet (worldwide). NAT allows hundreds of devices to share a single IP address, such as 10.0.0.1. The Internet is transformed from a connectionless network to a connection-oriented network thanks to NAT. A NAT box must keep track of each connection that passes through it (the mapping). Connection-oriented networks, not connectionless networks, have the ability to preserve connection state. The mapping table of the NAT box will be lost if it crashes. As a result, all of its TCP connections will be lost. Router crashes have no effect on TCP in the absence of NAT. The transmitting process just times out after a few seconds, and all unrecognized packets are resent. As a result of NAT, the Internet becomes just like a circuit-switched network. TCP and UDP are not necessary for Internet processes. If a user on machine A decides to communicate with a user on machine B using a new transport protocol (for example, for a multimedia application), the application will fail because the NAT box will be unable to discover the TCP Source port appropriately. Some programs provide IP addresses in the text body. The receiver then extracts and uses these addresses. Because NAT is unaware of these addresses, it is unable to replace them, so any effort to utilize them on the remote side will be unsuccessful. This is how File Transfer Protocol (FTP) works, and it can fail if NAT is present unless specific safeguards are taken! Because the TCP Source port information is only 16 bits long, an IP address can only be mapped to a maximum of 65,536 (216) machines. However, the true number is 61,440 machines, which is 65,536 – 4096 (4096 being allocated for special uses).

As a result, if three machines in an organization conduct NAT, each may manage up to 61,440 machines, not 65,536! Many security vulnerabilities are caused (brought about) by NAT: a user sitting on a machine with a private IP address can send spam emails to people without being easily detected.

## 2.6 Internet Control Protocol

In addition to IP, which is used for data transfer, the Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP and DHCP.

### 2.6.1 The Internet Control Message Protocol (ICMP)

The routers keep a tight eye on the Internet's functionality. ICMP, or Internet Control Message Mechanism, is an error-reporting protocol that operates in conjunction with IP. IP transmits an ICMP error message within an IP datagram if there is a network fault, such as a failure in one of the pathways. As a result, ICMP requires IP as its transport protocol.

ICMP also sends out alerts when something unexpected happens. The Internet is also tested using ICMP. In response to datagrams that cannot be delivered or have other issues, routers send ICMP messages. The router encapsulates an ICMP message in an IP datagram and transmits it back to the source of the undeliverable datagram.

To determine whether a station is reachable, the ping command employs ICMP as a probe. Ping encapsulates an ICMP echo request message in a datagram and forwards it to a specified destination. The user selects the destination by typing its IP address or name into the command line, such as #ping 200.100.50.25. There are about a dozen different types of ICMP messages defined. The most significant are listed in the table below. It should be noted that each ICMP message type is encapsulated within an IP packet. This is shown in Figure 2.13

| Message type | Description |
|---|---|
| Destination unreachable | Packet could not be delivered |
| Time exceeded | Time to live field hit 0 |
| Parameter problem | Invalid header field |
| Source quench | Choke packet |
| Redirect | Teach a router about geography |
| Echo request | Ask a machine if it is alive |
| Echo reply | Yes, I am alive |
| Timestamp request | Same as Echo request, but with timestamp |
| Timestamp reply | Same as Echo reply, but with timestamp |

**Figure 2.13 – ICMP features**

### 2.6.2 The Address Resolution Protocol (ARP)

ARP is a technique for determining a host's MAC address based on its IP address. The sender broadcasts an ARP packet containing another host's Internet address and waits for it (or another host) to respond with its MAC address. A table, commonly referred to as the ARP cache, is used to keep track of the relationship between each MAC address and its corresponding IP address. To reduce delay and loading, each host maintains an ARP cache (of address translations). ARP defines the protocol rules for establishing this correlation and converting addresses in both directions. ARP allows the Internet address to be independent of the MAC address; however, it is only effective if all hosts support it. The alternative for hosts that do not perform ARP is to use a preconfigured mapping of IP addresses to MAC addresses.

#### 2.6.2.1 How does ARP operate?

If an incoming packet for a host machine on a specific network enters the gateway asks for a physical host or MAC address matching the IP address in the ARP program. The ARP program looks in the cache of the ARP and provides the address to enable the packet to be converted and sent to the machine in the right packet size and format. If no IP address entry is found, ARP will send a request packet to all machines of the LAN in special format to see if a machine knows that it has that IP address. An IP address machine returns a reply that indicates the IP address itself. This can be shown in Figure 2.14

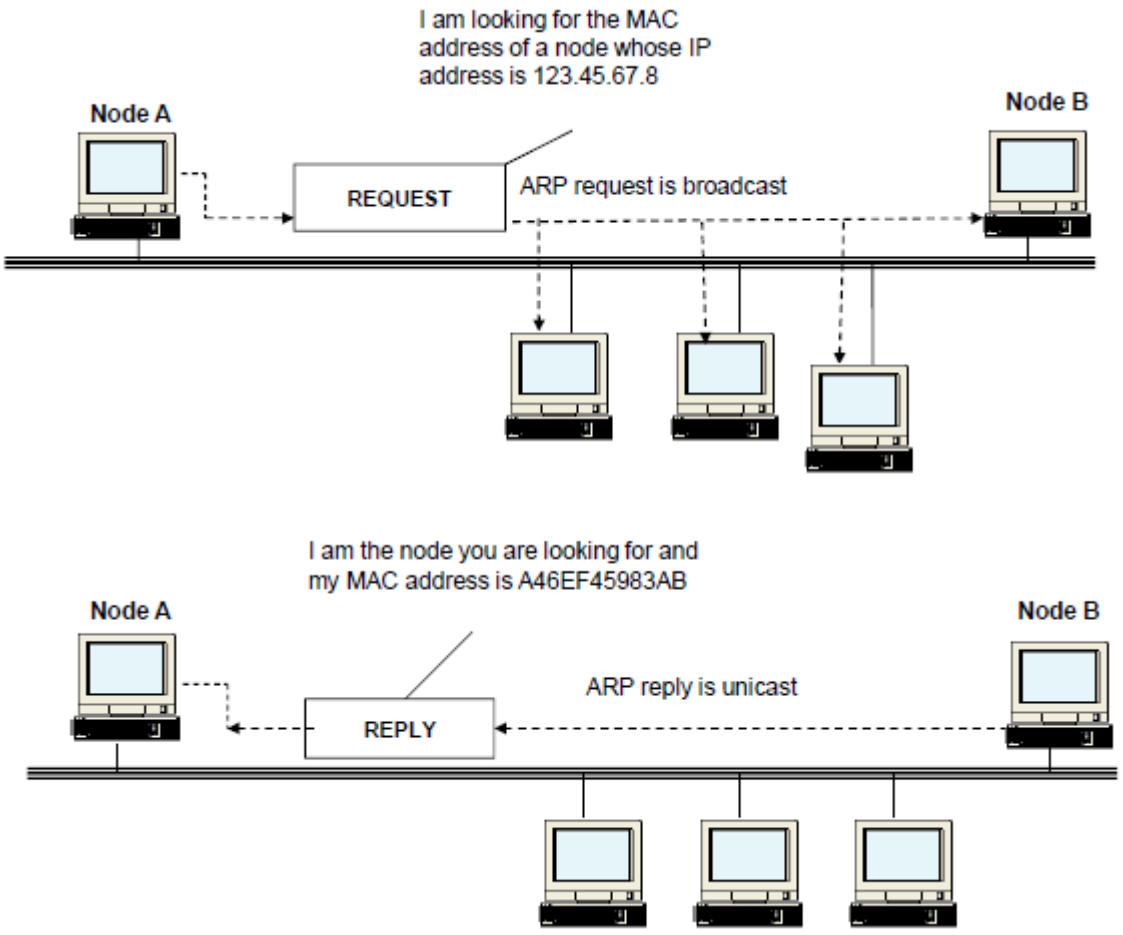



**Figure 2.14 – Operation of the ARP**

The benefit of ARP over configuration files is its ease of use. Without assigning an IP address for each machine and deciding on subnet masks, the system manager needs to do a lot. The rest is done by ARP. ARP can work more efficiently with various optimizations. First, once a machine has run ARP, the result is cached if it needs to contact the same machine in the near future. Next time, it will find the map in its own cache, so that a second broadcast is not required. The problem of finding which MAC address corresponds to a specific IP address is solved by ARP.

### 2.6.3 Reverse Address Resolution Protocol (RARP)

The opposite problem must sometimes be solved: What is the corresponding IP address with a MAC address? Especially when the diskless workstation is booted (no hard drive, therefore no OS). This problem occurs. Normally, a machine such as this is installed on a remote server with the binary image of an OS. But how is his IP address learned? RARP was the first solution designed (Reverse Address Resolution Protocol). This protocol enables a newer workstation to transmit its MAC address and say that I have 48-bit MACs 14.04.05.18.01.25. Do you know my IP address anybody out there? The **RARP server** sees this request, looks up the MAC address in its configuration files, and sends back the corresponding IP address.

RARP is a protocol that allows a physical machine to request the acquisition of its IP from the ARP table or cache of a gateway server. In the LAN gateway router, a network administrator creates a table to map the addresses of a MAC into the appropriate IPs. When you set up a new machine, the RARP client program requests its IP address from the RARP server on the router. If an entry was configured on the router table, the RARP server will return to the machine the IP address, which it will store for use in the future. NOTE: RARP is available for Ethernet, Fiber Distributed-Data Interface, and Token Ring LANs as shown in Figure 2.15

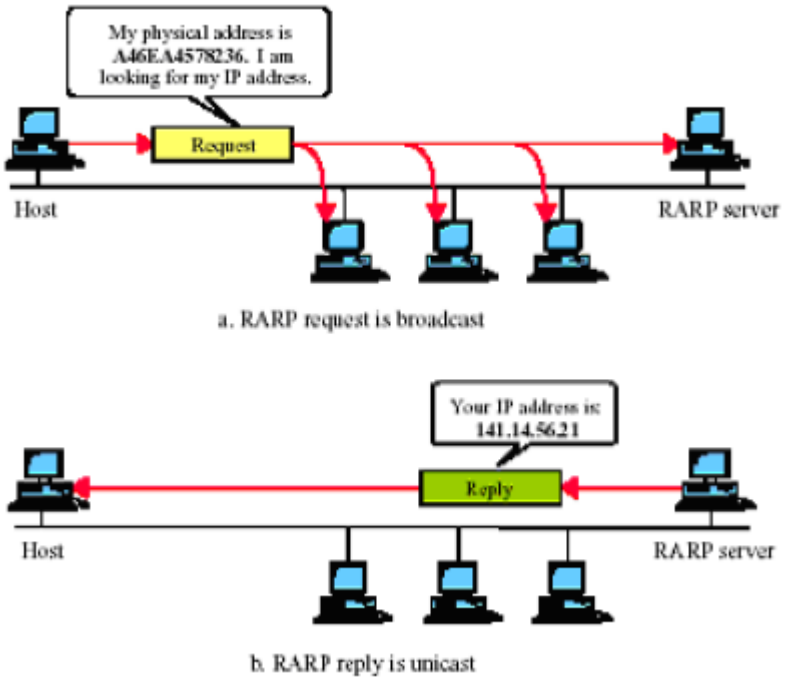



**Figure 2.15 – The RARP Server**

The use of RARP is better than the incorporation of an IP address in the memory image, as it enables all machines to use the same image. Each workstation would need its own image if the IP address were entered in the image. A disadvantage of RARP is that it uses all 1s (limited broadcast) destination addresses to reach the RARP server. However, these transmissions are not transmitted by routers, so that each network needs a RARP server.

### 2.6.4 Bootstrap Protocol (BOOTP)

As mentioned above, RARP uses a 1s (limited broadcasting) destination address to reach RARP servers. However, these transmissions are not transmitted by routers, so that each network needs a RARP server. To overcome this problem, the Bootstrap Protocol (BOOTP) was invented as an alternative bootstrap protocol. In contrast to RARP, BOOTP uses UDP posts sent via routers. Further information, including the IP address of the memory image file server, the IP address of the default router, and the subnet mask to use, is available in this diskless workstation. The problem with RARP is that it operates on the data link layer and therefore is only available on the local LAN for assigning IP addresses to customers. To access the RARP server, RARP uses a destination address of all 1s (limited diffusion). However, these transmissions are not transmitted by routers, so that each network needs a RARP server. An alternative bootstrap protocol – BOOTP, instead, can be used to overcome this problem. In contrast to RARP, BOOTP uses UDP posts sent via routers. If you don't have the IP address of the client when you boot, you can use a BOOTP server for IP address. It will use a 255.255.255.255 IP address. The BOOTP server will react to the broadcast if the Client is on the same LAN as the BOOTP Server and the client's MAC address will be given and the IP address provided. If the BOOTP server is located on another LAN, i.e. on the other side of a router, it is not possible for us to have transmissions sent to the client, or for the router to pass broadcasts.

In contrast to RARP, BOOTP uses UDP posts sent via routers. Further information including the IP address of the memory picture file server, IP address of the standard router and the subnet mask to use is also provided on the diskless workstations. A serious BOOTP problem is that tables mapping IP address to Ethernet address needs manual configuration. If a new host is added to a LAN, it cannot use BOOTP until the administrator has assigned it an IP address and has entered the BOOTP configuration table (Ethernet address, IP address) manually. The BOOTP configuration is shown in Figure 2.16

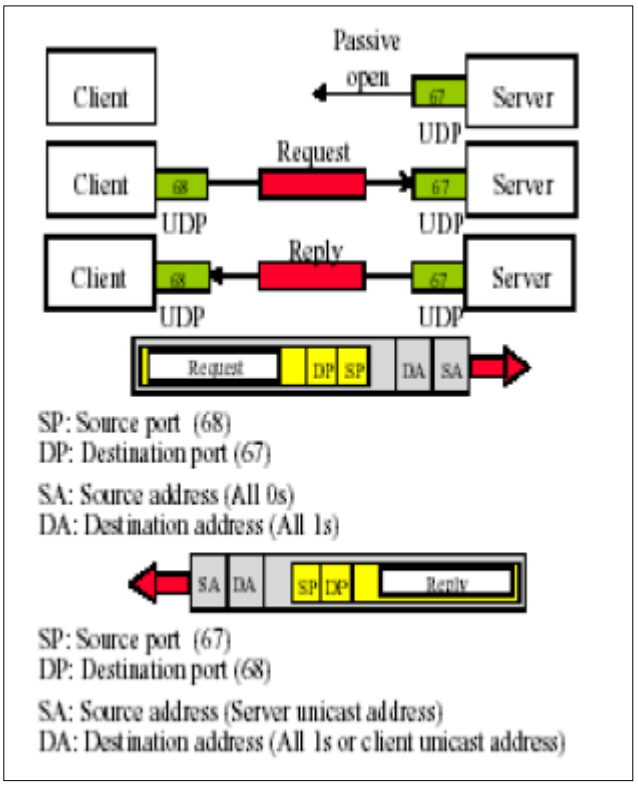



**Figure 2.16 – The BOOTP Configuration**

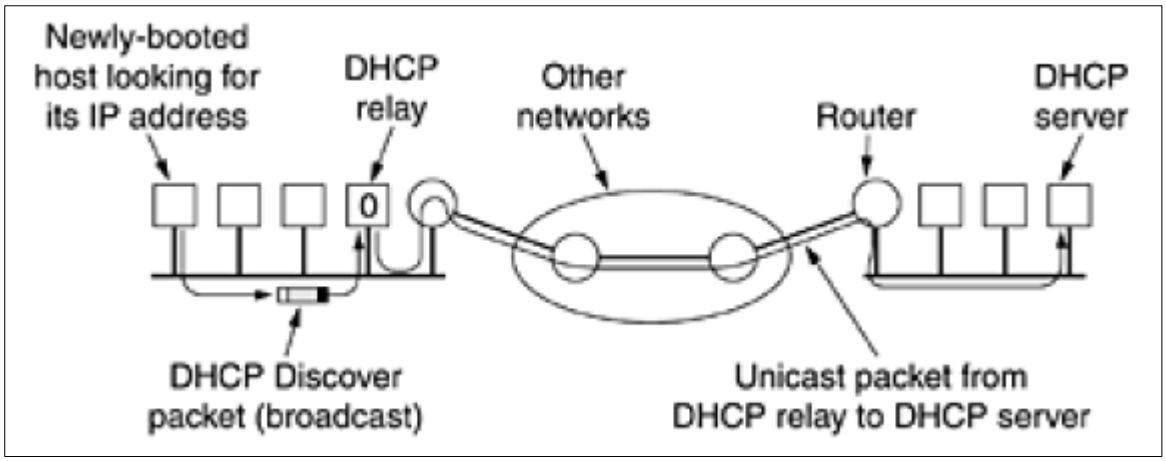



**Figure 2.17 – The DHCP Server**

## 2.6.5 Dynamic Host Configuration Protocol (DHCP)

BOOTP has been extended and given an additional name to remove this error-prone step (the above-mentioned disadvantage) (DHCP). DHCP allows for both manual and automatic assignment of IP addresses. DHCP automatically assigns IP addresses and other network setup information to network computers (subnet mask, broadcast address, etc.). A DHCP-configured client will send a broadcast request for an address to the DHCP server. A 'lease' is issued by the DHCP server and assigned for the client. You can specify on the server the term of a valid rental. This allows you to move a computer to different networks, and configure the appropriate IP address, gateway, and subnet mask. D HCP reduces the amount of time necessary to configure clients. For ISPs, the number of IP addresses it can use is limited. A "static" IP address can be assigned to specified hardware by DHCP servers.

### 2.6.5.1 How does a DHCP Server assign an IP Address to a client requesting for it?

**Version 1**

- Lease Request: Client broadcasts request to DHCP server with a source address of 0.0.0.0 and a destination address of 255.255.255.255. The request includes the MAC address which is used to direct the reply.
- IP lease offer: DHCP server replies with an IP address, subnet mask, network gateway, name of the domain, name servers, duration of the lease and the IP address of the DHCP server.
- Lease Selection: Client receives offer and broadcasts to ALL DHCP servers that will accept given offer so that other DHCP server need not make an offer.
- The DHCP server then sends an ACK to the client. The client is configured to use TCP/IP.
- Lease Renewal: When half of the lease time has expired, the client will issue a new request to the DHCP server.

### 2.6.5.2 How does a DHCP Server assign an IP Address to a client requesting for it?

**Version 2**

- Like RARP and BOOTP, DHCP is based on the idea of a special server that assigns IP addresses to hosts asking for one. This server need not be on the same LAN as the requesting host. Since the DHCP server may not be reachable by broadcasting, a DHCP relay agent is needed on each LAN, as shown in the figure that follows.
- To find its IP address, a newly-booted machine broadcasts a DHCP DISCOVER packet. The DHCP relay agent on its LAN intercepts all DHCP broadcasts.
- When it finds a DHCP DISCOVER packet, it sends the packet as a unicast packet to the DHCP server, possibly on a distant network. The only piece of information the relay agent needs is the IP address of the DHCP server.
- An issue that arises with automatic assignment of IP addresses from a pool is how long an IP address should be allocated. If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost. After a period of time, many addresses may be lost. To prevent that from happening, IP address assignment may be for a fixed period of time, a technique called **leasing**.
- Just before (or when half of) the lease expires, the host must ask the DHCP for a renewal.
- If it fails to make a request or the request is denied, the host may no longer use the IP address it was assigned earlier.

*Note: Version 2 is slightly more technical than Version 1.*

Both versions are, however, good and acceptable. DHCP supports the "lease" concept where a server can assign a client address for a certain time. DHCP can dynamically reconfigure networks that have more computers than available IP addresses with very short leases. For computers containing Web/Mail/DNS servers which require a permanent IP address, DHCP can still support static addresses.

## 2.9 Summary

This unit has provided with an overview of the various technologies that are needed for a full swing of IPv4 addressing scheme. The international standards of IEEE and ISO have been discussed. The frame format and different technologies. The various types of classes in terms of class A to Class E have been discussed along with the NAT and IP masquerading. The chapter ends with a description of different types of IP protocols

## 2.10 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 2.11 Activities

- Describe the different elements in an IPv4 protocol,
- Explain the various items in the IPv4 protocol header,
- Describe fundamental concepts of the Network Address Translation (NAT) & IP Masquerading,
- In addition to IP, which is used for data transfer, the Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP and DHCP
- Suppose there are many requests to the Internet (using 24.2.249.4). How does the NAT box know how to redirect these requests to their respective PCs?

## 3.1 Introduction

The TCP/IP model is the computer network model used today. In the 1970s it was founded as a model of open, vendor-neutral public networking by DARPA (Defense Advance Research Project Agency). The TCP/IP model offers general guidance on the design and implementation of network protocols, as does the OSI model of reference. There are only four layers of the TCP/IP model, compared with the OSI model. These layers describe various network functions and have own standards. The levels are as follows: Application, Transport, Internet and Link layer. This unit covers a description of the several layers along with critiques related to the OSI reference model.

## 3.2 Unit Objectives

- Explore the rationale of the TCP/IP,
- Recognise the fundamental concepts of layers in the TCP/IP reference model,
- Be able to distinguish between protocol and networks in the TCP/IP,
- Compare the OSI and TCP/IP Reference Models,
- Criticize the TCP/IP RM.

## 3.3 Rationale of TCP/IP

The TCP/IP protocol is the basis for the ARPANET, the forerunner of all Wide Area Computer Networks, including the worldwide Internet. ARPANET (Advanced Research Projects Agency Network) was a research network. Using leased telephone connections, it eventually connected hundreds of colleges and government locations. When satellite and radio networks were added later, the previous protocols couldn't communicate with them, necessitating the creation of a new reference architecture.

### 3.3.1 Design goals of a new architecture:

It is capable of seamlessly connecting multiple networks. The connectors remain intact while the source and target machines operate (survive loss of subnet hardware). The architecture is also flexible because applications have been envisaged with different requirements, from the transfer of files to the transmission of real time voice. After its two main protocols it was later known as the TCP/IP reference model (TCP and IP). The choice of a packet-switching network on a connectionless Internet layer led to all these requirements. The design of the architecture is shown in Figure 3.1

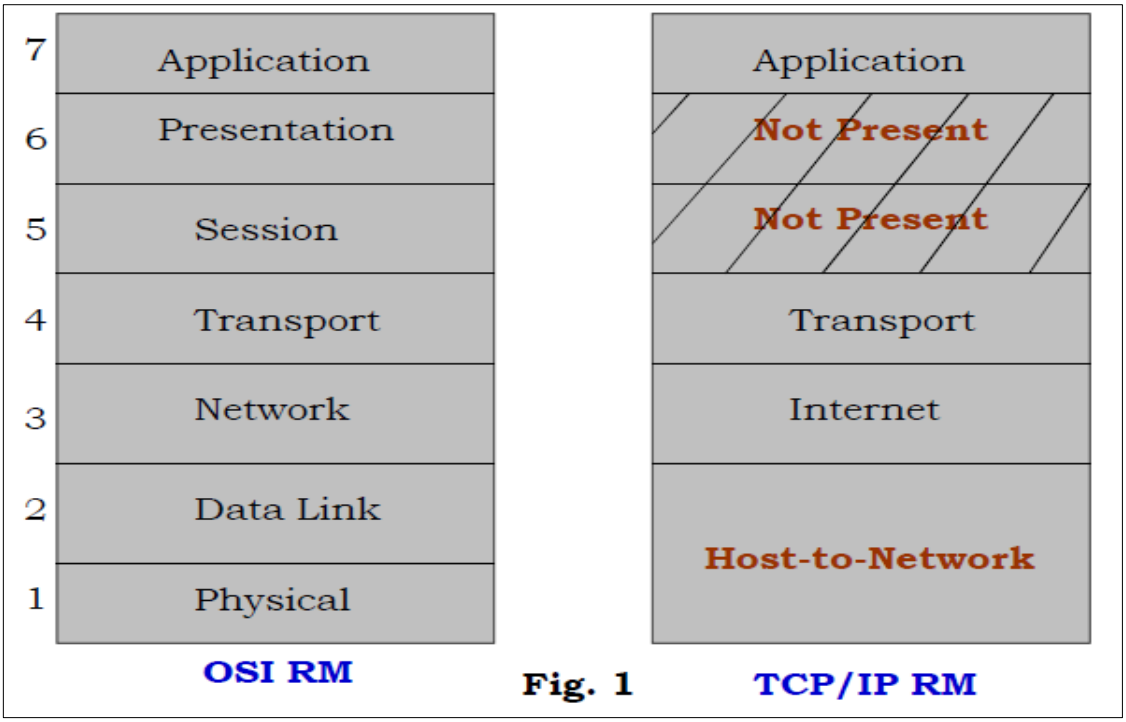



**Figure 3.1 - Diagrammatic illustration of the TCP/IP RM and OSI RM**

### 3.3.2 Layers of the TCP/IP RM: The Internet Layer

This is the main player holding together the entire architecture. The Internet Layer allows hosts to inject and travel packets independently to any network (potentially on a different network). In this case, it is up to higher layers to reorganize the packets even in a different order than they were dispatched if the delivery is desired. The web layer defines the IP format and protocol of an official packet (Internet Protocol). The task of the layer is to supply IP packets to the destination.

### 3.3.3 Layers of the TCP/IP RM: The Transport Layer

It is now usually called the transport layer above the internet layer of the TCP/IP model. It is meant to enable peer entities to conduct conversations in source and destination hosts (just as in the OSI transport layer). In the TCP/IP RM, there are defined two end-to-end transport protocols.

#### 3.3.3.1 TCP (Transmission Control Protocol)

TCP is a reliable connection-focused protocol that allows the delivery on any other machine without mistake of a byte stream originating on one machine. The byte stream is fragmented into discrete messages and passed on to the layer of the Internet. The receiving TCP process mounts the received messages back into the output stream at the destination. TCP also handles flow control in order to ensure that a quick sender is unable to swamp a slow receiver with more messages.

#### 3.3.3.2 UDP (User Datagram Protocol)

For applications that do not wish to provide TCP sequence or flow control, UDP is an unreliable, connectionless protocol. It's also widely used for one-stroke, customer poor response requests and applications where prompt delivery is more important than precise delivery, such as speech or video transmission. Figure 3.1 shows the relationship between IP, TCP and UDP. IP is implemented on many other networks since the model was developed.

### 3.3.3.3 Protocols and networks in the TCP/IP model

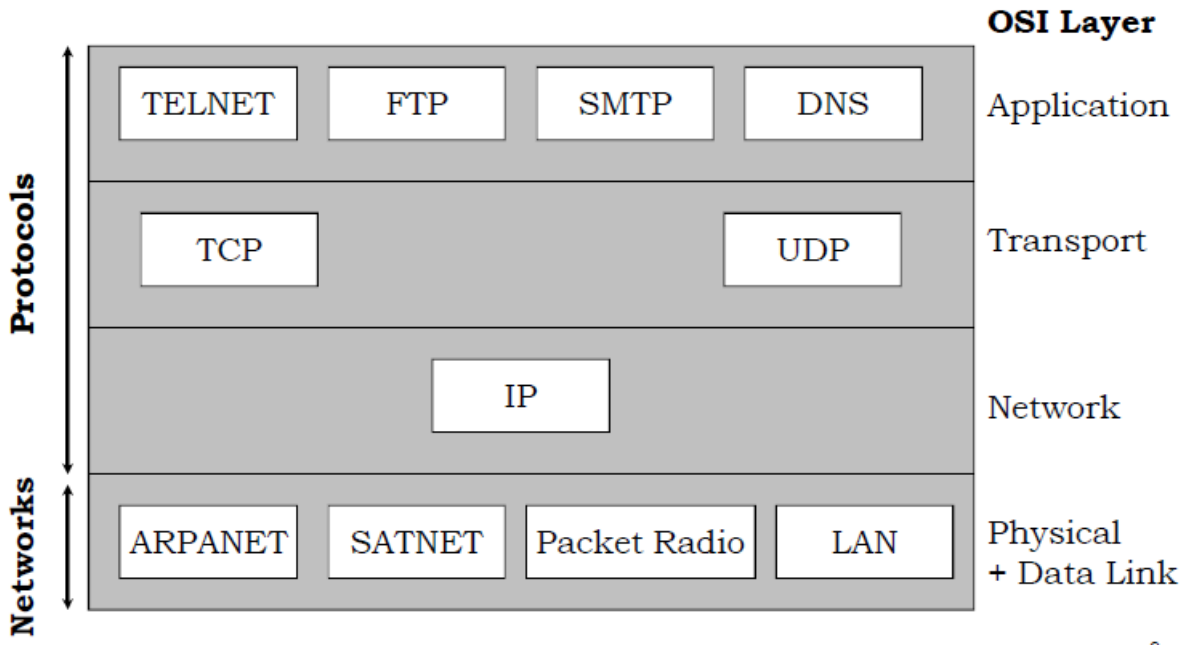



**Figure 3.2 – Relationship between layers in TCP/IP**

## 3.3.4 Layers of the TCP/IP RM: The Application Layer

There are no session or presentation layers in the TCP/IP model. There was no need for it, so it was not taken on board. This is the view demonstrated by experience in the OSI model: most applications are of little use. The application layer is located above the transport layer. All higher protocols: virtual terminal (TELNET), file transfer (FTP) and electronic mail are included in the application layer (SMTP). The protocol virtual terminal enables a user to log on and work on a remote machine on a single machine. The File Transfer Protocol allows data to be moved from one machine to another efficiently.

Electronic mail was originally a type of transferring of the file, but then it was developed into a specialized SMTP protocol. Over the years many additional protocols have been included: System domain name (DNS) on their network addresses for Mapping host names and HTTP – the World Wide Web pages collection protocol.

### 3.3.5 Layers of the TCP/IP RM: The Host-to-Network Layer

There's a great void under the internet layer. The model TCP/IP refers to nothing but to indicate that the host must connect to the network by using some protocol so that it can send IP packets. The protocol is not defined and varies by host and network.

## 3.4 Comparison of the OSI and TCP/IP Reference Models

The reference models OSI and TCP/IP share a great deal. Both are based on a stack of autonomous protocols concept. Corresponding layers have approximately similar functionalities. There is a complete, network-independent transport service in both models for processes that want to communicate, for example, through layers and including the carrying layer. The two models also differ in many ways, notwithstanding these fundamental similarities.

In the original case, the TCP/IP model does not clearly distinguish between the service, interface and protocol. For instance, "SEND IP PAC KET" and "RECEIVE IP PACKET" are the only real services provided by the Internet layer. The protocols in the OSI model are therefore better hidden than in the model of TCP/IP and can be replaced as technology progresses relatively easily.

Before inventing their respective protocols, the OSI reference model was designed. This order does not mean the model favoured a certain set of protocols, so that it is generally and adaptably. The reverse was true for TCP/IP: first were protocols and the model was only a description of the protocols that existed. The protocols fitting the model were not problematic. The only problem was that no other protocol stacks were in place. Consequently, other, non-IP (non-TCP/IP) networks were not particularly helpful for describing.

The OSI model supports connectionless communication on the network layer but only connections on the transport layer. The network layer is connected. The TCP/IP model supports only network-level connectionless mode, but both modes are supported in the transport layer and give users the choice.

## 3.5 Critique of the TCP/IP Reference Model

Firstly, the model does not make it clear that service, interface and protocol concepts are distinct. Good software engineering practice calls for the distinction between specification and implementation, which is very carefully performed by OSI and not by TCP/IP. The TCP/IP model is therefore not very much a guide to new networks with new technologies. Secondly, the TCP/IP model is generally unsuitable to describe any protocol stack other than TCP/IP. For example, it is entirely impossible to try to use the TCP/IP model to describe Bluetooth.

Thirdly, in the normal sense of the word in the context of layered protocols, the host-to-network laying is not really any layer. It's a crossover (between the network and data link layers). It is crucial to distinguish between an interior and a layer. Third, the TCP/IP model does not (or even mentions) differentiate between layers of physical and information link. They are totally different. The physical layer is related to copper wire, optic fiber and wireless communication characteristics. The job of the data connection layer is to determine the beginning and the end of frames with the necessary reliability from one side to the other. Both as separate layers should include a proper model. This is not the case with the TCP/IP model.

Finally, while IP and TCP protocols have been carefully developed and properly implemented, many other protocols have been ad hoc. Then the protocol implementation was freely distributed, leading to its widespread use, deep consolidation and thus difficult to replace. Some of them are now somewhat embarrassing. For example, TELNET was designed for a mechanical TV terminal of 10 characters per second. It doesn't know any graphical user and mouse interfaces. However, even nowadays it is still widely used!

## 3.6 Summary

Layered networking can be accomplished. Network designers organize protocols to reduce the complexity of design. Each layer follows a client and server end systems communication protocol. Each network entity has a part of layer n. Through messages, these parts communicate with each other. The layer-n data data units [n-PDU] refer to these messages. All necessary processes for effective communication are dealt with and divided into the layers of logical groups. The layered architecture is known if a communication system is designed in that way. The Model OSI represents a set of guidelines for the creation and implementation of network applications by network designers. It also offers a framework for networking standards, devices and internetworking systems. This paper discusses the differences between the TCP/IP model and the OSI reference model, which consists of 7 layers and 5 layers. The responsibilities of each layer are its own. For all communicating activities on the Internet, the TCP/IP reference model is a solid foundation. The unit explore the complex concepts of the TCP/IP and the OSI model.

## 3.7 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings

## 3.8 Activities

- Describe the different layers in the TCP/IP reference model,
- Compare and contrast between network and protocol in the TCP/IP reference model,
- Elaborate on the various critiques of the TCP/IP reference model.

## 4.1 Introduction

A number of technologies for connecting computers, systems and individual networks could be used for a WAN. The current technologies used differ. Current technologies – including circuit switching, frame switching, cell switching, X.25 switching, frame/cell switching, ATM and two other solutions – are summarized by Cisco Systems, Inc. These technologies administer the use of bandwidth by network applications and other details. The use of the First In-First Out (FIFO) method is for example a frame switching process so that no application could influence other applications' performance. The X.25 switch permits terminal devices to use any WAN protocol. There are advantages and disadvantages of each technology are discussed in this chapter.

## 4.2 Unit Objectives

- Recognise the need for connection oriented WAN services,
- Be able to discuss the X.25 Protocol,
- Explore the layered architecture in the Frame Relay,
- Describe the functions of the Digital Subscriber Line (DSL).

### 4.3.1 Connection-oriented WAN services: X.25

X.25 is the protocol standard for WAN communications for the International Telecom Union Telecommunications Standardization Sector (ITU-T). X.25 define how connections are established and maintained between user devices and network devices. X.25 is intended to function efficiently, irrespective of the type of network systems. Subscribers will be charged on the basis of their network utilization. In the 1970s, common carriers began to develop the X.25 standard. At the time, WAN protocols were needed that were able to connect over public data networks (PDNs). X.25 is now being managed by ITU-T as an international standard.

#### 4.3.1.1 X.25 Network Components

Network X.25 equipment is divided into three general classes:

1. Data Terminals Equipment (DTE) — DTE devices are end systems which communicate across the network of the X.25 devices. Terminals, personal computers, or network hosts are usually located at subscribers' premises.

2. Data Circuit Finishers (DCE) - Special communication devices such as modems are DCE devices (and packet switches). They provide the interface between DTE and Packet Switching Exchange (PSE) devices and are generally located on the operator's premises.

3. Packet exchange switching (PSE) - PSE is a switch which comprises the major portion of the network of the carrier. Data are transmitted from one DTE to another through the X.25 packet switched network (PSN).

Figure 4.1 shows the relationship between the three types of X.25 network devices:

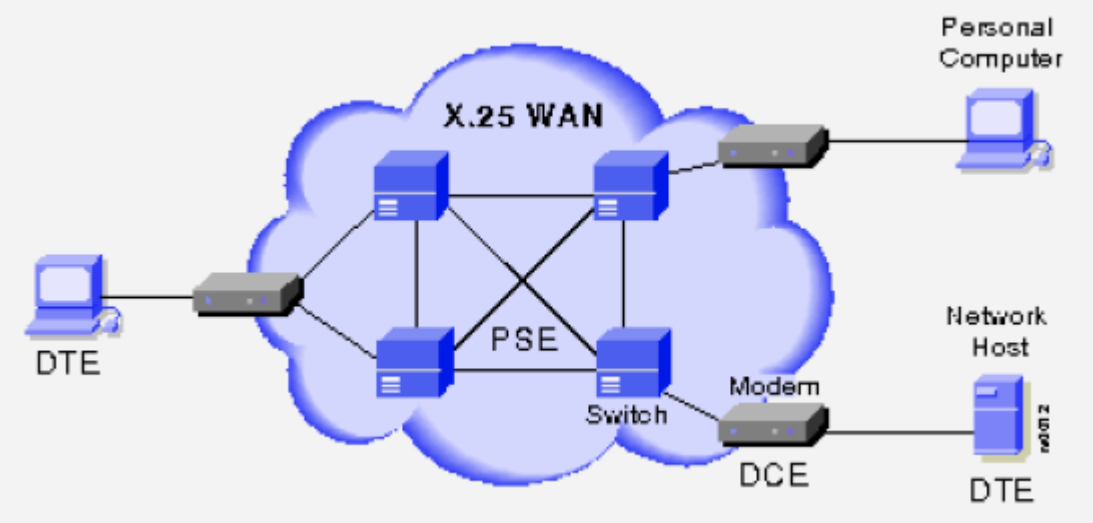



**Figure 4.1 – Types of X.25 network devices**

### 4.3.1.2 Packet Assembler/Disassembler (PAD)

A device common to X.25 networks is a packet assembler/disassembler (PAD) as shown in Figure 4.2. If the entire X.25 functionality can be implemented by using a DTE device (such as a character-mode end device). The PAD is between a DTE and a DCE device. Three main functions are performed:

1. **Buffering** - The PAD buffers data sent to or from the DTE device.
2. **Packet assembly** - The PAD assembles outgoing data into packets and forwards them to the DCE device. (This includes adding an X.25 header.)
3. **Packet disassembly** - The PAD disassembles incoming packets before forwarding the data to the DTE. (This includes removing the X.25 header.)

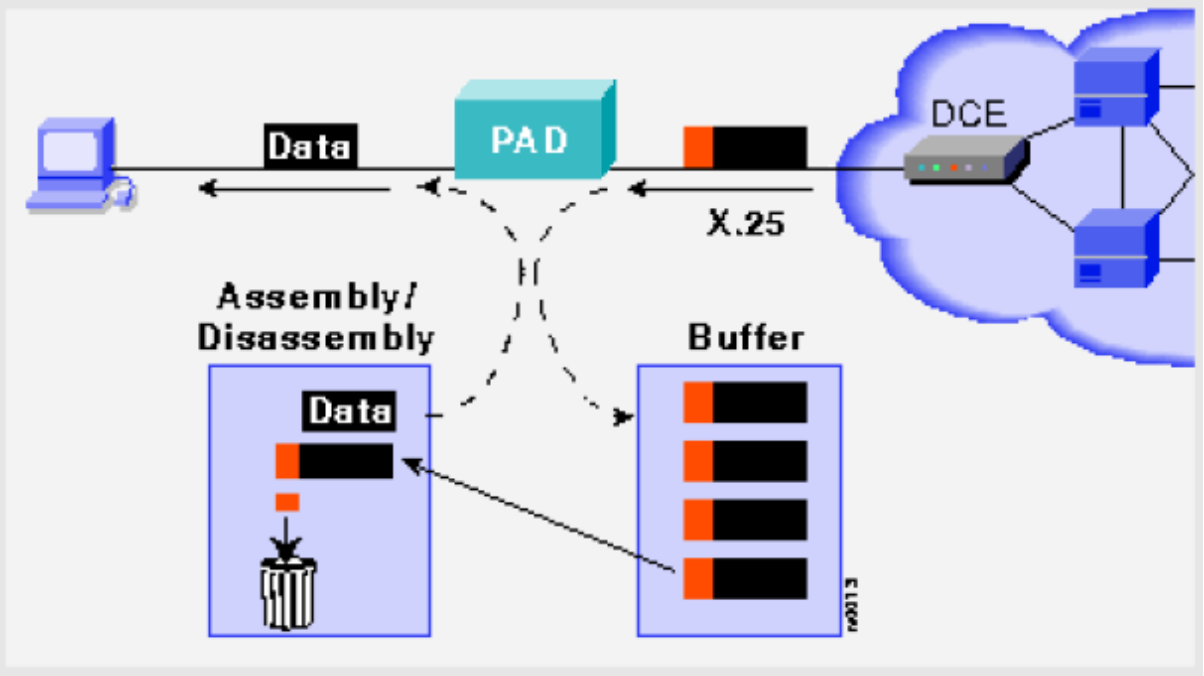



**Figure 4.2 – Packet Assembler/Disassembler**

### 4.3.2 Frame Relay

Frame Relays is a Wide Area (WAN) high performance protocol operated in the OSI (Open System Interconnection) reference model physical and data connection layers. Initially, the Frame Relay was designed to be used across the ISDN interfaces. It is also used today across a range of other network interfaces.

#### 4.3.2.1 Frame Relay Features

Frames Relay offers an interface between user and network devices for data communication. The basis for communication between user devices across the WAN is this interface. Typical speeds of communication are between 56 and 2 Mbps for frame relay (although lower and higher speeds are supported). Frame Relay is significantly more efficient than X.25, the so-called replacement protocol. Because it supports advances in technology, such as fiber optic cabling and digitized transmission, Frame Relay can eliminate time consuming processes (such as errors and flow control) needed to use older WAN media and protocols that are less reliable.

#### 4.3.2.2 Frame Relay Devices

WAN frame relay devices fall into two main categories:

- **Data terminal equipment (DTE)** - DTE are the custom end node and web-based devices. Terminals, computers, routers and bridges are examples of DTE devices.
- **Data circuit-terminating equipment (DCE)** - DCE are internet networking equipment owned by the company. These are packet switches in most cases (although routers or other devices can be configured as DCE as well). Logical entities are DTE and DCE devices. In other words, DTE devices initiate an exchange of communication, and DCE devices respond.

Figure 4.3 shows the relationship between the two categories of devices:

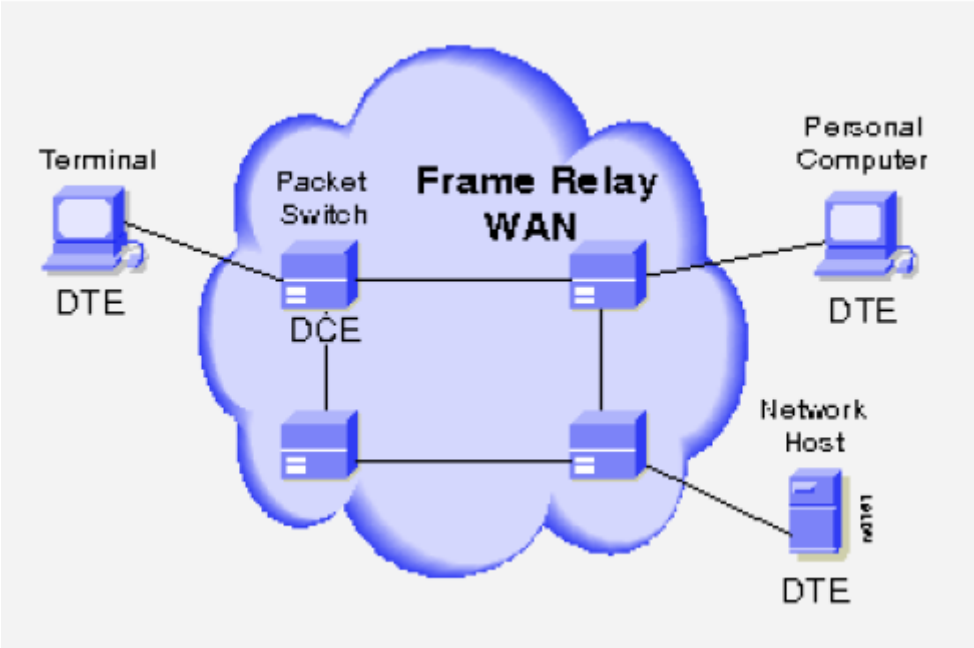



**Figure 4.3 – Relationship between DTE & DCE**

### 4.3.3 Digital Subscriber Line (DSL)

DSL is a technology for the telecommunications connection using existing lines of copper phones, offering a high-speed Internet. Some DSLs (particularly ADSLs) have the advantage of being able to co-exist in the same way as the traditional voice service "POTS," even ISDN. This is done by using various frequency ranges over the voice range (voice is up to 4KHz). In essence, two lines are provided: one for voice, and one for Internet connectivity. There should be no interference between the two "lines," if everything works normally. This provides DSL with a possible wide consumer base and helps to minimize service providers' costs. The DSL market, which seeking high speed Internet access at a reasonable price, is positioned for the Small Office and HOme market and (SOHO). It can also be used for connecting low to mid-range bandwidth servers and provides an easy-to-use solution for small LANs, as it typically provides "always-on" access.

### 4.3.4 ADSL

ADSL is similar to ISDN in several ways (Figure 4.4). The copper lines must be electrically "clean" for both technologies and can only be used within a limited distance from the local exchange of the telephone company. In many cases ADSL can operate on existing twisted telephone cables of twisted quality without disrupting the existing telephone connections - that makes it necessary to prevent local telephone companies from running additional lines in order to provide ADSL service. The principle of ADSL is to maintain at a time a high-speed data connection, because the voice does not use any of the bandwidth available from a standard twisted copper pair line. For this purpose, ADSL splits only the lower 4KHz channel for the Plain Old Telephone System (POTS), faxes and analogue modem data in the maximum 1MHz bandwidth of a copper wire connection. For parallel digital communication, the other 256 available channels are used. Asymmetrical, the downlink uses 192 4KHz channels and only the uplink uses 64. Thus, ADSL can be considered simply to take and transform into a parallel string a serial string of digital data, thus increasing the data output.

This modulation technique is referred to as the Discrete Multitone (DMT), the coding and decoding is performed in the same way as the conventional dial-up modem, at the exchange and user end. The only additional subscribers to equipment needed for using ADSL was an ADSL modem when the service was first available for commercial use.

Three connectors are needed: a standard RJ11 telephone jack for analogue telephone service and an Ethernet twisted-pair connector connecting ADSL modem to a PC is needed to the wall jack then out to the phone company.

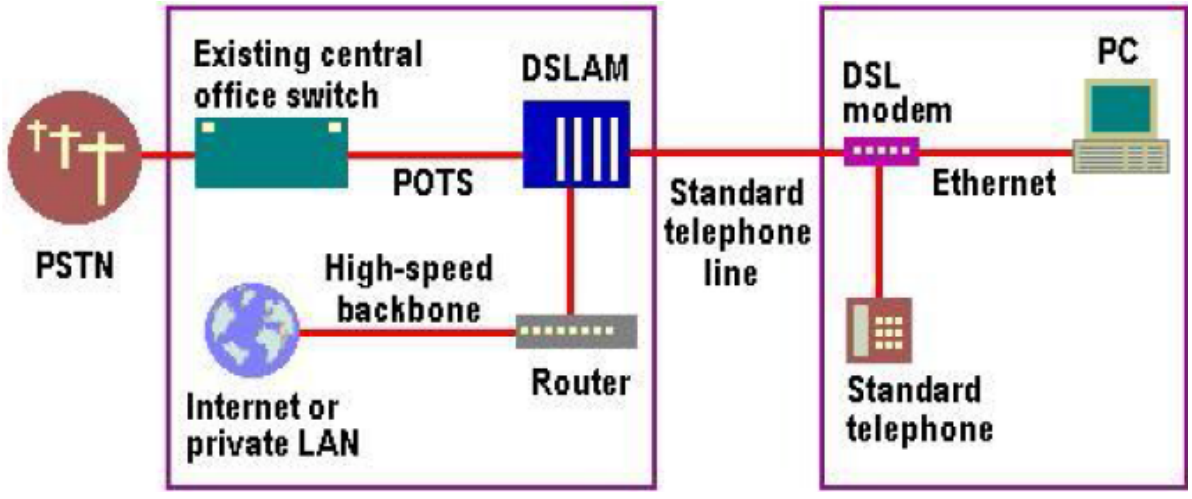



**Figure 4.4 – ADSL Connection**

At the end of the operator the ADSL modem collects and assembles high-frequency digital data for PC or network transmission. At the exchange point, the DSLAM connects an ADSL user to a wider internet, adding incoming ADSL lines into a single data connection to transmit on voice and data networks. DSLAM connects to the Internet. The telecommunications are sent to the Internet via a high-speed backbone via the switched telephone and the digital data routed (implemented as T1, fibre, ATM, or DSL). ADSL modems are now available in a number of forms and have evolved over the years. Others connect via Ethernet to a PC via a USB port.

Most devices permit Internet access on multiple PCs. Integrated modem/routers support a network of PCs, some of which are supported by an integrated firewall that provides various levels of protection. Actual efficiency ratings depend on a range of external factors: copper line length, wire gage, bridged taps, and interference cross-coupling. Line attenuation with length and frequency increases and decreases as the diameter of the wire increases.

The following is done by ADSL:

| **Data Rate** | **Wire Gauge** | **Wire Size** | **Distance** |
|---|---|---|---|
| 1.5/2 Mbit/s | 24 AWG | 0.5mm | 5.5 km |
| 1.5/2 Mbit/s | 26 AWG | 0.4mm | 4.6 km |
| 6.1 Mbit/s | 24 AWG | 0.5mm | 3.7 km |
| 6.1 Mbit/s | 26 AWG | 0.4mm | 2.7 km |

## 4.7 Summary

ADSL - Asymmetric Digital Subscriber Line is a Copper based High speed network access technology. It is a rapidly growing broadband access solution for home networking and small business systems. It uses multi-carrier modulation over unused frequency bands in phone lines and supports data rates up to 6144 Kbps downstream and 640 Kbps upstream. The chapter provides a broad description of the various connection oriented WAN networks.

## 4.8 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 4.9 Activities

- Elaborate on the components of the X.25,
- Use a diagram to show the different devices in the X.25 protocol,
- Describe the difference between packet assembler and disassembler,
- Differentiate between frame relay and DSL.

## 5.1 Introduction

Technologies that fragment data into small parts are typically extremely poor because when a piece of data is lost in transit, no mechanism is available to detect and retransmit lost cells. The only way for the damaged cell to be recovered is to forward the whole large packet back. An alternative to retransmit the whole packet inefficiently is to transmit only the lost or damaged individual cells. The ATM technology only allows cells in each packet that have not been received properly to be retransmitted. The transmission performance is also improved by decreasing the flow control requirements at each network connection.

## 5.2 Unit Objectives

- Recognise the switch to ATM,
- Be able to distinguish the various layers in the ATM,
- Explore the format of ATM,
- Describe the difference of ATM interface specifications for private and public networks

## 5.3 ATM – Asynchronous Transfer Mode

The Asynchronous Transfer Mode (ATM) is the cellular ITU-T standard where the information for several different service types, such as voice, video or data are transferred to small fixed-size calls. This is an International Telecommunication Union-Telecommunications Standards (ITU-T). Connection-oriented are the ATM networks. The following section summarizes the protocols, services and operations of ATMs.

Figure 5.1 depicts an example of a private ATM network and a public ATM network carrying voice, video & data traffic.

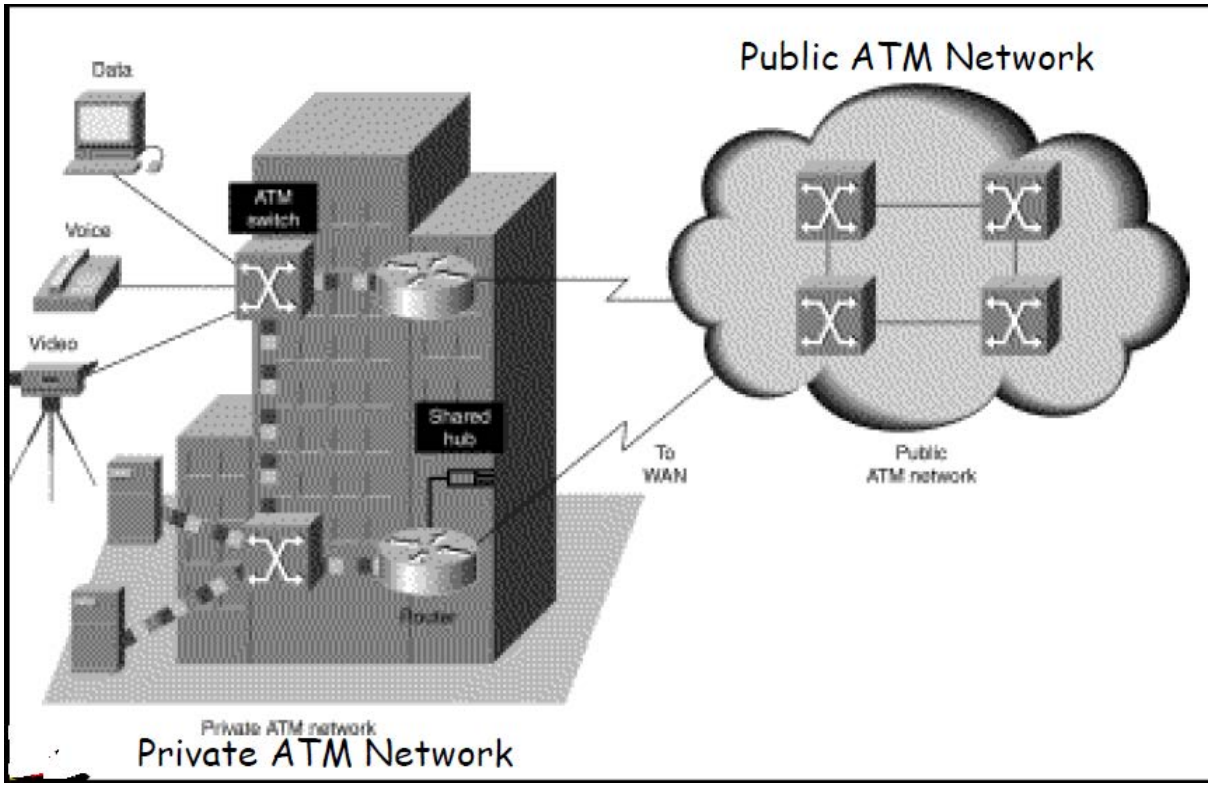



**Figure 5.1 – Example of an ATM**

### 5.3.1 ATM Standards

The ITU-T Integrated Digital Network of Integrated Services (B-ISDN) standard is used to support ATM. It was originally designed for the transfer of voice, video and data through public networks as high-speed technologies. The ITU-T vision on ATM was extended to include public and private networks in the ATM Forum. The work on the following specifications has been released by ATM Forum:

- User-to-Network Interface (UNI) 2.0
- UNI 3.0
- UNI 3.1
- UNI 4.0
- Public-Network Node Interface (P-NNI)
- LAN Emulation (LANE)
- Multiprotocol over ATM

### 5.3.2 ATM Devices in the Network Environment

The ATM is a cellular switching and multiplexing technology, which combines the advantages of circuit switches with packet switches (guaranteed capacity and constant transmission delays) (flexibility and efficiency for intermittent traffic). It provides a scalable bandwidth of several megabits per second (Mbps) (Gbps). A Timing Division Multiplexing (TDM) is more efficient because of the asynchronous nature of ATM than sync technologies.

Every user has a time slot with TDM and in that time it cannot be sent by any other station. 1 When a station has a lot of data to send, it can only send when the time slot is up, even if all other time slots are empty. When the time slot comes up, the time slot is sent out empty and destroyed if a station does not have anything to transmit. As ATM is asynchronous, time slots with the source of the transmission in the header for each ATM cell are available on request.

TDM assigns each user to a time slot. No station in this time slot can send it. If you want to send a station a lot of data, it can only send when the slot has arrived, even when all other slots are empty. But if a station has nothing to transmit when its time slot arrives, the time slot is empty and wasted. Because ATM is asynchronous, time slot data identifying the transmission source in the header of every ATM cel may be obtained on request.

### 5.3.3 Basic ATM Cell Format

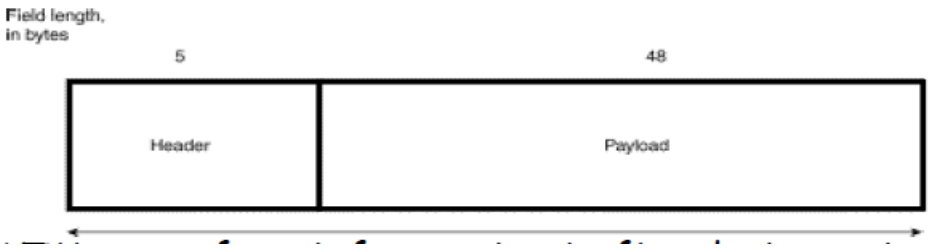



**Figure 5.2 – ATM Cell format**

In fixed-size units called cells, ATM transfers the information as depicted in Figure 5.2. There are 53 bytes in each cell. The first 5 bytes contain information about the cellular header, while the other 48 contain payload (user information). Why is ATM using small cells of fixed dimensions? Small, fixed cells are ideal for transfers of voice and video transmission since this kind of traffic is intolerant of delays caused by waiting to download, among other things, a large data packet.

### 5.3.4 ATM Devices

An *ATM network* is made up of an *ATM switch* and *ATM endpoints*. A cell transit via the ATM network is managed by an ATM switch. The work of an ATM switch is defined: the input cell from an ATM end point is accepted (or from another ATM switch). Then the cell header information is read and changed and the cell switches quickly to the output interface. An ATM endpoint (or end system) has an ATM network adjuster. For example, work stations, routers, digital service devices (DSUs), LAN switches and video code decoders are the examples of ATM endpoints (CODECs). An ATM network made up of ATM switches and ATM endpoints as shown in Figure 5.3

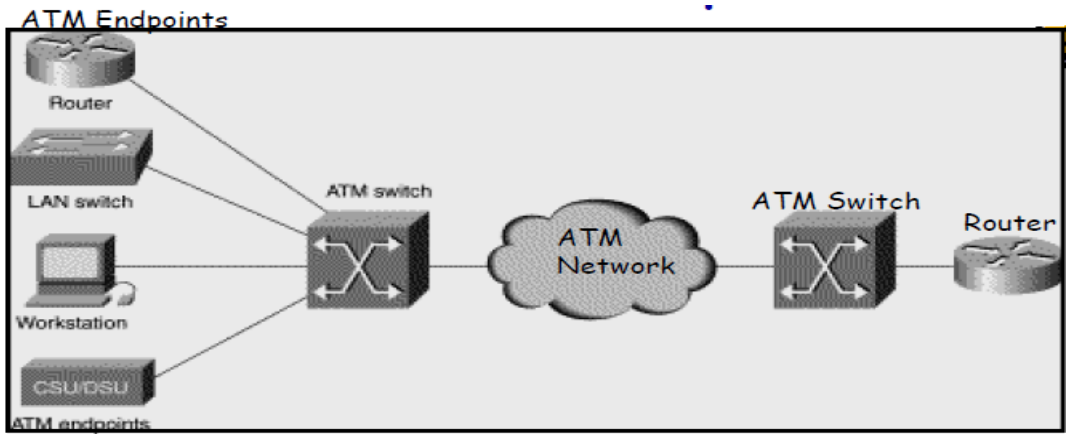



**Figure 5.3 – ATM Devices**

### 5.3.5 ATM Network Interfaces

An ATM network consists of a set of ATM switches connected via ATM interfaces or dot-to-dot connections. Two main interface types are supported by switches ATM: UNI (Network Interface User) and NNI (Network Node Interface). The UNI connects an ATM switch to ATM end systems (e.g. hosts and routers). Two ATM switches are connected to the NNI. The UNI and NNI are able to be further subdivided into public- and private UNIs and NNIs, depending on whether this switch is owned and located at the client's premises or is publicly owned and operated by the telephone company.

An ATM endpoint and a private ATM switch are connected by a private UNI. Its public counterpart (public UNI) links a public switch with an ATM terminal (or a private switch). Two ATM switches within one private organization are connected to a private NNI. A public NNI connects the same public organization with two ATM switches. The Broadband Intercarrier Interface (B-ICI) provides two public switches from different service providers. An additional specification is provided. Difference of the private and public network ATM interface specifications is shown Figure 5.4

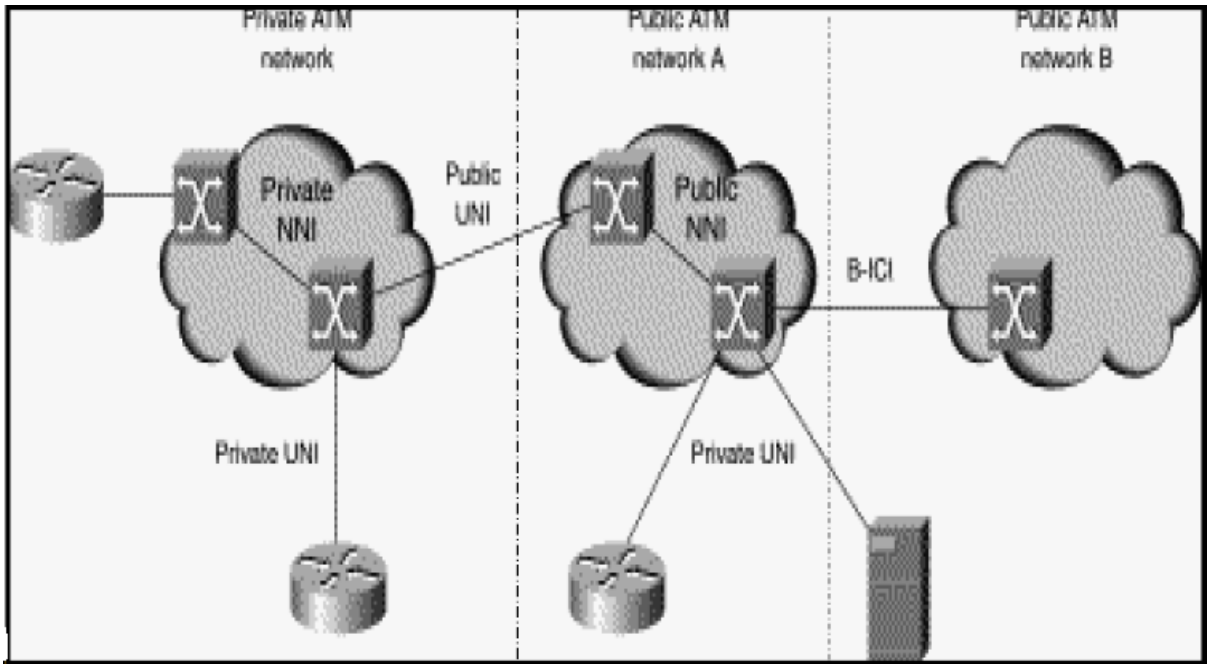



**Figure 5.4 – ATM Interface**

### 5.3.6 ATM Cell Header Format

One of two formats may be an ATM cell header: UNI or NNI. The UNI header is used in private ATM networks to communicate between ATM ends and ATM switches. This NNI header is used for ATM switch communication as shown in Figure 5.5

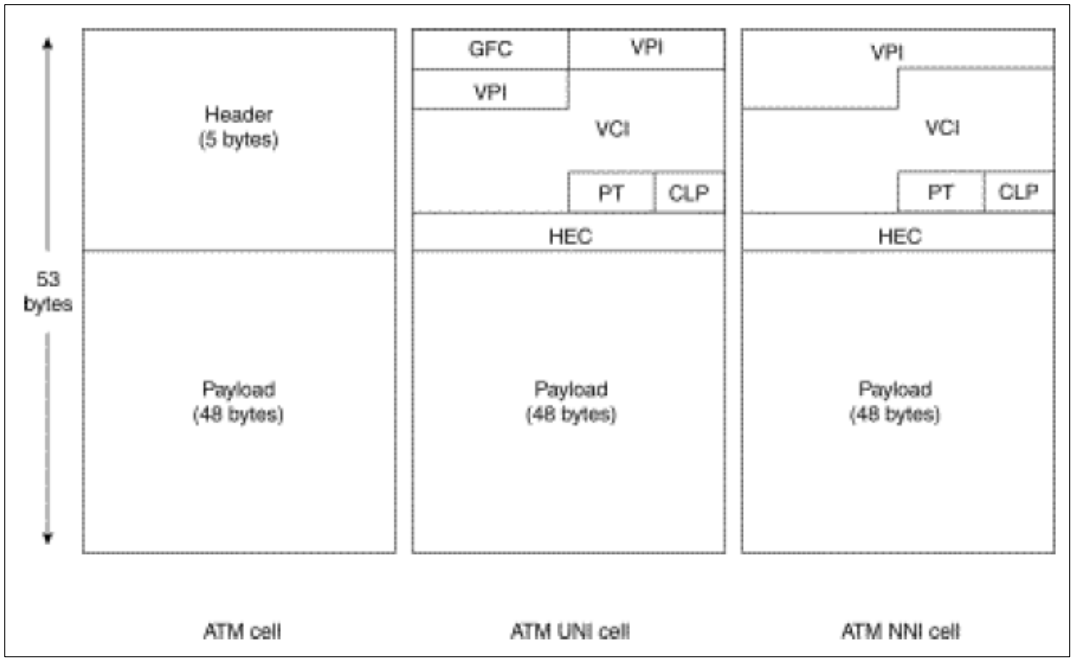



**Figure 5.5 – ATM cell header format**

In contrast to UNI, the Generic Flow Control (GFC) field does not appear in the NNI header. The header also has a VPI field that covers the first 12 bits, which allows for bigger trunks between public ATM Switches. In addition, the NNI header has a Virtual Path Identifier (VPI) field.

### 5.3.7 ATM Cell Header Fields

Although several others are used in the fields of the ATM cell header in addition to GFC and VPI header. Figure 5.5 summarizes the following descriptions of the ATM cell header fields:

- **Generic Flow Control (GFC)—** Provides local functions, such as the identification of multiple ATM interface stations. This field is not normally used and is default to 0. (binary 0000).

- **Virtual Path Identifier (VPI)—** When the VCI passes through a series of ATM switches on its path, the next target of the cell will be identified.

- **Virtual Channel Identifier (VCI)—** When the cell passes through a series of ATM switches on the way to the cell's destination, it identified the next destination with the VPI.

- **Payload Type (PT)—** Indicates whether the cell contains user data or control data in the first bit. The bit is set to 0 if the cell contains the user data. The control data is set to 1. If it contains control data. In addition, the third bit shows whether the cell is last in a number of cells that show one single AAL5 frame (1= last cell for a frame). The second bit indicates the amount of congestion (0 = no congestion, 1 = congestion).

- **Cell Loss Priority (CLP)—** Indicates if the cell must be removed if the network is confronted with extreme congestion. If the CLP bit is equal to 1, cells with the CLP bit equal to 0, should preferably be discarded from the cell.

- **Header Error Control (HEC)—** Only the first 4 bytes of the header are calculated for checksum. In these bytes, HEC can remedy a single bit error by preserving the cell instead of discarding it.

## 5.4 ATM Services

Two types of ATM services exist: (1) Permanent Virtual Circuits (PVC) – for **manually** routed connections, (2) Switched Virtual Circuits (SVC) – for **dynamically** routed connections.

• **PVC -** It provides for site-to-site connectivity. A PVC is like a leased line in this manner. PVC ensures a connection available and does not require call setup procedures between switches, among its advantages. PVCs inconvenience is that there is manual set-up and static connectivity. The PVC must be supplied manually with each equipment between the source and the destination. In addition, PVC is not available for any network resilience.

• An **SVC** is created and released dynamically and remains in use only as long as data is being transferred. It is like a telephone call in this sense. A signal protocol between the ATM end pointer and the ATM switch is required for dynamic call control. The advantages of SVCs are that there is flexibility in connection and call-setup that a networking device can process automatically. Disadvantages are that additional time and overhead for connection establishment is required.

## 5.4 ATM Virtual Connections

ATM networks are basically link-oriented and therefore, before the data is transferred, a virtual channel (VC) should be established on the whole ATM network. (A virtual canal equals a virtual circuit approximately.)

Two types of ATM connections exist:

- virtual paths identified through VPIs, and
- virtual channels identified via a VPI and Virtual Channel Identifier combinations (VCI).

A virtual path is a bundle of virtual channels, which are all transparently switched on a VPI based basis over the ATM network. However, all VPIs and VCIs only have local significance across a certain connection and are reworked on every switch if necessary. The physical media which carries virtual channels and virtual paths are a transmission path. Figure 5.6 that follows illustrates how VCs concatenate to create VPs, which, in turn, traverse the media or transmission path.

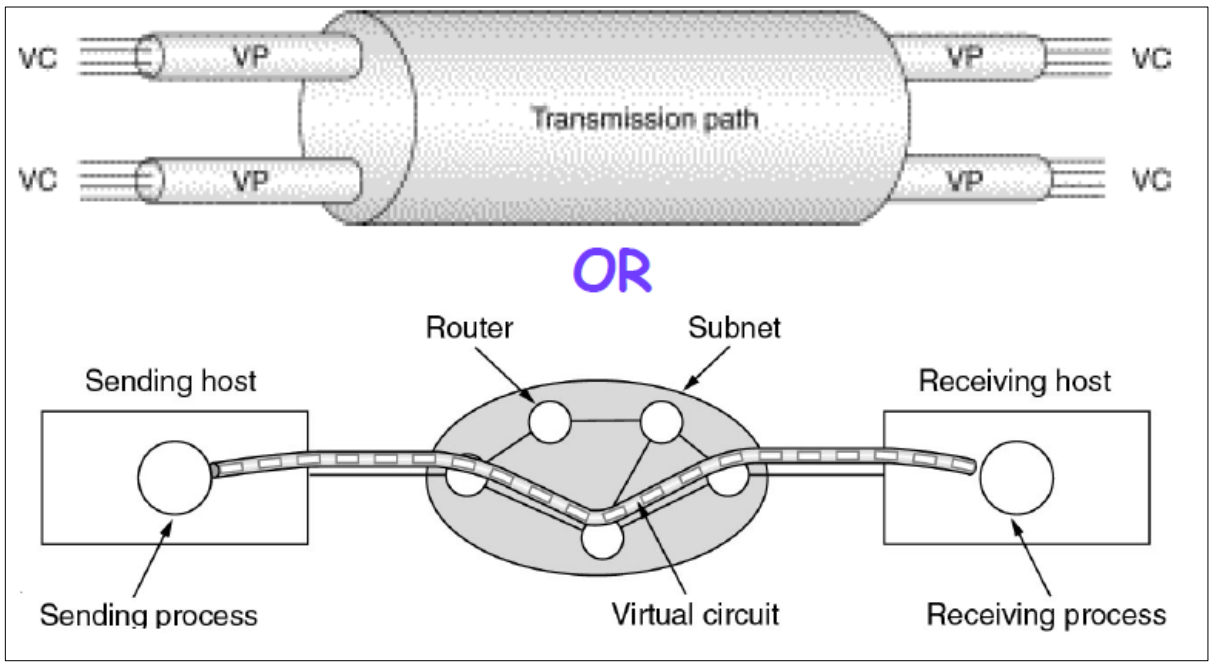



**Figure 5.6 - How Virtual Circuits (VCs) Concatenate to Create Virtual Paths (VPs)**

## 5.5 ATM Switching Operations

The ATM switch's essential operation is simple: A link on a known VCI or VPI value is provided to the cell. In order to identify the outgoing ports of the connection and the new VPI/VCI value on the connection on that connection the switch looks up the connectors value in a local translation table. The switch retransmits the cell with the relevant connection identifiers on the outgoing connection. Since all VCIs and VPIs have local relevance throughout a particular link, these values are kept for each switch as necessary.

The ATM architecture as shown in Figure 5.7 uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model. The ATM reference model is composed of the following planes, which span all layers:

- Control - This plane is responsible for generating and managing signaling requests.
- User - This plane is responsible for managing the transfer of data.
- Management - This plane contains two components: – Layer management manages layer-specific functions, such as the detection of failures and protocol problems. Plane management manages and coordinates functions related to the complete system.

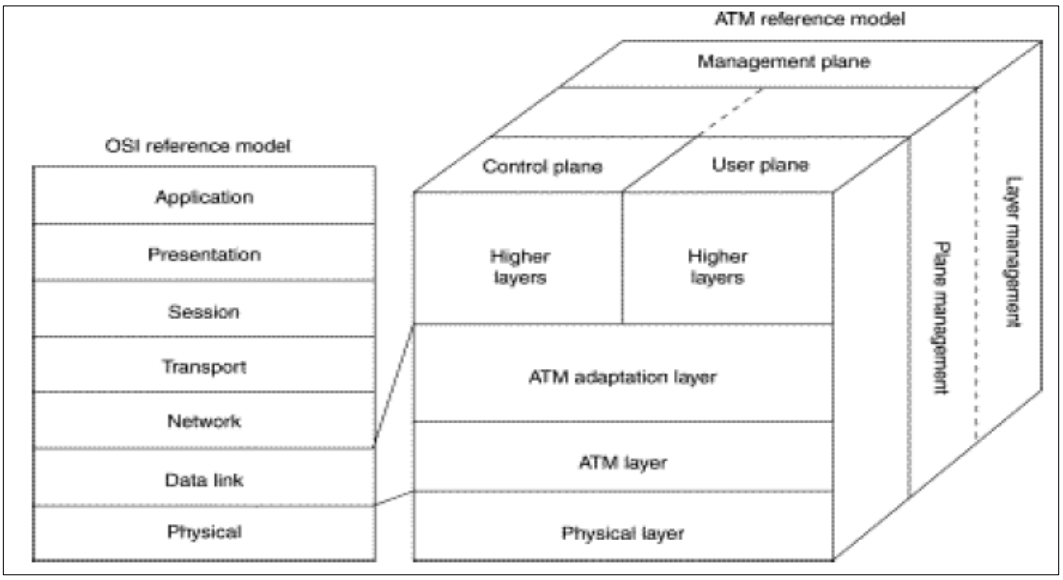



**Figure 5.7 - OSI Reference Model and ATM Reference Model**

## 5.6 Layers in ATM Reference Model

The ATM reference model is composed of the following ATM layers:

- **Physical layer -** The physical layer of ATM manages medium-dependent transmission similar to the physical layer of the OSI reference model.

- **ATM layer** - The ATM layer is roughly analogous to the data-connection layer in the OSI model, in combination with the ATM adaptation layer. The ATM layer ensures that virtual circuits are shared over a physical connection (cells multiplexing) and cells pass through the ATM network (cell relay). For that to happen, the header of each ATM cell uses the VPI and VCI information.

- **ATM adaptation layer (AAL)** - The AAL is roughly analogous to the OSI model's data link layer together with the ATM layer. The AAL is responsible for the isolation from the details of ATM processes of higher layer protocols. The adaptive layer prepares user data for cell conversion and divides data into cell 48-byte payloads.

- Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

## 5.7 Summary

ATM is a leading enabled communications technology at its current stage in the evolutionary technological development, providing users and network providers with new applications and providing greater bandwidth to networks. Becoming the leading infrastructure for delivering almost all kinds of communications, including data, voice, image and multimedia, to buildings and desktops around the world, ATM has high bandwidth capabilities and cells-oriented architecture. The telecommunications industry has taken a very careful look at critical performance and adapted existing legacy systems to the implementation of ATMs, ensuring that the ATM not only will be the future design solution but will today also be able to provide cost-effective applications.

## 5.8 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings

## 5.9 Activities

- Describe the different layers in the TCP/IP protocol suite,
- Explain the difference between OSI and TCP/IP protocol suite,
- Describe fundamental characteristics of how communication takes place at the application layer,
- Differentiate between UDP and TCP,
- Elaborate on the need for IP and datagrams.

## 6.1 Introduction

Transmission media are the physical pathways that connect computers, other devices and network people (guided or unguided). The signals are used for data representation by computers and telecommunication devices. These signals are transmitted by electromagnetic energy from device to device. Electro power, radio waves, infrastructure, visible light, ultraviolet, and X and gamma rays are examples of electromagnetic energy. The electromagnetic spectrum is all these electromagnetic signals. In order to transfer data such as twisted pair, coaxial cable, optical fibers, satellite and wireless etc., every spectre portion requires a certain or unique transmission media.

## 6.2 Unit Objectives

- Recognise the history of bandwidth and transmission media,
- Be able to understand the Henry Nyquist channel,
- Describe the different network transmission media,
- Differentiate between twisted pair, coaxial and optical fiber.
- Explore the need for total internal reflection of light,
- Explain the different fiber optics network.

## 6.3 Bandwidth and Transmission Medium

Without losing any power in the process, no transfer facility can transmit signals. All transmission plants, unfortunately, reduce the various components by various quantities and therefore cause distortion. In general, the amplitudes are transmitted without decreasing from 0 to certain frequency fc [measuring in cycles/second or Hertz (Hz)] attenuated by all frequencies above that cutoff frequency. The bandwidth is called the range of transmitted frequencies without being strongly attenuated. In practice, the cut is not very sharp, so the quoted bandwidth is frequently 0 to half the power. The bandwidth is a physical property of the medium and is typically dependent on its construction, thickness and length. In some situations, a filter is added to the circuit in order to limit every customer's bandwidth.

## 6.4 The Maximum Data Rate of a Channel

An AT&T engineer, Henry Nyquist, realized that a finite capacity even for a perfect channel. He derived the equation for a finite bandwidth that is noiseless to the maximum data rate. Nyquist has proven that if a low-pass H bandwidth filter has been used to execute an arbitrary signal, only 2 H (exact) samples per second can fully reconstruct this filtered signal. Where V levels are the signal, Nyquist's theorem says: Signal:

**Maximum data rate for a noiseless channel =2H $log_2$V bits/sec**

H=bandwidth, V=transmission speed

If random noise is present, the situation deteriorates rapidly.

The amount of thermal noise present is measured by **the ratio of the signal power to the noise power**, called the **signal-to-noise ratio**. If we denote the signal power by S and the noise power by N, the signal-to-noise ratio is S/N. Usually, the ratio itself is not quoted; instead, the quantity 10 log10 S/N is given.

Claude Shannon carried Nyquist's work further and extended it to the case of a channel subject to random (that is, thermodynamic) noise. Shannon's major result is that the maximum data rate of a noisy channel whose bandwidth is H Hz and whose signal-to-noise ratio is S/N, is given by:

**Maximum data rate for a noisy channel=H $log_2$ (1+S/N) bits/sec**

H=bandwidth, S/N= signal-to-noise ratio

**The above is more commonly known as Shannon's Law (for a noisy channel)**

## 6.5 Network Transmission Media

The data are converted to electrical signals throughout the network. These signals are generated by analog signaling, electromagnetic waves, or as voltage pulses sequence (digital signaling). A signal must travel along a physical path, if it is to be sent from one place to another. The physical path used to signal the transmission media between a signal transmitter and a signal recipient (media). The physical layer has the purpose of transporting a crude bit stream between machines. For the actual transmission, different physical media can be used. Each has its own bandwidth, time, installation and maintenance facilities. Two types of media are available: guided and unguided. Guided media included copper wire and fibre while unguided media included radio waves and air lasers.

### 6.5.1 Guided Media

Guided media are produced in order to contain signals and behave predictably in a narrow way. Twisted pair cables, coaxial cables and optical fiber cables are the three most frequency types of guided devices.

### 6.5.2 Twisted Pair

Twisted pair (as shown in Figure 6.1) wiring refers to a cable type made up of two (or more) copper wires in a plastic sheath, twisted around one another. The wires are twisted in order to reduce electrical interference from one cable to the next. The variety of twisted pair cables is "shielded" and "unshielded." Shielded cables (SCCs) have an electromagnetic interference shield enclosing the cables. The most common in the business world is unshielded twisted pair cable (UTP), which is cheap and highly flexible. Unscheduled twisted pair is available in five categories ranging from 1 to 100 megabits per second in speed.

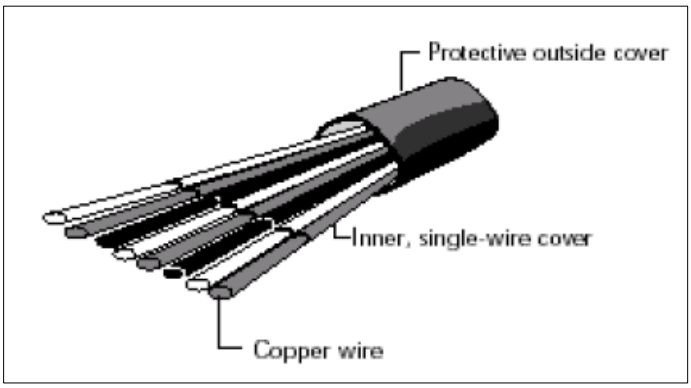



Figure 6.1 – Twisted Pair

**The following categories exist:**

| **STP** | **Maximum Data Rates** |
|---|---|
| IBM Type 1 | 100 Mbps |
| IBM Type 2 | 16 Mbps |

| **UTP Type** | **Maximum Data Rates** |
|---|---|
| Category 1 | 4 Mbps |
| Category 2 | 24 Mbps |
| **Category 3** | **10 Mbps** |
| Category 4 | 16 Mbps |
| **Category 5** | **100 Mbps** |

Category 5 twisted pairs are similar to category 3 pairs, but with more twists per centimeter, which results in less crosstalk and a better-quality signal over longer distances, making them more suitable for high-speed computer communication. Up-and-coming categories are 6 and 7, which are capable of handling signals with bandwidths of 250 MHz and 600 MHz, respectively (versus a mere 16 MHz and 100 MHz for categories 3 and 5, respectively). Figure 6.2 depicts the category 3 and 5.


**Figure 6.2 - Category**

### 6.5.3 Coaxial Cable

It contains a coaxial cable, which carries the signal and is enclosed by a concentration-physical channel consisting of a film or a cable mesh. This is known as the "coaxial" cable. As a basis for electrical interference, the exterior channel. Thanks to this grounding feature, multiple coaxial cables can be placed in a single pipe or sheet without significant data integrity loss. Two different types of coaxial cable are divided – the Thinnet and Thicknet. Thinnet coaxial cable (Thin Coax/10Base2) The cable used by cable TV companies is similar. It's not as flexible as twisted pairs, but still used in LAN applications. Thicknet (Thick Coax/10Base5) is similar to the thinnet but in diameter it's larger. The size increase means that the maximum distance between two network devices is increased. However, the disadvantage of increasing size is a loss of flexibility. Because thicknet is considerably harder than thinnet, the potential for deployment is much smaller. Thicknet is mainly used as a network backbone for the various network components, with thinnet branches.

A coaxial cable is made from a stiff, insulating material, copper cable as a core. The insulator is enclosed as a twisted mesh by a cylindrical conductor. A protective plastic sheath covers the outer conductor. Figure 6.3 shows a cut-off view of a coaxial cable.

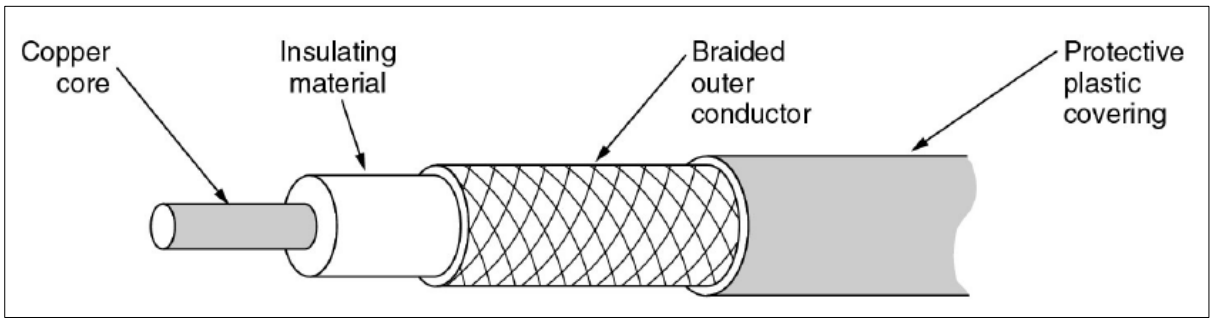



**Figure 6.3 – Coaxial Cable**

### 6.5.4 Fiber Optic Cable

The optical fiber cable (Figure 6.4), better known as the fiber optic, transmits data with low data integrity over very long distances. Moreover, as the data is transmitted instead of as an electro-pulse, the electromagnetic interference of optical fibres. The light pulses are enclosed in an insulating sheet in a glass or plastic wire or fiber. Optical fibers are more fragile than wire, are hard to split and have a lot to work on. There is therefore a main use of optical fibers to transmit long-range data, where the hardware to relay the data signal on lower cost media would be higher than the cost of optical fiber installations. It is also used where very large amounts of data need to be transmitted on a regular basis. An optical transmission system has three key components:

- a light source
- a transmission medium and
- a detector.

A pulse of light usually shows a 1 bit and a missing light shows a 0 bit. The medium is an ultra-thin glass fiber. When light falls on it, the sensor produces an electrical pulse. By mounting a light source on one side of the optical fiber, and a detector on the other side, we have a unidirectional data transmission system that accepts, converts and transmits electrical signals by light pulses and then transfers the output on the receiving end to an electric signal.

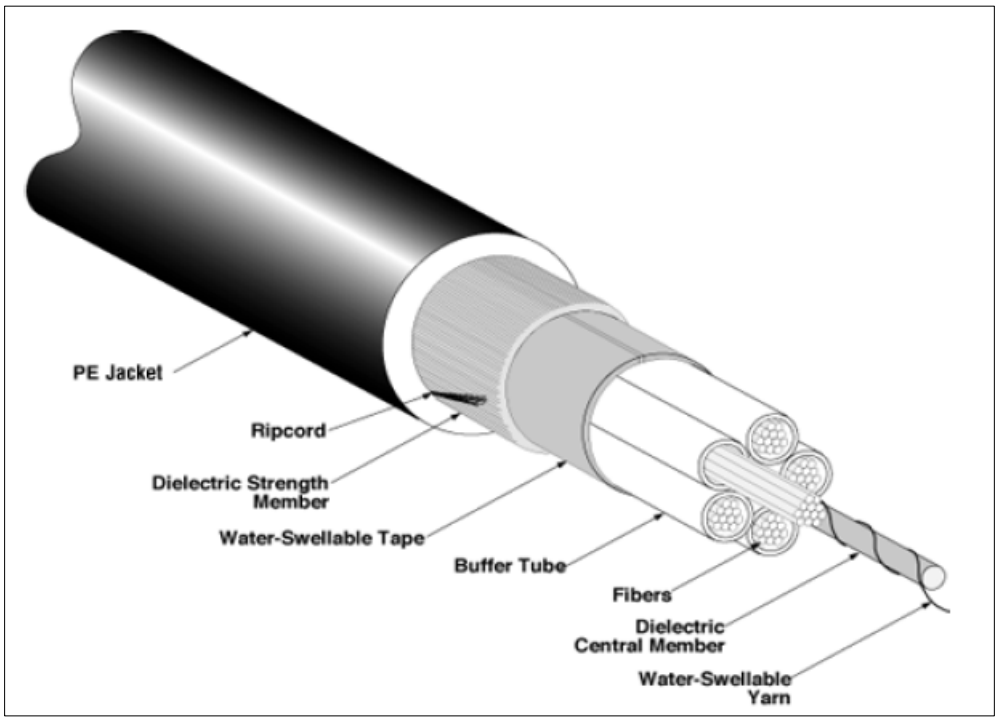



Figure 6.4 – Fibre Optical Cable

### 6.5.4.1 Total Internal Reflection of Light

For example, when a light ray passes from a fused silica into the air, at the silica/air frontier, the ray is refracted (bound), as shown in the Figure (a). Here we see a light ray occurrence at an angle of α1 that emerges at an angle β1 at the border. The refraction rate depends on the characteristics of the two media (in particular, their indices of refraction). The light is refracted into the silica at angles above a certain critical value; none of it escapes into the air. Thus, a light ray incident **at or above** the critical angle is trapped inside the fiber, as shown in Figure (b) and can propagate for many kilometers with virtually no loss. Figure 6.5 shows an example of reflection of light.

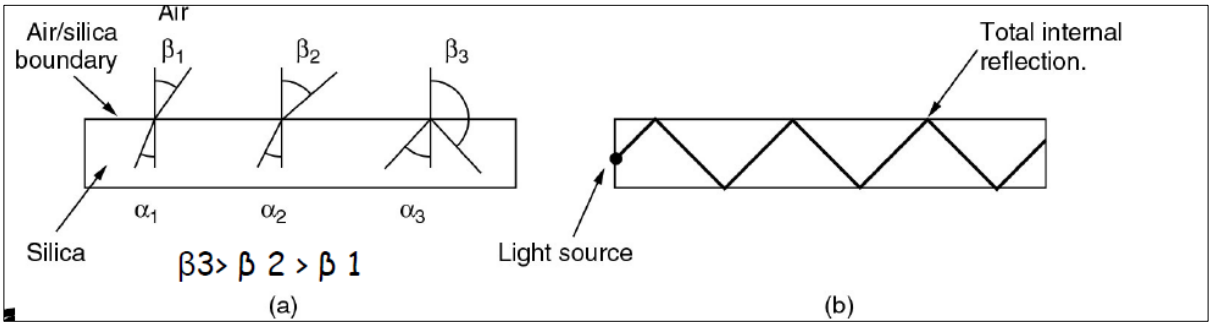



Figure 6.5 - (a) Three examples of a light ray from inside a silica fiber impinging on the air/silica boundary at different angles. (b) Light trapped by total internal reflection

### 6.5.4.2 Multi-mode and Single-mode Fiber

Only one trapped ray is shown in Figure 6.5 (b). However, as any light-ray occurrences in the border above the critical angle are internally reflected, many various rays bounce at different points of view. The fiber with this property is called a multimode fiber. Each strip is said to have a different mode. If however, the diameter of the fibers is reduced to a few wavelengths, the fibers act as a wave guide and only in a straight line can they propagate, without bounce, yielding a single-mode fiber. Fibers in single-mode are more expensive, but are commonly used over long distances. Single-mode fibers currently available can transmit data at 50Gbps for 100 km without amplifier. Even higher data rates have been achieved for shorter distances.

### 6.5.4.3 Transmission of Light through Fiber

The attenuation of light through glass depends on the wavelength of the light (as well as on some physical properties of the glass). For the kind of glass used in fibers, the attenuation (in decibels per linear kilometer of fiber) is given by the formula:

**Attenuation in decibels=10 $log_{10}$ (transmitted power/received power)**

Note: Light pulses sent down a fiber spread out in length as they propagate. This spreading is called **chromatic dispersion**, the amount of which is wavelength dependent.

## 6.6 Fiber Optic Networks

### 6.6.1 Fiber optic ring with active repeaters

Looks like a ring network with a collection of point-to-point links, as shown in the figure below. The interface at each computer passes the light pulse stream through to the next link and also serves as a T junction to allow the computer to send and accept messages as shown in Figure 6.6

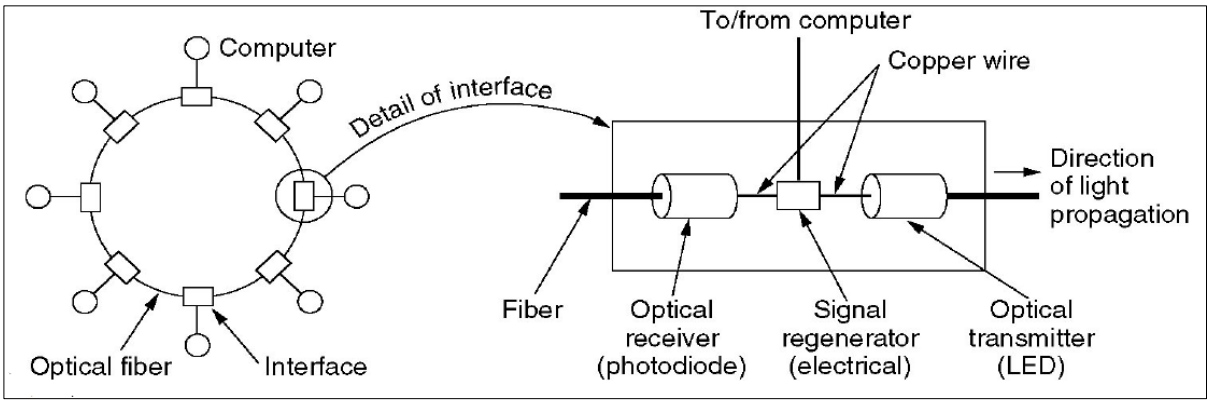



Figure 6.6 – Fiber Optic ring with active repeaters

The advantage is that the individual computer links can be kilometers long, with no limit to the overall ring size as the signal is regenerated on each interface. If an active replayer fails, however, the ring is broken and the network is closed.

### 6.6.2 Passive star connection

Both LANs and the long-wheel transmission can be used with fiber optics, although tapping into them is more difficult than connecting to Ethernet. Each interface has a fiber from its transmitter into a silkscreen in this design as shown in Figure 6.7, with the input fibers fused to an end. Each receiver is equally fused with fibers fused to the other end of the cylinders. Whenever a light pulse is issued by an interface, it is dispersed within the passive star to light all receptors, thereby achieving transmissions. The passive star actually combines all the incoming signals with the combined result across all lines. The number of nodes within our network is limited by the sensitivity of the photodiodes, as input energy is divided into all outgoing lines.

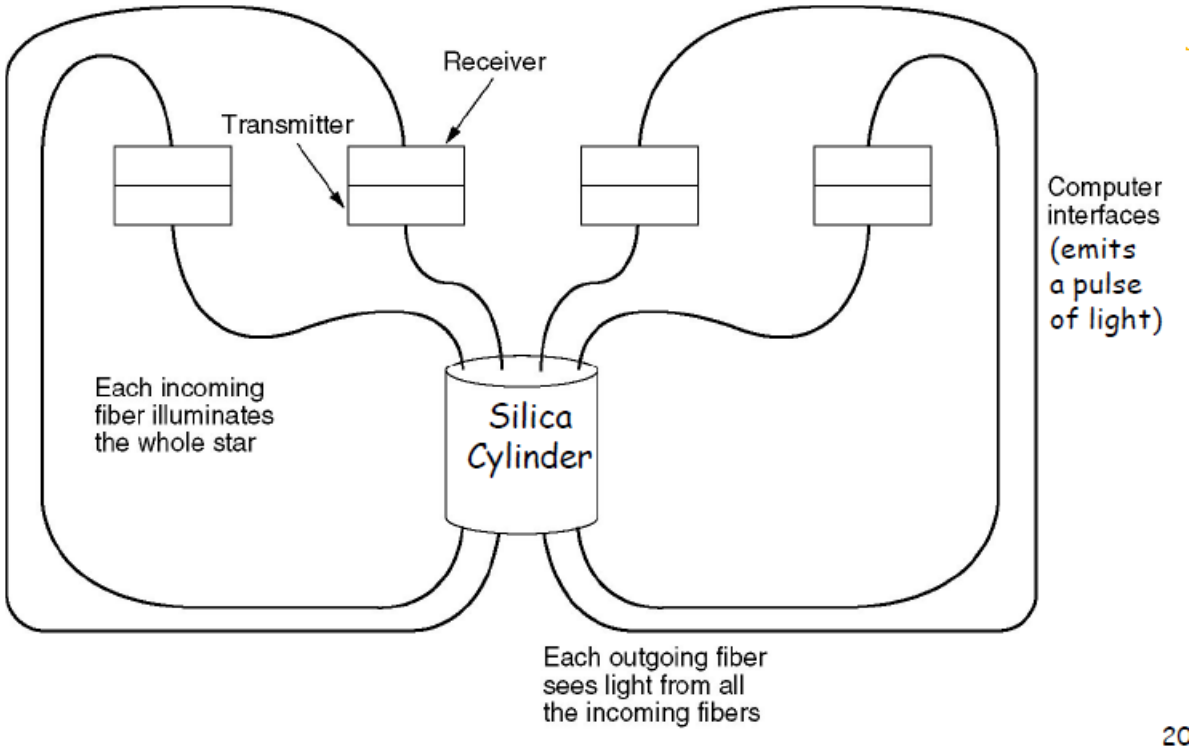



Figure 6.7 – Passive Star Connection

## 6.7 Assessment of Fiber Optic

The advantage is that it can handle much higher bandwidths than copper. This alone would require its use in high-end networks. Due to the low attenuation, repeaters are needed only about every 50 km on long lines resulting in a substantial cost saving. It is not affected by power surges, electromagnetic interference or power failures. It also not affected by corrosive chemicals in the air, making it ideal for harsh factory environments. Also, it is thin and lightweight. It is much lighter than copper and much lower installation cost.

However, it is a less familiar technology requiring skills not all engineers have. It can be damaged easily by being bent too much. Since optical transmission is inherently unidirectional, two-way communication requires either two fibers OR two frequency bands on one fiber. Fiber interfaces cost more than electrical interfaces.

In brief as shown in Figure 6.8, Optical Fiber is much better.

| | Twisted pair | Coaxial cable | Fibre optics | Microwave (unguided) |
|---|---|---|---|---|
| **Network type** | LAN | LAN | Any | WAN |
| **Transmission Distance** | Short | Short | Moderate | Long |
| **Cost** | Low | Moderate | High | Moderate |
| **Security** | Good | Good | Excellent | Poor |
| **Transmission speed** | Low-High | Low-High | Very high | Moderate |

| Type | Medium | Max Length | Connector |
|---|---|---|---|
| 10Base5 | Coax | 500 m | Vampire Tap |
| 10Base2 | Coax | 185 m | BNC |
| 10BaseT | UTP | 100 m | RJ-45 |
| 10BaseF | Fiber | 2000 m | ST/SC/MT-RJ |
| 100BaseT | UTP | 100 m | RJ-45 |
| 100BaseF | Fiber | 2000 m | ST/SC/MT-RJ |
| 1000BaseT | UTP | 100 m | RJ-45 |
| 1000BaseLX | SMF | 5000 m | ST/SC/MT-RJ |
| 1000BaseSX | MMF | 550 m | ST/SC/MT-RJ |

**Figure 6.8 – Summary of Fiber Optic**

## 6.8 Summary

Optical fibre is better than twisted pair and coaxial connections in guided media in terms of networking performance, but optical fibre cable connectivity is more sensitive and requires greater costs. The coaxial cable exceeds twisted pairs. It is also remarkable here that a twisted pair is not easy to connect with the coaxial cable without order. For Unguided, WiMAX outperforms other media in a better long-range networking performance, although Wi-Fi replaces short-range WiMAX with a greater access power. All unguided media are better here than guided for easy access.

## 6.9 Additional Reading


- "*Computer Networks, 5th Edition*". Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure,* "*Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- "*Computer Networking, 7th Edition*". Jim Kurose, W. Ross
- "*Computer Networks, A system approach 4th Edition*". Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- "*Computer Networks, 5th Edition*". Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- "*Computer Science, 2nd Edition*". Langfield, Duddell Publisher : Cambridge International.
- "*Principles of Communication Networks, 6th Edition*". Zorsi,
- "*Principles of Networks and System Administration, 6th Edition*". Burgess,
- "*Computer Science, 3rd Edition*". Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 6.10 Activities

- Describe the concept of bandwidth,
- Explain the various guided and unguided transmission media,
- Elaborate on the range of fiber optical media,
- Describe fundamental characteristics of single mode and multi-mode,
- Explain Nyquist theorem,
- Elaborate on the various fiber optics network.

## 7.1 Introduction

In the communication channel, errors can occur when sending data from sender to receiver. The sender may send packets faster than the recipient may receive, in which case the packets may delay their transfer. Feedback-based flow control can be used in the error-prone communication medium to make communication reliable by waiting for the sender to receive the feedback that the packets sent have been properly received and waiting to receive the following. This is typically called a stop-and-wait protocol and takes time, as the sender needs to await recipient feedback so that the rest of the packets can be sent. Slides window protocol is used to prevent stop-and-wait protocol disadvantages

## 7.2 Unit Objectives

- Recognise the need for ARQ,
- Be able to distinguish among stop and wait, go back and selective repeat,
- Explore benefits and drawbacks of different ARQ techniques,
- Describe the Vertical Redundancy Check,
- Understand Longitudinal Redundancy Check,
- Explain hoe checksum works,
- Study the cyclic redundancy check.

## 7.3 Automatic Repeat Request (ARQ).

Automatic repetition request is called an error control system using a reverse (feedback) channel (ARQ). They are based on protocols requiring data blocks to be transmitted when errors are detected. The channel connects two nodes on physical layer over which the link protocol works (e.g., across a length of cable or over a wireless medium). Edge-to-edge ARQ is also available across a subnet where the path comprises several mediums. It uses a re-transmission mechanism to retransmit lost (i.e. missing or corrupted) frames for every framework to detect channels errors. It requires both a forward and return path and should be used over links that employ full- or half-duplex links. It also allows sender to detect lost or corrupted frames and to schedule retransmission. Detection of frame loss may be via a link protocol timer, by detecting missing acknowledgement frames, by receiving explicit negative acknowledgement frames and/or by polling the link receiver status. The various types of ARQ includes the Stop-and-Wait, Go-Back-N and Selective-Repeat.

### 7.3.1 STOP AND WAIT ARQ (IDLE ARQ!)

One sender transmits a single framework with stop-and-wait and waits for a receiver acknowledgment as shown in Figure 7.1. The transmitter then either goes on to the next picture, or repeats the same picture transmission if the recognition shows that the original picture was either lost or damaging. ARQ is popular because it is easy to implement. It is also suitable for networks that delay bandwidth.

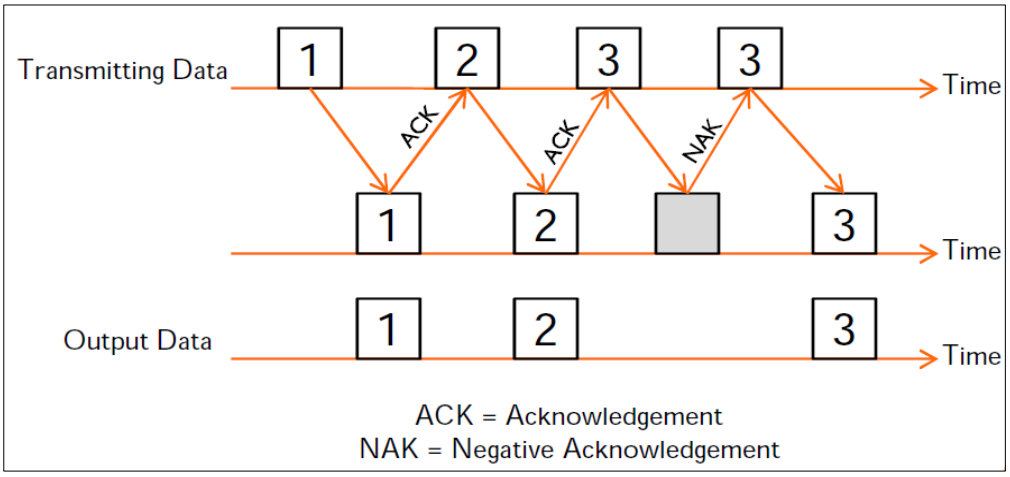



Figure 7.1 – Stop and Wait ARQ

## 7.3.2 GO BACK N ARQ

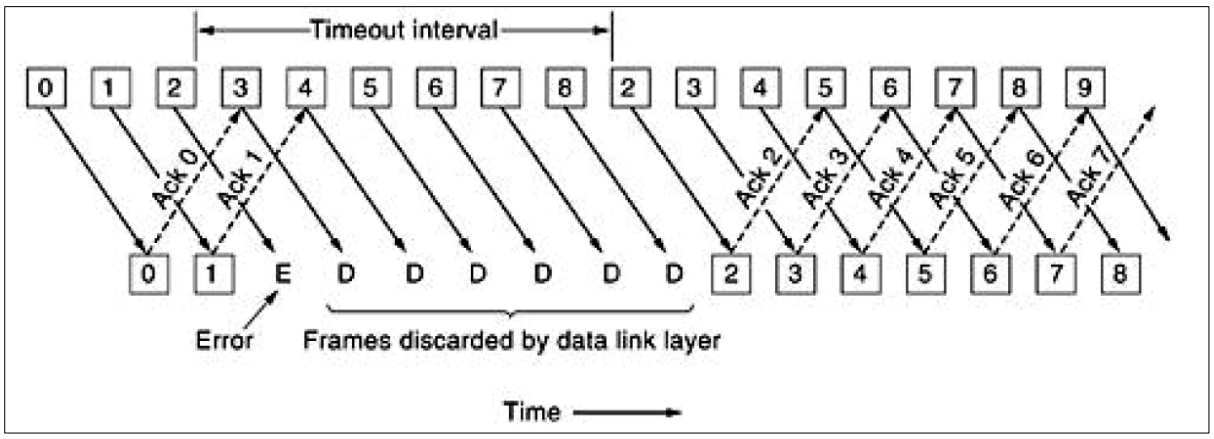
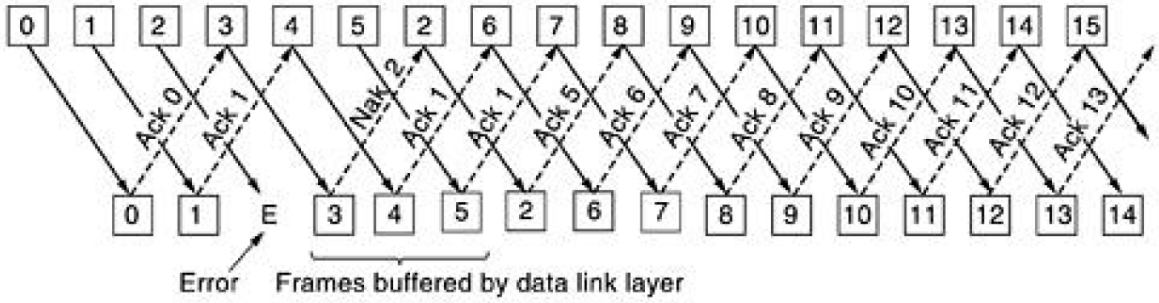



Figure 7.2 – Go and Back ARQ

In view of the above chart in Figure 7.2, assume that the boxed numbers are data packets which are transmitted from sender to receiver via the communications medium. The packet flow from the sender begins with a packet number zero (1), 2,... up to 9. If the receiver receives the packet zero, it sends the sender positive acknowledgement and expects the following packets to receive. An error was reported when sending packet 2 and therefore the packets sent after packet 2 have been removed. The sender only has to start again from packet number 2 to 9 to the receiver, but does not send good received packets. The drawback is the amount of time it took to throw out packets after packet number 2 and then resume sending packet 2.

## 7.3.3 ELECTIVE REPEAT ARQ



In view of the above chart, assume that the boxed numbers are data packets which are transmitted from sender to receiver via the communications medium. Packs numbered 0 to 15 are sent to the recipient by the sender. When the recipient receives a packet, he sends the sender a positive message and expects the following packets to be received. There was an error when you sent the number 2 packet. Selective Repeat does not remove the packets after packet number 2 as in Go Back N but sends them to the receiver. Only the failed packet number 2 is sent back to the recipient by the sender. Compared to Go Back N, sends error and prevents packet duplication. The recipient sequence of the received packet is sorted. In case of a packet that is sent error compared to Go Back N, this protocol loses little time and prevents packet duplication of sent.

## 7.4 Error Detection

Data transmission may contain one-bit errors or length n burst errors (n: distance between the first and last errors in data block). How to detect errors is the problem? Unable to detect errors if only data is transmitted. Therefore, send more information with data to meet or add redundancy to a particular relationship. This section describes the different methods used to detect errors.

### 7.4.1 Vertical Redundancy Check (VRC)

This system appends a single bit at the end of data block such that the number of ones (1s) is even. It uses even Parity (odd parity is similar). Like:

- 0110011 →01100110
- 0110001 →01100011

VRC is also known as **Parity Check. The overall p**erformance is that it detects all odd-number errors in a data block

### 7.4.2 Longitudinal Redundancy Check (LRC)

It organizes data into a table and create a parity for each column as shown in Figure 7.4

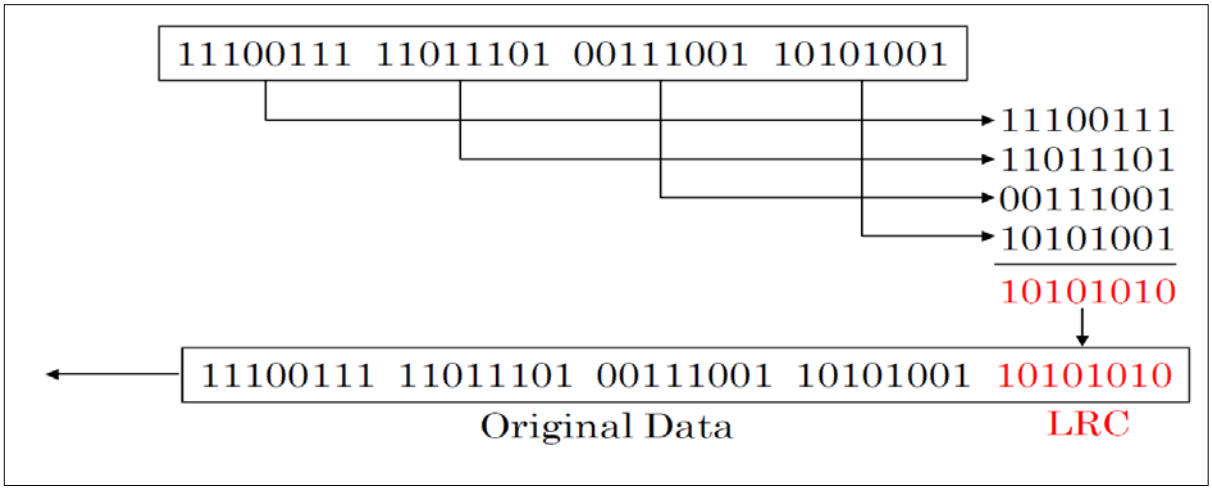



Figure 7.4 – Longitudinal Redundancy Check

Its performance is that it detects all burst errors up to length n (number of columns) and misses burst errors of length n+1 if there are n-1. There are uninverted bits between the first and last bit. If the block is badly garbled, the probability of acceptance is

### 7.4.3 Checksum – Redundancy Cyclic Check

It used by upper layer protocols. It is similar to LRC, uses one's complement arithmetic. It is a powerful error detection scheme. Rather than addition, binary division is used. It uses the Finite Algebra Theory (Galois Fields). Thus, it can be easily implemented with small amount of hardware. There are shift registers like the XOR (for addition and subtraction). Let us assume *k* message bits and *n* bits of redundancy, this is shown in Figure 7.5

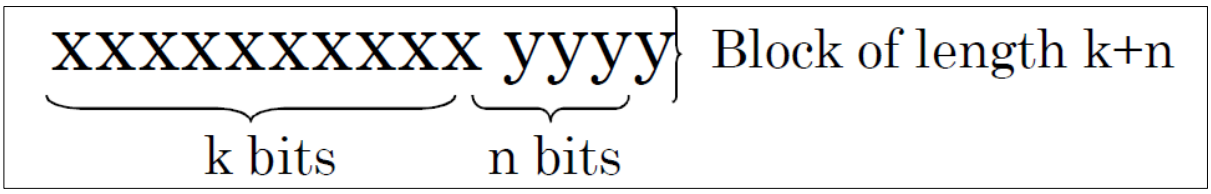



Figure 7.5 - Checksum

Associate bits with coefficients of a polynomial

$$1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1$$
$$1x^6+0x^5+1x^4+1x^3+0x^2+1x+1$$
$$= x^6+x^4+x^3+x+1$$

Let M(x) be the **message polynomial and** Let P(x) be the **generator polynomial. Thus, the** P(x) is fixed for a given CRC scheme and P(x) is known both by sender and receiver. To create a block polynomial F(x) based on M(x) and P(x) such that F(x) is divisible by P(x)

$$\frac{F(x)}{P(x)} = Q(x) + \frac{0}{P(x)}$$

The sending check is done by using the following formula:

- Multiply M(x) by $x^n$
- Divide $x^n$M(x) by P(x)
- Ignore the quotient and keep the reminder C(x)
- Form and send F(x) = $x^n$M(x)+C(x)

The Receiving check computation is done by:

- Receive F′(x)
- Divide F′(x) by P(x)
- Accept if remainder is 0, reject otherwise

## 7.5 Proof of CRC Generation

Prove that $x^n M(x) + C(x)$ is divisible by $P(x)$

$$P(x)\overline{)x^n M(x)}^{\,Q(x)}, \text{ remainder } C(x)$$

$$\therefore x^n M(x) = P(x)Q(x) + C(x)$$

$$\frac{x^n M(x) + C(x)}{P(x)} = \frac{P(x)Q(x)}{P(x)} + \frac{C(x) + C(x)}{P(x)}$$

$\frac{P(x)Q(x)}{P(x)}$: Remainder 0 ; $\frac{C(x) + C(x)}{P(x)}$: Remainder 0

**Note: Binary modular addition is equivalent to**

**binary modular subtraction → C(x)+C(x)=0**

**An example is shown below**

- Send
  - M(x) = 110011 → $x^5+x^4+x+1$ (6 bits)
  - P(x) = 11001 → $x^4+x^3+1$ (5 bits, n = 4) → 4 bits of redundancy
  - Form $x^nM(x)$ → 110011 0000 → $x^9+x^8+x^5+x^4$
  - Divide $x^nM(x)$ by P(x) to find C(x)

```
          100001
11001 ) 1100110000
        11001
          10000
          11001
           1001  = C(x)
```

Send the block 110011 1001

- Receive

```
11001 ) 1100111001
        11001
            11001
            11001
            00000
              ↓
No remainder
→ Accept
```

The properties of CRC can be describing below:

Example:

- CRC-12 = x12+x11+x3+x2+x+1
- CRC-16 = x16+x15+x2+1
- CRC-CCITT = x16+x12+x5+1

CRC-16 and CRC-CCITT catch all

- Single and double errors
- Odd number of bit errors
- Bursts of length 16 or less
- 99.997% of 17-bit error bursts
- 99.998% of 18-bit and longer error bursts

This is implemented as follows:

- Message = 1011011 $\quad k = 7$
  $P(x) = 1101 = x^3+x^2+x^0 \quad n = 3$

**Conventional Method:**

$$
\begin{array}{r}
1100101 \\
1101\overline{)1011011000} \\
\underline{1101} \\
1100 \\
\underline{1101} \\
0011 \\
\underline{0000} \\
0111 \\
\underline{0000} \\
1110 \\
\underline{1101} \\
0110 \\
\underline{0000} \\
1100 \\
\underline{1101} \\
001
\end{array}
$$

## 7.6 Summary

Error control describes how errors in the data link layer, particularly in network management, are detected and handled. In this article, we present an overview of error control and error correction. In the data link layer, error control occurs. We talk mainly about the type of mistakes to detect mistakes and how mistakes are corrected to allow the receiver to extract the real data.

## 7.7 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 7.8 Activities

- Describe the different features of ARQ,
- Explain the various types of ARQ,
- Describe in details how errors can be detected in networks,
- Differentiate between vertical redundancy check and longitudinal redundancy check.

## 8.1 Introduction

For over 30 years it has been a major research topic to design and analyse an efficient Medium Access Control (MAC) protocol. This chapter is focused on the analysis and modification of the famous CSMA/CD MAC protocol (through simulation). Due to unused channel periods, the existing protocol does not consider wasting bandwidth. Considering this, it is possible to improve the performance of the MAC protocol. This work aims to change the existing protocol so that it can be adapted to network status. When unused periods are detected, the modified protocol acts appropriately. In this way, the efficient utilization of bandwidth increases and how it works when load is increasing and packet sizes differ.

## 8.2 Unit Objectives

- Recognise the need for ALOHA protocol,
- Be able to distinguish between collision and carrier,
- Explore benefits and drawbacks of the CSMA/CD,
- Describe the algorithm of the CSMA/CD,
- Understand concepts of PURE ALOHA,
- Explain the concept of SLOTTED ALOHA.
- Study the assessment of the ALOHA's protocol.

## 8.3 Aloha Protocol

Aloha, also referred to as the Aloha Protocol/Method, means a simple system in which each source (transmitter) sends data in a network whenever there is a frame to be sent. If the frame reaches the destination (receiver) successfully, the following frame is sent. If you do not receive the frame at the address, you will be returned. The Aloha protocol is an OSI Layer 2 protocol (Data Link Layer) for broadcast topology LAN networks. Aloha works perfectly with a wireless broadcasting system or a two-way half-duplex system. But when networks are more complex, e.g. in an Ethernet system with several sources and destinations in which data travels many paths all at once (conflict). The heavier the volume of communication, the worse are the problems with the collision. As a result system efficiency is degraded, because the data contained in both frames are lost when two frames collide.

A scheme called Slotted Aloha has been designed to minimize collisions, to optimize network efficiency and to increase the number of subscribers who can use a given network. The system uses signal called beacons to tell each source when the channel is clear to send a frame at precise intervals. A more sophisticated Carrier Sense Multiple Access Detection (CSMA/CD) protocol can be further improved.

Although ground-based radio transmission is used by Aloha system, the basic idea applies to any system in which uncoordinated users compete for a single common channel. The use of a shared medium in transmission is important to ALOHA. This shows the need for more modern dispute management schemes such as Ethernet's CSMA/CD.

## 8.4 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD is a network control protocol that uses a carrier sensing system. A station that transmits data that detects a new signal while transmitting a frame stops transmitting that frame, sends a jam signal and waiting for a random time interval (called "back off time") before attempting to retransmit that frame. CSMA/CD is pure Carrier Sense Multiple Access modification (CSMA). Collisions detection is used to increase the CSMA performance when a collision is detected and the likelihood of the second collision in retrieval is reduced.

Carrier Sense refers to the fact that every station listens to see whether any other station broadcasts before a broadcast starts. Multiple access points to every station having access - as with bus systems - to the common transmission medium (cable). The principle of listening to see whether other stations transmit while transmitting collision detection is referred to. Network devices contend for network media in networks that use CSMA/CD technology such as Ethernet. If a device has data to send, it listens first to see if any device uses the network at the moment. If not, the data will be sent. When the transmission has been completed, he is listening to see if there has been a collision. When two devices simultaneously send data, a collision occurs. Each device backs off and waits for a random time before resending its data if a collision happens. (Note: a collision between the two devices in most cases is not reoccurring). This is shown in Figure 8.1

Collision detection methods depend on the media, but colliding can be detected by comparing transmitted data with received information on electric buses like Ethernet. If they differ, the first transmitter's signal (a collision), and transmission ends immediately, is overlaid by another transmitter. There is a jam signal sent which causes all transmitters to stop at random intervals, thus reducing the likelihood of a crash when the first attempt is made. In the OSI model, CSMA/CD is a layer 2 protocol. The CSMA/CD protocol is the traditional Ethernet. Its algorithm is depicted in Figure 8.2.

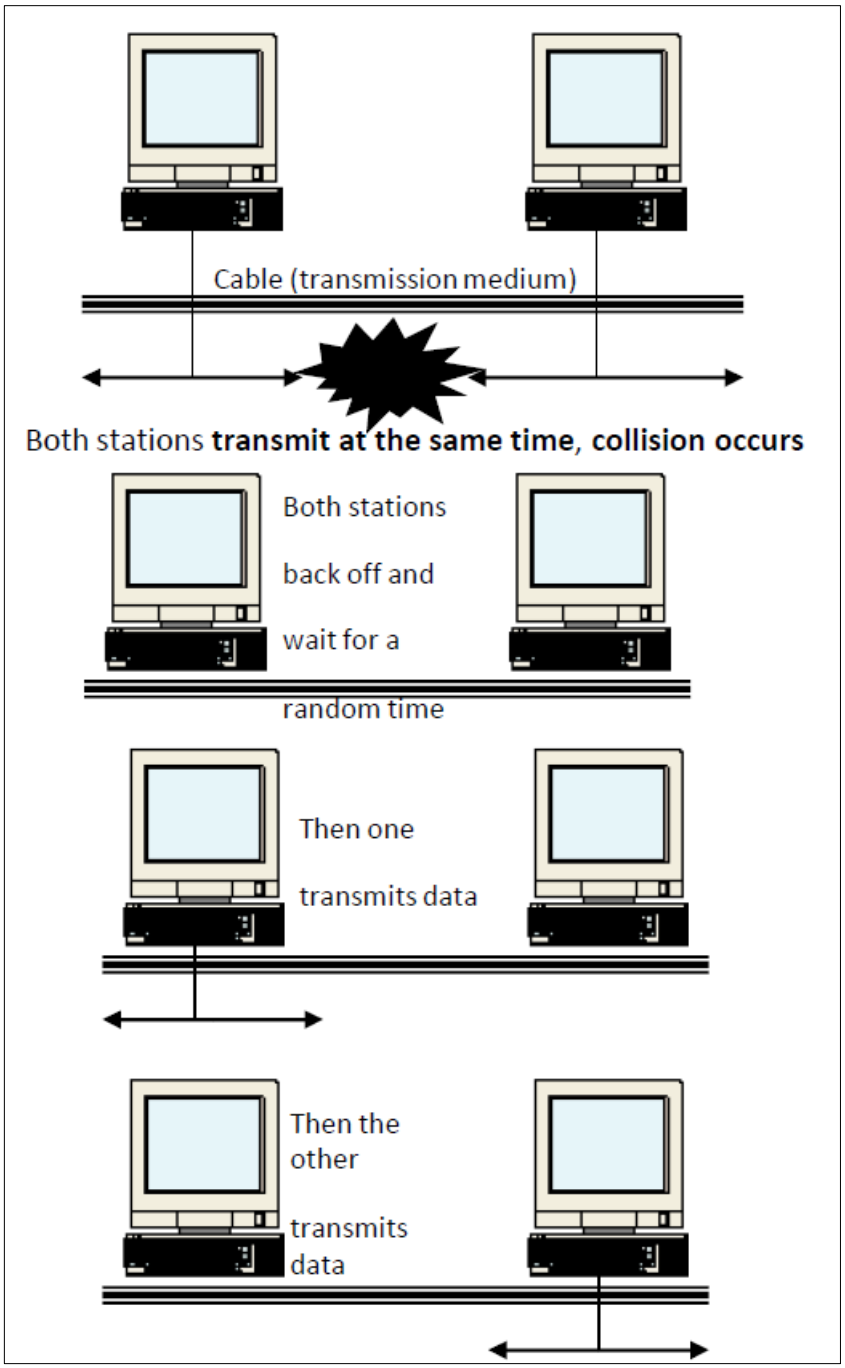



**Figure 8.1 - Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

### 8.4.1 Algorithm of CSMA/CD

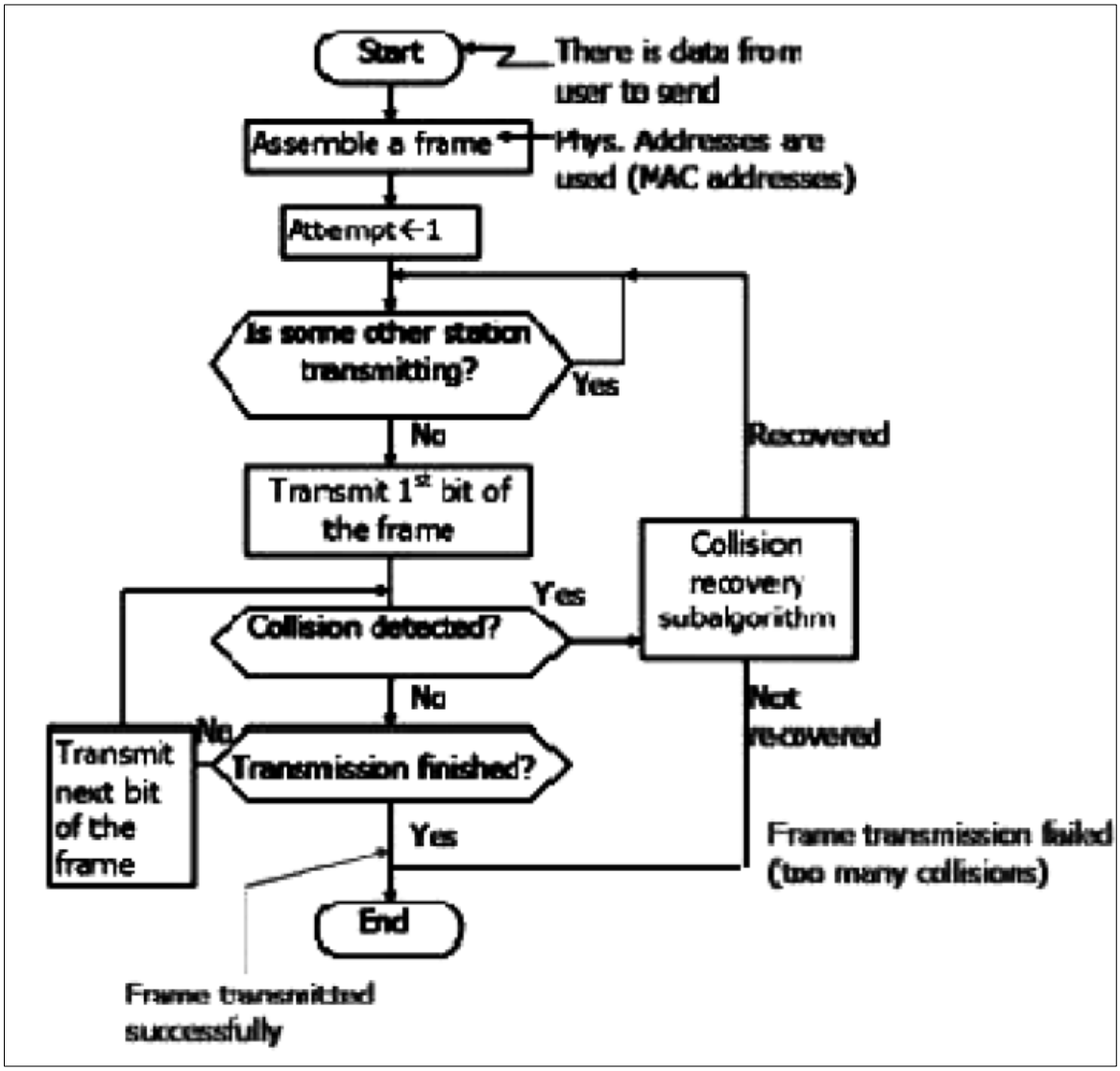



Figure 8.2 – Algorithm of ALOHA

Back to ALOHA: the use of the common media to transmit ALOHA was important. This showed that more modern control systems such as CSMA/CD, used by Ethernet, are needed. All nodes in ALOHA were transmitted at the same frequency. This meant that some system was necessary to check who was able to speak. ALOHA has been similar to modern Ethernet and Wi-Fi networks. ALOHA has been faced with problems. Two variants of ALOHA are the **PURE ALOHA and SLOTTED ALOHA**

The aloha PROTOCOL is simple: if you have packet to send, "just do it" or if packet suffers collision, try resending later as shown in Figure 8.3

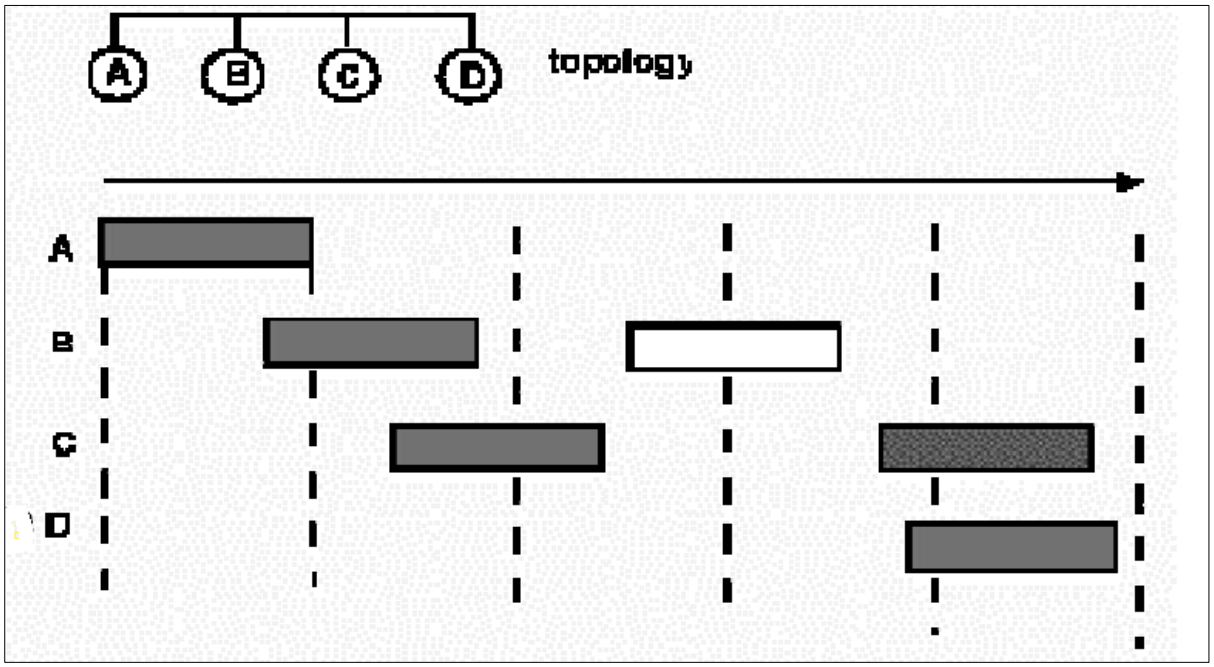



Figure 8.3 – Philosophy of ALOHA

## 8.5 PURE Aloha Protocol

Stations can access the channel with Pure Aloha whenever the data is transmitted as shown in Figure 8.4. Since there is a risk of a data collision, each station must either monitor its transmission on retransmission or wait for the destination station to acknowledge it. The transmitting station can determine the success of the transmitted packet by comparing the transmitted packet with the received packet or through a lack of an acknowledgement. In the event of failure of the transmission, the re-crisis probability is reduced after a random period of time. They overlap partially when packets collide.

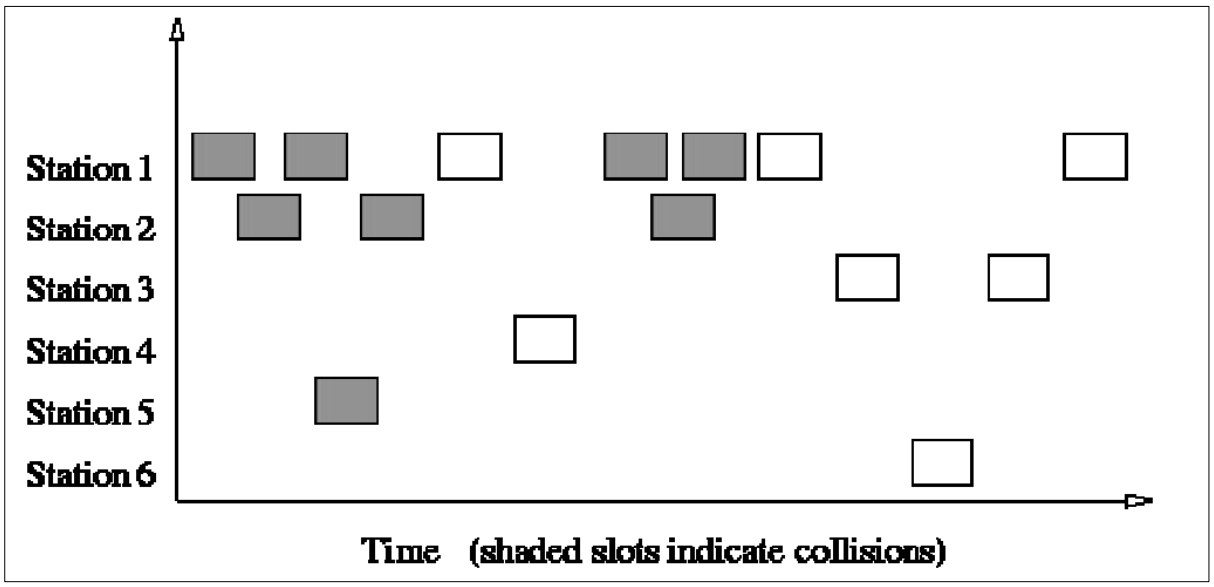



Figure 8.4 – Pure ALOHA Protocol

The advantages are that it is superior to fixed assignment when there is a large number of bursty stations and also adapts to varying number of stations. However, theoretically proven throughput maximum of 18.4% and requires queueing buffers for retransmission of packets.

### 8.5.1 Algorithm for PURE Aloha Protocol

- Nodes transmit on a common channel.
- Transmit frame of fixed length.
- When two transmissions overlap, they garble each other (collision).
- The receiving node acknowledges the correct frames it receives.
- When a node does not get an acknowledgment within a specific timeout, it assumes that its frame collided.
- When a frame collides, the transmitting node schedules a retransmission after a random delay.

### 8.5.2 SLOTTED Aloha Protocol

The Aloha Protocol can be doubled by restricting the freedom of transmission of the individual stations. The transmission time is broken into slots, which corresponds to the transmission time of a single packet if the packet is constant in length. Stations may transmit only at slot borders. They are fully overlapping rather than partially when packets collide. This doubles the effectiveness of the Aloha Protocol and is called Slotted Aloha. This is shown in Figure 8.5

The aadvantages are that it doubles the efficiency of Aloha and also is adaptable to a changing station population.

However, it is theoretically proven throughput maximum of 36.8%. It requires queueing buffers for retransmission of packets and there need to be synchronization. There are also collisions, wasting slots. There are idle slots, hence wastage of bandwidth.

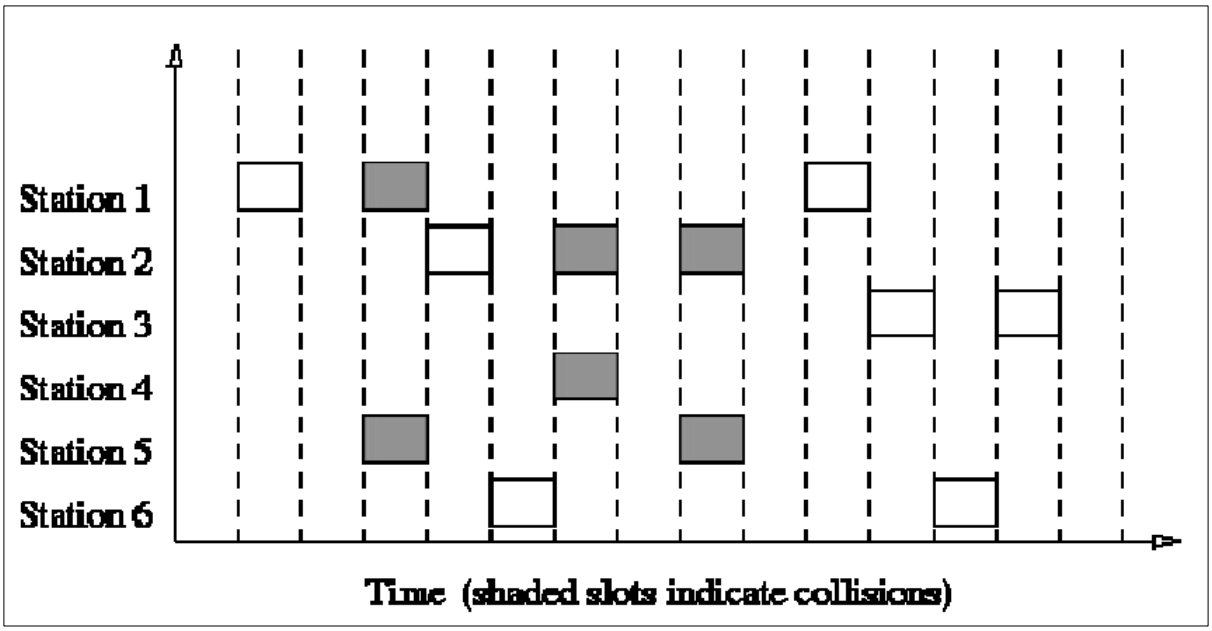



Figure 8.5 – Slotted ALOHA

The SLOTTED Aloha Protocol evaluation can be summarized as follows: The channel bandwidth in Slotted Aloha protocol is a constant stream of slots with the time required to transmit a single packet. On the next available slot boundary, a station with a sending packet will transmit. In the event of a collision each colliding station will retransmit randomly to reduce the risk of colliding. The limits imposed on random retransmission of the packet obviously affect the delays associated with the successful delivery of the packet. The chance of a collision is high if the limit is too short.

## 8.6 Summary

This unit analyses the performance of the non-slotted ALOHA and CSMA in wireless networks distributed by space. Users/packets are randomly sent to their intended destinations using a fully distributed MAC protocol according to Poisson processes (either ALOHA or CSMA). A model shall be considered and if the received model exceeds the threshold value for the duration of the packet a packet transmission is successful. For both MAC protocols, precise limits to the probability of failure are developed, which depends on the density of transmissions.

## 8.7 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 8.8 Activities

- Describe the different features of the ALOHA protocol,
- Explain the term protocol,
- Describe fundamental characteristics of CSMA/CD,
- Differentiate between PURE ALOHA and SLOTTED ALOHA,

## 9.1 Introduction

This chapter describes the interesting solutions for the consideration of real-time traffic in a wireless environment are the collision-flowing Medium Access Control (MAC) protocols based on Carrier Sense Multiple Access (CSMA). The purpose of this chapter is precisely to present the main CSMA-MAC collision-free protocols for single-hop Wireless Local Area Networks (WLANs) with a comprehensive presentation.

## 9.2 Unit Objectives

- Recognise the need for Carrier Sense Multiple Access (CSMA) Protocols,
- Be able to distinguish among bit-map protocol and binary countdown,
- Explore benefits and drawbacks of wireless LAN protocols,
- Describe various configurations for a wireless LAN,
- Understand the concept of hidden station problem,
- Explain the various objectives behind MACA,
- Study the need for exposed station problem,
- Distinguish between the examples of MACA,
- Explain the concept of collision in MACA.

## 9.3 Carrier Sense Multiple Access (CSMA) Protocols

Slotted ALOHA provides the best channel use for 1/e, as all stations transmit at will without taking into account what the other stations do. Consequently, it is clear that many collisions will occur. However, in local area networks, stations can detect what other stations do and adapt their behavior. These networks can be used much better than 1/e. Some performance improvement protocols have been discussed in this chapter. The Carrier Sense Protocols Are Protocols, in which stations listen to a carrier (that is, a transmission) and thus act.

### 9.3.1 Versions of Carrier Sense Protocols

The two versions are the persistent and non-persistent CSMA. The first carrier sense protocol is called 1-persistent CSMA. Operation: if there is data to send to a station, the station first hears the channel to see whether someone else is transmitting. The station waits until it gets inactive, if the channel is busy. The station transmits a frame when it detects an idle channel. When a collision happens, the station waits randomly and begins everything again. The protocol is called 1 perpetual because when it finds the channel idle, the station transmits 1 probability.

The delay in propagation has a major impact on protocol performance. There is a small opportunity for another station to be ready to send and sense the channel shortly after a station starts to send. If the second signal of the first station has yet to reach the second, the latter will feel a vacuum channel and start transmitting it as well. Therefore, the longer the spread delay, the higher the performance of the protocol, the more important is this effect. There will still be collisions even if the propagation delay is zero. When two radio stations are ready in the midst of the transmission of a third station, they both wait until the transmission ends and then each radio station will start to transmit at the same time and collide.

### 9.3.2 Non-persistent CSMA

The second sensory protocol to carrier is CSMA that is not persistent. This protocol is a conscious attempt to be less covetous than the previous protocol. Operation: a station senses the channel prior to sending. The station starts transmission if no one else sends. When the channel is already in use, however, the station doesn't always feel it for immediate seizure (upon detecting the end of the previous transmission). Rather, the algorithm is waiting for a random time and then again. This algorithm thus gives better channel use than 1-persistent CSMA but longer delays.

### 9.3.3 p-persistent CSMA

P-persistent CSMA is the last protocol. It works as follows on slotted channels. Operation: when a station is ready for sending, the channel is sensed. If idle, the probability p will be transmitted. It will delay until the next slot at a probability q=1-p. If this slot is still, the probabilities p and q will either be transmitted or deferred again. This process is repeated until either the frame or another station has started to transmit. The 'unhappy' station acts as if there were a collision in the latter case (i.e., it waits a random time and starts again). If the station senses the channel occupied at first, it will wait until the next slot.

## 9.4 CSMA versus Aloha

CSMA protocols are clearly an improvement on ALOHA because they ensure that no station starts sending when the channel is being occupied. The stations will also be improved if their transmissions abort when a collision is detected. In other words, two stations will almost immediately detect the collision if they sense that the channel is idle and begin to transmit simultaneously.

### 9.4.1 Collision-Free Protocols

Even when a station unambiguously has captured the channel, collisions with CSMA/CD do not occur, but during the contention period. These collisions affect the performance of the system particularly when the cable is long with short frames. Universal applicability is not CSMA/CD. Some protocols in this lecture will not be discussed, even during the contendance, which resolve the contention for the channel without any collisions.

**In the protocols to be discussed, the following 4 assumptions are made:**

- There are exactly N stations.
- Each station has a unique address from 0 to N-1 wired into the network.
- It does not matter that some stations may be inactive part of the time.
- Propagation delay is negligible.

*The basic question remains: Which station gets the channel after a successful transmission?*

## 9.5 Bit-Map Protocol

Every contention period consists of exactly N slots in this first collision-free protocol. If 0 has a frame to be sent, the 0th slot will transmit 1 bit. During this slot, no other station can transmit. No matter what station 0 does, station 1 is allowed to transmit a 1 during slot 1, but only if a frame is in the queue. Station j can generally advertise that it has a frame to send by inserting 1 bit of slot j. Each station has complete knowledge of which stations it wishes to transmit, after all N slots have passed. They start to transmit in numerical order at this point as shown in Figure 9.1

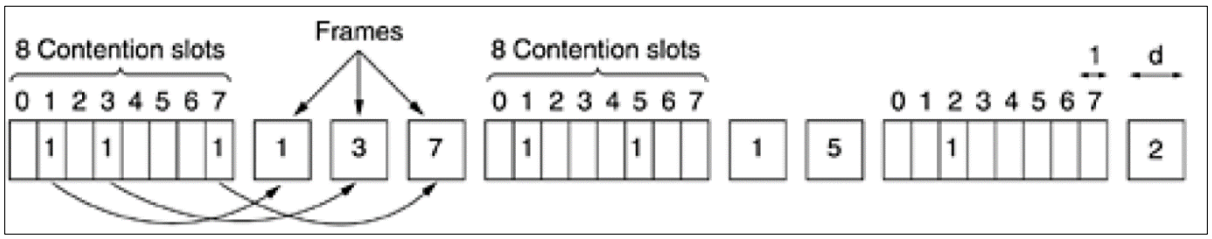



**Figure 9.1 – Bit-Map Protocol**

Since everyone agrees on who will go next, no collisions will ever occur. After its frame is transmitted by the last ready station, all stations can monitor an event easily, and a further N bit contention period is started. When a station is ready right after the little slot is gone, it is out of luck and must remain silent until each station has an opportunity and the bit map returns. Protocols such as this in which the desire to broadcast is called reservation protocols prior to actual transmission.

## 9.6 Binary Countdown

One problem of the basic bitmap protocol is that the overhead rate is 1 bit per station, so the networks with thousands of stations are not well-adjusted. The use of binary station addresses is a better approach. A station that wants to use the channel broadcast their address now, starting with the high order bit, as a binary bit string. It is assumed that all addresses are the same length. BOOLEAN ORed together are the bits at each position of the address from various stations. This is known as the binary countdown protocol. The implicit assumption is that transmission delays are insignificant, so that all stations almost instantly see asserted bits.

An arbitration rule must therefore be applied to prevent conflicts: once the station sees a high-order bit position of 0 overridden with 1 it renounces. In the first bit of the station transferring 0, 0, 1, and 1 respectively, for example when the stations 0010, 0100, 1001 and 1010 are all trying to get the channel. These are organized into a 1. Stations 0010 and 0100 see the 1 and know that the channel is competing for a more numerous station, and therefore give up the current round. The 1001 and 1010 stations continue. A clear example is shown in Figure 9.2

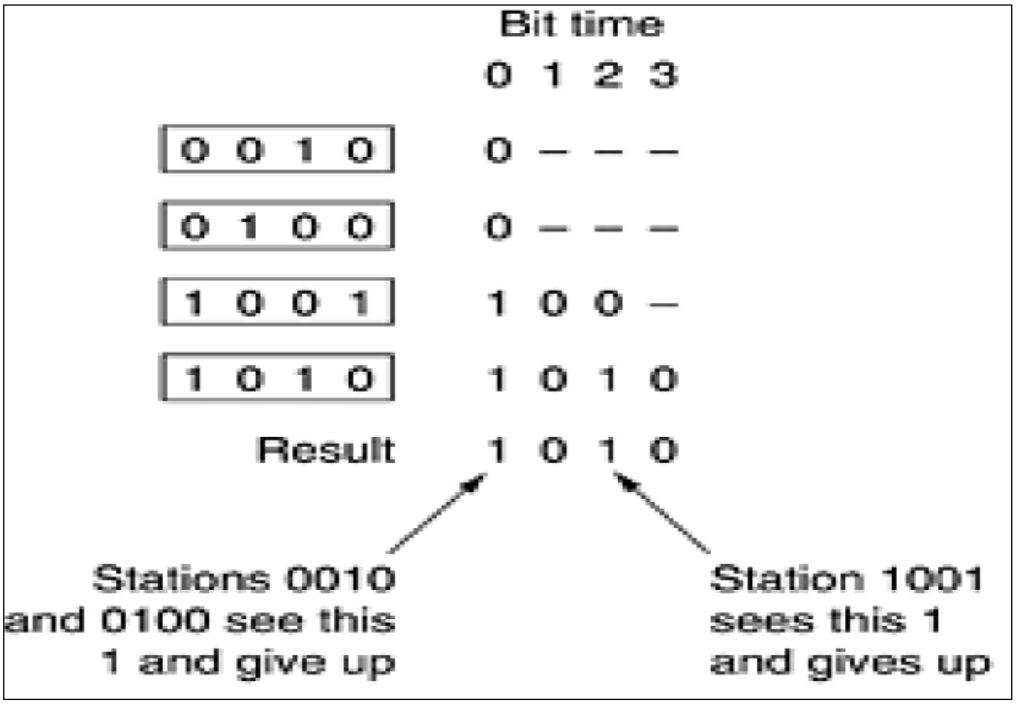



Figure 9.2 – Binary Countdown

## 9.7 Wireless LAN Protocols

The demand to connect them to the outside world is increasing as the number of mobile computing and communication devices grow. Even mobile phones could connect to other phones at the very first time. This was not the first portable computers, but soon thereafter the modems became commonly used on computers on the notebook. To go online, these computers needed to be connected to a wall socket for the telephone. Wired connection to the fixed network required portable, but not mobile, computers!

Notebooks must use radio (or infrared) signals for communications in order to achieve true mobility. Dedicated users can read and send e-mails during hiking or boating in this way. Wireless LAN can be considered as computer systems that communicate via radio signals. These LANs obviously have somewhat different features from conventional LANs and require special protocols for the MAC sublayer!

### 9.7.1 Common configuration for a Wireless LAN

A base station office building (also known as access points) located strategically around the building. The copper or fiber is used for all base stations. If the transmission capacity of the basic stations and laptops is adjusted to 3 or 4 meters, each room will become a cell and all buildings will be transformed into a large cellular system. Contrary to mobile phone systems, each cell has only one channel covering the whole bandwidth that is available and all its stations. It usually has 11 to 54 Mbps bandwidth.

**Assumption:** All radio transmitters have some fixed range. When a receiver is within range of two active transmitters, the resulting signal will generally be garbled and useless. **NOTE:** In some wireless LANs, not all stations are within range of one another, which leads to a variety of complications. Furthermore, for indoor wireless LANs, the presence of walls between stations can have a major impact on the effective range of each station.

## 9.8 CSMA's approach towards a Wireless LAN

Listen for other broadcasts and transmit them only if nobody else does. This protocol is not adequate, as interference with the receiver and not the sender is what matters. Consider the figure that follows in order to see the nature of the problem, which illustrates four wireless stations. The radio range is such that A and B are within the range of each other and can interfere. C may also interfere, but not with A, with B and D.

## 9.9 Hidden Station Problem

**Consider the scenario when A is transmitting to B as shown in Figure 9.3**

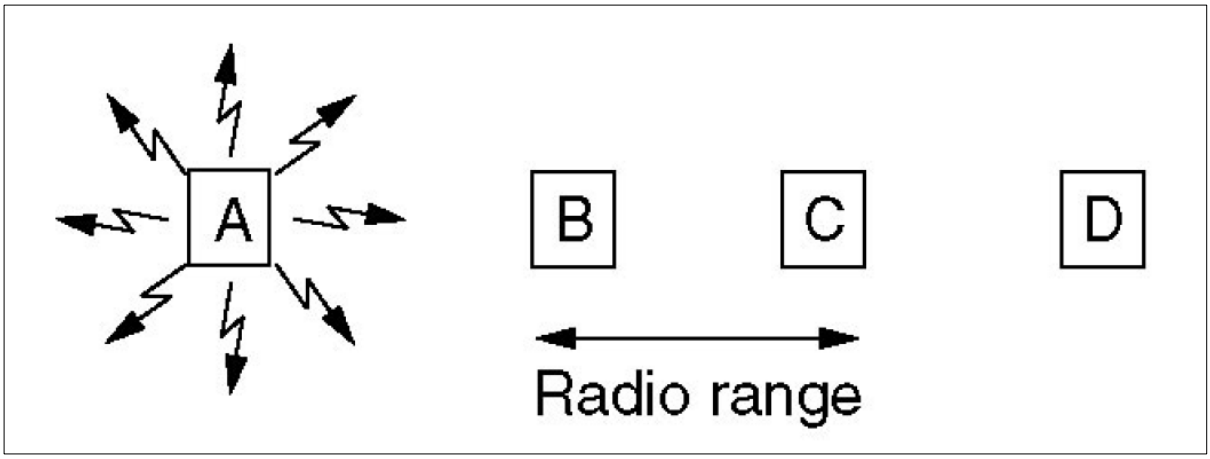



Figure 9.3 – Transmission from A to B

When C senses a medium, it won't hear A, because A's out of range, so that it can falsely pass to B. If C begins to transmit, it interferes with B and wipes out the frame of A. A station's problem is that the potential competitor is not able to detect the medium because the competitors are too far away.

## 9.10 Exposed Station Problem

**Consider the scenario when B is transmitting to A as shown in Figure 9.4**

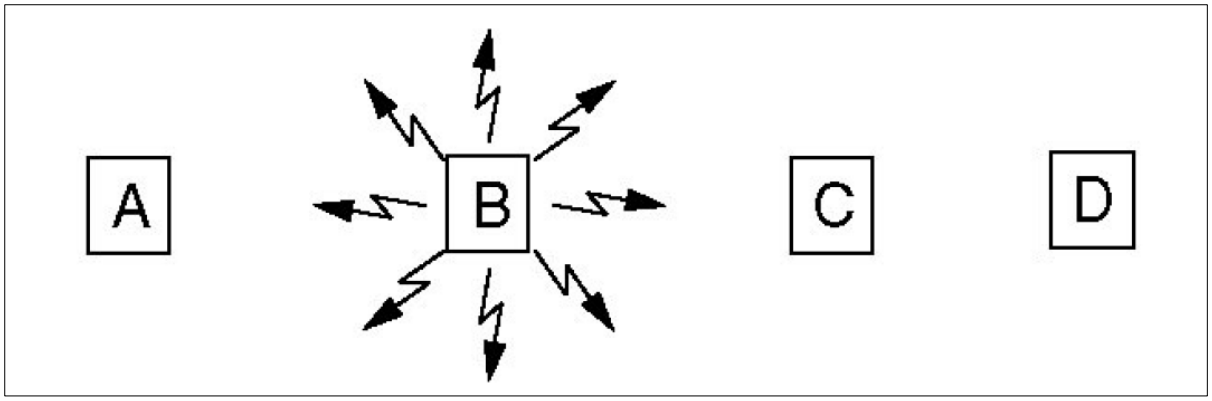



Figure 9.4 – Exposed station problem

When C senses the medium the transmission is continuous and false concludes that this transmission cannot send to D if in fact it would only cause an incorrect reception in the area between B and C, where neither receiver is located. The problem of the exposed station is. This is called the **exposed station problem**

The problem is that a station really wants to know if there is any activity around the recipient before starting a transmission. It just tells CSMA if the station senses the carrier is active. All signals are transmitted with a wire to all stations so there can be only one transmission in the system. Multiple transmissions can only occur simultaneously in a system based on short-range radio waves, provided that all destinations are different and these are not mutually exclusive.

## 9.11 Multiple Access with Collision Avoidance (MACA)

The aim of the sender behind MACA is to stimulate the recipient to produce a short frame, so nearby stations can detect that transmission and avoid transmitting over the (large) time frame of the upcoming data framework. This is shown in Figure 9.1

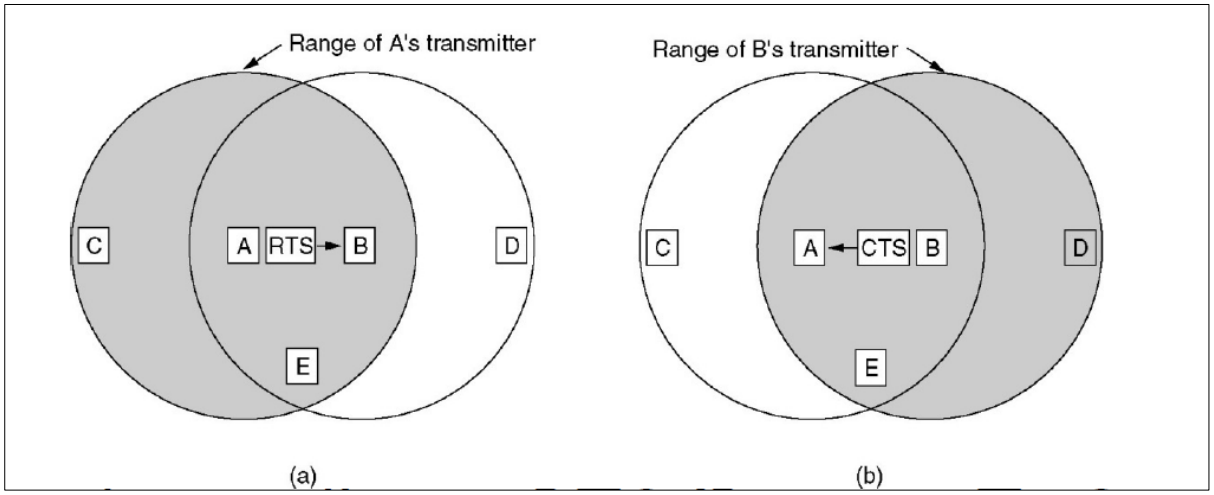



**Figure 9.5 - MACA**

A begins by sending an RTS frame to B, as shown in the figure (a). This short frame (30 bytes) contains the duration of the data frame to be followed. Then B answers with the frame CTS, as shown in the figure Clear to send (b). The framework CTS includes the length of the data (copied from the RTS frame). A starts its transmission upon receipt of the CTS frame.

## 9.12 How would stations overhearing the RTS and CTS react?

Any RTS station is clearly close to A and must remain silent for long sufficient time to return CTS to A without conflict. Any station which listens to the CTS is obviously close to B and must remain silent in the coming transmission of data for the length of which the CTS framework can be examined. **Example of MACA is shown in Figure 9.6**

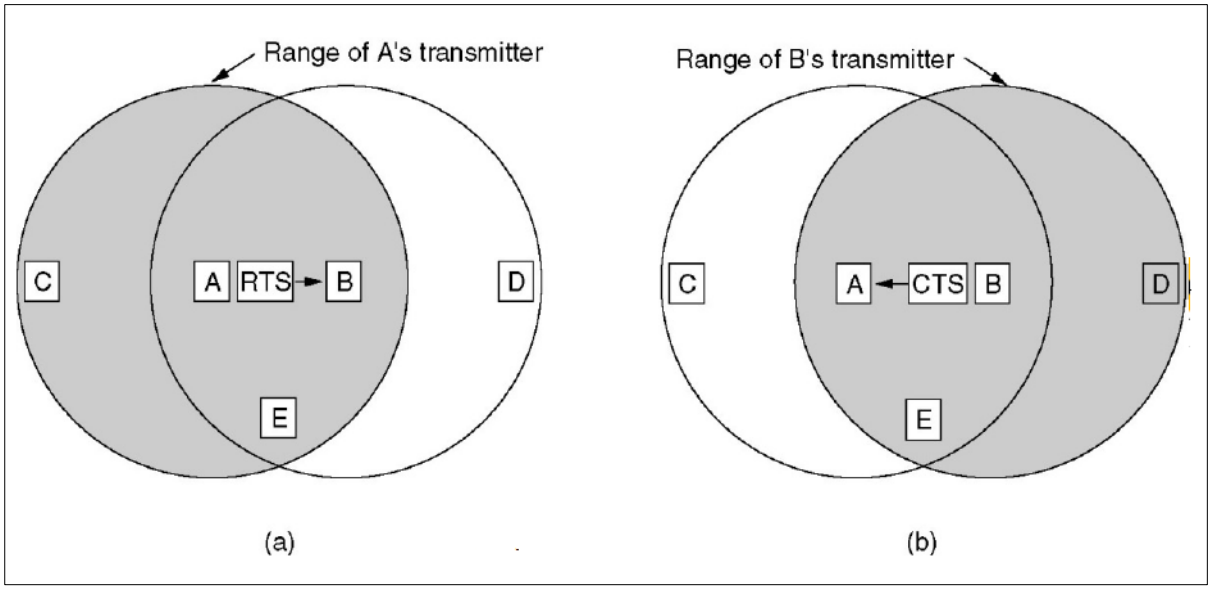



**Figure 9.6 – Further MACA**

C is in the A range, but not in the B range. It thus listens to the A RTS but not to the B CTS. Until it interferes with CTS, it is free to transmit during the transmission of the data frame. D is in the B range, however, not A. It does not listen to the RTS, but listens to the CTS. When you hear CTS, it warns that the station is near a frame, therefore it delays sending everything until the frame is completed. Station E hears both control messages. Like D, the data frame is silent until it is complete.

## 9.13 Can collisions still occur with MACA?

For instance, both B and C (both in the range A) could send RTS frames to A simultaneously. These are going to crash and get lost. If a crash occurs, a transmitter unsuccessfully waits for a random amount of times (i.e. one without hearing a CTS within the intended interval) and will try again later. The binary exponential back off is the algorithm used - the same is used on Ethernet. Multiple Collision Access Avoidance Wireless (MACAW) has been designed and renamed a new MACAW protocol to improve its performance (MACA for Wireless). Problems in MACA identified and in MACAW resolved It was found that losses of frames were not transmitted without recognition of the data connection layer until much later the transport layer was aware of its absence. After every successful data frame, an ACK frame was introduced to solve this problem. It was noted that CSMA is of some use in preventing the station from simultaneously sending an RTS to the same destination as another nearby station, thus adding carrier sensing. Moreover, for each data stream (source-destination pair) the back-door algorithm was run separately instead of for each station. This change increases the protocol's fairness. Finally, a mechanism to exchange information on congestion was added to the stations, so that the back-up algorithm reacts less violently to temporary issues and improves system performance.

## 9.14 Summary

Wireless networks build on IEEE Standard 802.11 and its various flavours in universities, businesses and homes are growing and proliferating. The stations and access points share a common channel for data transmission in each of these networks. The network participants should avoid simultaneous transmission as air is a broadcasting channel. If two participants send a collision and both senders' data may be lost at the same time. The Medium Access Control (MAC) is responsible for handle collisions and minimize their impact on performance.

## 9.15 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 9.16 Activities

- Describe the different features of Carrier Sense Multiple Access (CSMA) Protocols,
- Explain the various versions of Carrier Sense Multiple Access (CSMA) Protocols,
- Describe fundamental characteristics of propagation delay,
- Explain CSMA's approach towards a Wireless LAN,
- Elaborate on binary countdown,

## 10.1 Introduction

Local wireless networks (LANs) play a leading role in the IT revolution. They have entered a wide range of markets including the financial, corporate, health and education sectors. The quick use of wireless LANs bears witness to the advantages of this technology. Unfortunately, at this time most wireless deployments are essentially insecure. This is not an overstatement. It is a precise evaluation of the actual security situation for wireless environments 802.11. Due to its transmission feature, a number of safety issues were identified. This chapter aims to introduce the wireless LAN security mechanism and highlights its weakness.

## 10.2 Unit Objectives

- Draw the attention from wireless to wired networks,
- Explain the change in signal loss and fading,
- Offer a broad overview on multipath distortion,
- Highlight the need for shared airwaves,
- Give a brief apercu of wireless LAN components,
- Be able to distinguish between the different types of wireless networks,
- Identify the need for Virtual Private Network,
- Understand concept of SSID and Bluetooth.

## 10.3 Wireless versus Wired (Ethernet) Networks

For communications between fixed sites, wired networks, like Ethernet, are used. For communications between devices, wireless networks such as Wi-Fi are available. There is no distinction in fixed site devices, but the main benefit of Wireless is device mobility. The air is free, but one still needs a wireless connection to a computer or the wired network, a power and radios source to operate wireless networks. The cost of a wired network is easy to estimate. The network cable costs, interfaces and connecting wires; installation of the cable and the interface; network interfaces and long-term maintenance of the installed wiring facility.

Wireless network costs are harder to estimate. These include cables, access points, wireless interfaces, and long-term wireless troubleshooting and maintenance. The other significant problem of wireless devices is the need for a source of power. Wired network nodes can get power from a local receptor, but mobile devices are dependent on the battery or some power supply. Wireless devices can be plugged into a local power source, but then the mobility advantage is lost and power connections on the device are installed at a low cost. In some ways, the recent IEEE 802.3af Power over Ethernet (PoE) standard helps to solve the problem by transporting energy to the wired Ethernet network, so that wireless access points are available.

It is still too young for the standard to be accepted very early, but it is probably popular when products penetrate the market. The problem of the power of a wireless system itself is still unanswered by PoE.

## 10.4 Signal loss and fading

One of the most irritating aspects of the wireless network is probably the spontaneous loss of communication for no apparent reason. Often even before you can investigate the cause of your loss, the signal returns mysteriously. This happens with mobile phones, Wi-Fi and all the other LAN wireless technologies. The deterioration may occur because of interference in the same spectrum from other radio signals as well as moving equipment. Dead spots in buildings may occur, depending on their building materials. Every time the radio wave passes through a solid, the signal slows down in the line of sight between the access point and the wireless device. More than less dense materials are attenuated by denser materials.

## 10.5 Multipath distortion

Radio waves are moving in every direction from an omnidirectional antenna. If these radio waves hit a very thick item, like metal or stone, then they reflect, as the light reflects a mirror or another glittering surface. Even if the path from the transmission to the receiving antennas is clear, some of the signal reflected by other paths will reach the antenna. This is a multi-road distortion that can affect the signal received, because the longer route causes the signal to get out of phase with the signal from the direct route.

## 10.6 Shared airwaves

One of the problems with radio is that the spectrum is small and smart people are finding new uses constantly. It is the responsibility of government agencies to try and assign certain frequency bands to specific uses. The process of frequency allocation is highly political and technological-level. In addition, frequency assignment is highly dynamic and economically sensitive, and new solutions are emerging. Shared radio frequency users require some kind of access control so that interference can be prevented. With the demand for radio bands rising, higher frequencies can also be used economically. The increase to higher frequencies allowed for higher exchange rates. But this often leads to shorter messages and usually takes up the sender's range or distance from the receiver.

## 10.7 Loss of privacy

Anyone can receive the signal when a radio broadcast enters the air. Wired communication requires a physical electric link or at the very close proximity of the wire to intercept the signal. Governments have declared that it is illegal to intercept a wired signal and may only take place by a court order. For radio signals, there are no such limitations. Anybody can receive if you broadcast. However, some radio broadcasts have been illegally listened to by law. Radio signals can be made more private by solutions.
Although the level of privacy of ordinary wired communication cannot be precisely measured, many ways are not possible to make radio transmissions difficult to read, even if they are not impossible to receive. One of the most common ways for privacy to be achieved is through use of highly directional radio antennae that can intercept only if the spectra between sending and receiving antenna are accurately knowledgeable and accessible. Located on towers and rooftops, these sight-line antennas physically reduce the interception potential.

Encryption is the science of using a method and a key to scratch the data. Decryption is the way the data is scrapped using a key to restore it to its initial shape. To unlock and decrypt the data, the intercepter would need the encryption key. Easy encryption is sufficient to protect non-critical or non-vital data, but for data exchanges with personal or financial data more complex encryption is needed.

A physical wiring or network element, such as a cable hub or switch, is established for joining a wired network. Wireless devices are not connected and are neither network-unconnected. They must first try to join the wireless network in order to communicate. A network address is necessary as part of the protocol to connect to the network.

## 10.8 Wireless LAN Components

Wireless Internet consists of two kinds of devices: a wireless station and a point of access. A station or customer is typically a PC with wireless NIC or laptop or notebook. A Wireless Client may even be a desktop or a handheld device or equipment within a kiosk in a manufacture or other publicly accessed area (i.e. PDA) or custom device, such as bar code scanners. Wireless laptops and notebooks are the same as laptops and notebooks - 'wirelessly enabled;' except they are connected to network access points via wired NICs.

Wireless NICs are usually included with the slot or Universal Serial Bus (USB) port of the customer's personal memory card (PCMCIA) slot. Radio signals are used by the NICs to establish WLAN connections. The AP, a bridge between wireless and wired networks, typically includes a radio, wired network interface and software for bridging. The AP acts as a wireless network base, which aggregates several wireless stations to the wired network. There are different types of wireless networks as described below.

### 10.8.1 WLANS: Wireless Local Area Networks

WLANs as shown in Figure 10.1 allow users to form a network or gain access to the internet in a local area such as a university campus or library. A temporary network can be formed without an access point by a small number of users, as access to the network resources is not necessary. The radio communication device known as the Access Point connects network computers in a wireless local area network. The range of a single access point is up to 300 meters (100 meters). (Depending on the number of users involved, interference, barriers to transmission, such as walls and construction material, and other factors).

A Wireless Network Adapter Access Point communicates with devices that connect to a wired Ethernet LAN through an RJ-45 port. Access point devices normally cover up to 300 feet (approximately 100 meters). This area is known as a cell or range. With your laptop or other network device, users move freely in the cell. In order that users can even "roam" within or between buildings, access point cells can be linked together.

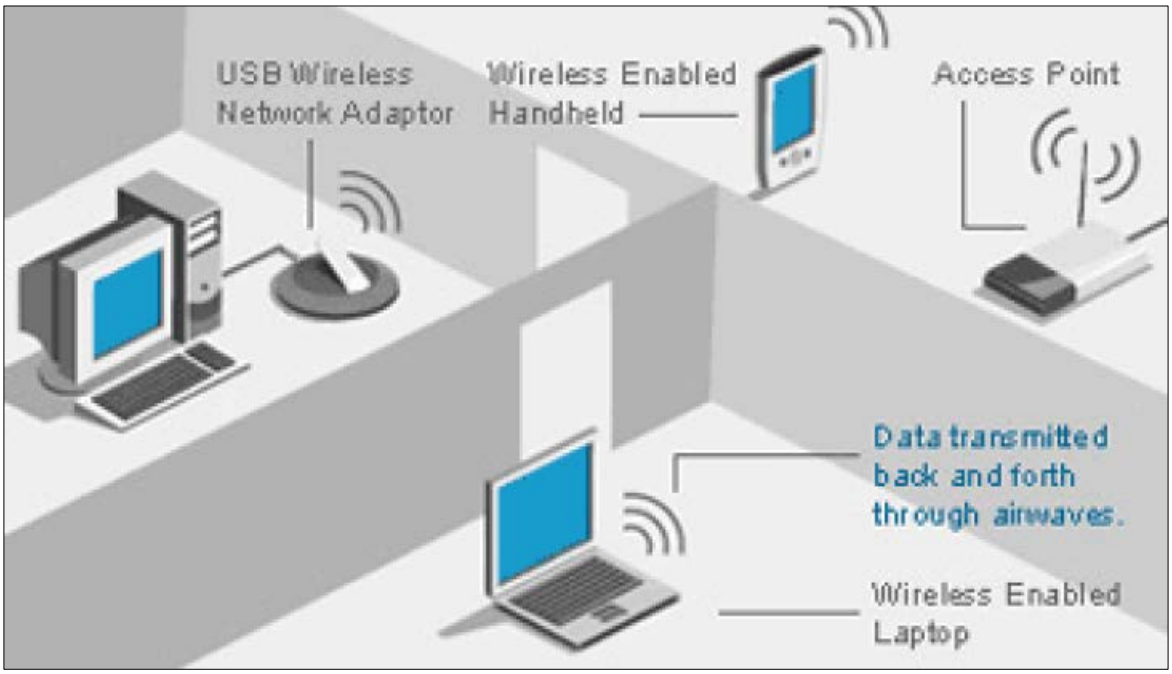



**Figure 10.1 – Wireless LANs**

### 10.8.2 WPANS: Wireless Personal Area Networks

Usually a personal area network (Figure 10.2) device can reach up to 160 feet (50 meters). (Depending on the number of users involved, interference, barriers to transmission, such as walls and construction material, and other factors). You can connect your system to a printer, synchronize your PDA and a mobile phone, download images from a digital camera, and transmit MP3 files with a wireless personal area network. Infrared (IR) and Bluetooth are the two existing technologies for wireless pans (IEEE 802.15). This allows personal device connectivity over an area of approximately 50 meters. But IR requires a direct site line and a smaller range.

Bluetooth® allows data transmission through shortened radio waves between devices such as mobile devices, handheld devices or notebooks or desktop computers, for example to update your calendar on the device and sync the data onto your notebook computer with the calendar. WPAN represents network technologies for wireless personal areas such as Bluetooth and IR.

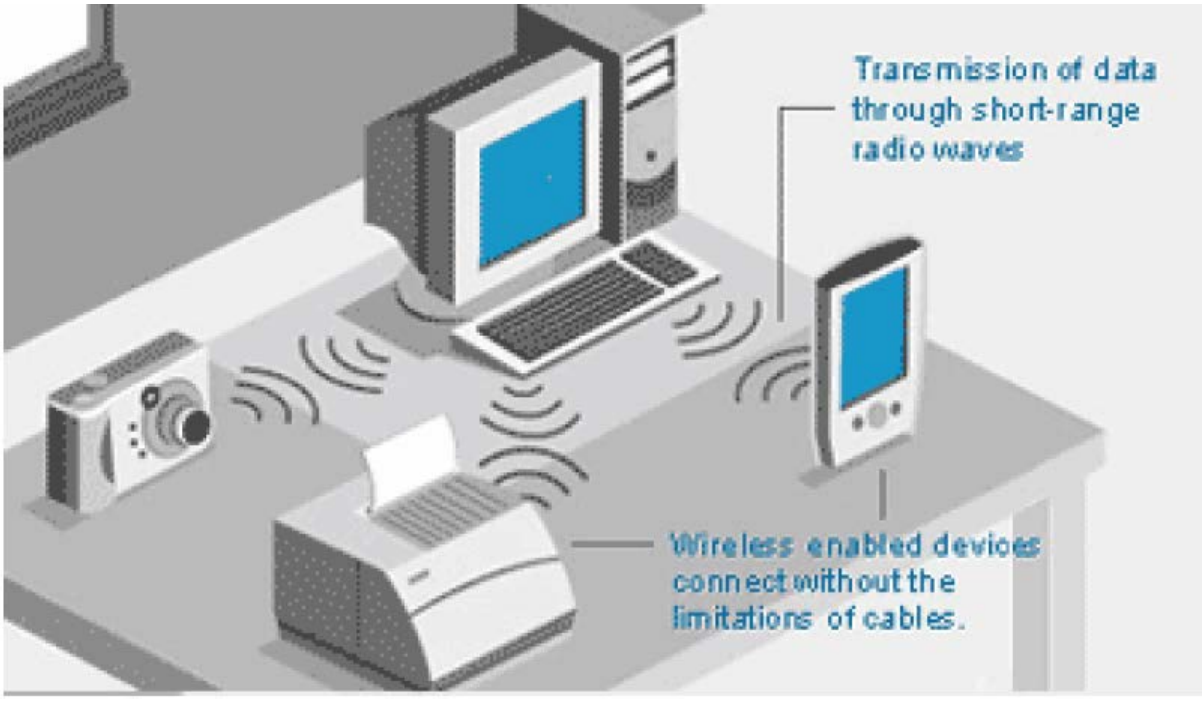



Figure 10.2 - WPAN

### 10.8.3 WWANS: Wireless Wide Area Networks

Wireless Wide Area Networks transmit data via a mobile telephone service provider via a mobile phone with connection speed of 56K. Its scope can reach 20 miles (30 km) and allow users to connect away from other network infrastructures while on the move. Such networks can be maintained through multiple satellite systems or antenna sites managed by an ISP in large areas, such as cities or countries. These systems are called 2G systems (2nd generation). WWAN includes broad coverage technologies like cellular 2G, Digital Cell Packet Data (CDPD) and the Global Mobile Communications System (GSM) and mobile devices. An example is depicted on Figure 10.3


**Figure 10.3 - WWAN**

Range that wireless data networks can handle:

- Wireless Personal Area Network: 0-50 m
- Wireless Local Area Network: 0-100 m
- Wireless Wide Area Network: 0-30,000 m

## 10.8.4 VPN (Virtual Private Network) Link

In environments where the data on the wireless network may be passed through the Internet, VPNs (Figure 10.4) may be used to provide another layer of security solutions.

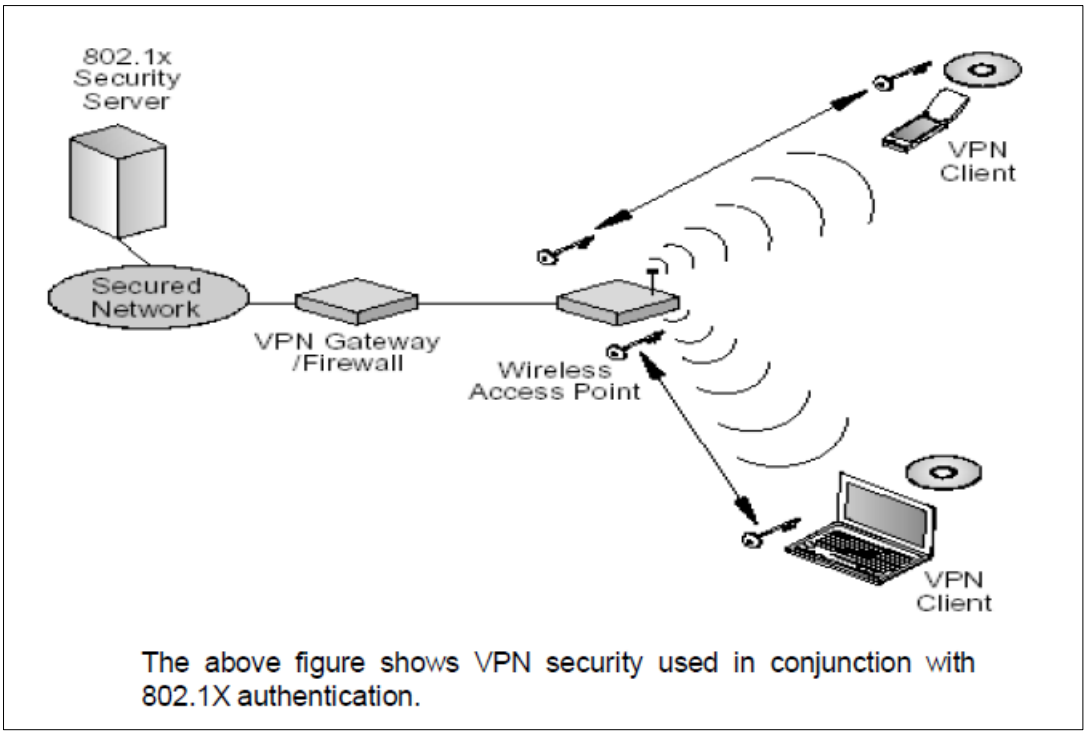



**Figure 10.4 - VPN**

## 10.9 MAC (Media Access Control) address filtering

Controlling which network adapters access the Access point is an instrument of MAC Address Filtering. There will be a list of MAC addresses in the access point and entry not allowed to anyone whose MAC address does not match the MAC address in the list on the wireless network adapter. If a computer requests, it compares its MAC address and permits to be granted or denied to the list of MAC addresses in the Access Point. When used with a packet encryption method, this is a very good security means. MAC addresses can nevertheless be spoofed. It is recommended only for smaller networks since each MAC address is entered in every Access Point with a high work rate. This type of security is usually used as a means of authentication, in conjunction with something like WEP for encryption. This security type is usually used as an authentication tool for encryption, in conjunction with WEPs. Figure 10.5 is a basic picture showing the filtering process of the MAC address:

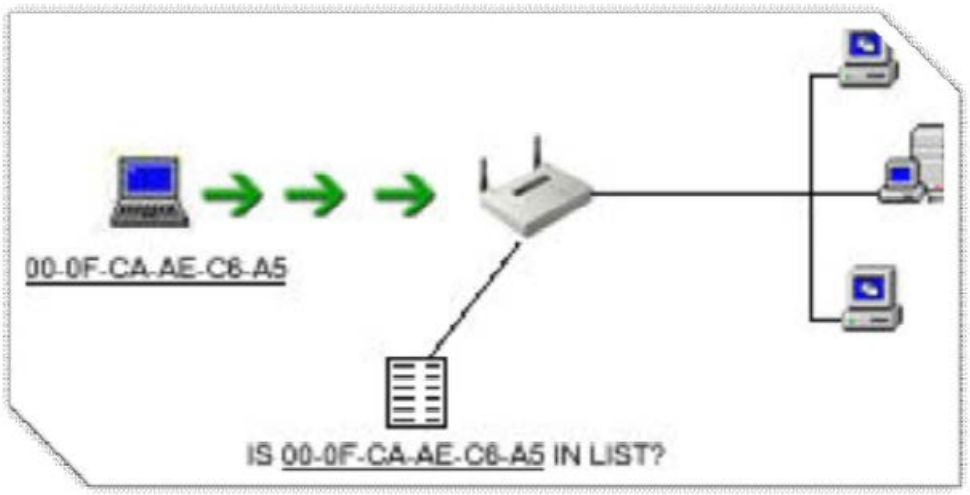



**Figure 10.5 - WEP**

A laptop, with MAC Address 00-0F-CA-AE-C6-A5 wants to access the wireless network via the access point. The access point compares this Address to its list and permits or denies access accordingly.

## 10.10 SSID (Service Set Identifier)

By enabling a WLAN network to split into different network with a unique identifier, SSID works with a simple password. These IDs are programmed to multiple points of access. A client computer with a respective SSID identifier for that network must be configured to access any of the networks. If they match, the customer's computer will be given access. SSID vulnerability is announced in plain text in the beacon messages of the access point. While users can easily determine the SSID via an 80.11 wireless LAN packet analyzer, a beacon message is transparent for users (for e.g., Sniffer Pro).

## 10.11 Bluetooth

Bluetooth is a simple wireless networking type that makes it possible to establish a small network that connects up to 8 devices at once. The PDAs, laptops, mobile phones and personal computers would be included in these devices. Bluetooth is a networked area because it has a very short distance of 30 to three hundred feet. This kind of range adds to the safety of such technology by not only requiring special equipment to sniff your link, it also needs to remain relatively close to you. Bluetooth's main features are that, contrary to Infra Red, the signal is not affected by walls and uses radio technology.

## 10.12 Wi-Fi

Wireless Link refers to two wireless protocol types, IEEE 802.11(b "wireless B") and IEEE 802.11g ("Wireless G"), which can work together. Both computers can be connected very quickly: 11 megabits per second (Mbps) for wireless B and 54Mbps for wireless G. By comparison, 100Mbps connect Ethernet networks. Wireless B and G can both broadcast 150 feet, but overlapping broadcast points allows you to expand the range of wireless G networks. The so called daisy chain is produced.

## 10.13 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. Most commonly used wireless handheld devices are text-messaging devices, PDAs and smart phones. Examples: Access Point (AP), Wireless Network Card, Personal Digital Assistants, Smart Phones

## 10.14 Wireless network types

Wireless network (hosted or managed) – also called a wireless network 'hosted or 'managed' – consists of a connection to an existing network of one or more access points (known as gateways or wireless routers). This allows the use of network resources such as printers and the Internet by wireless devices.

The Ad-Hoc is the second. Also called wireless network "unmanaged," "peer to peer" or "Bluetooth." Each device is directly connected to each other. The "piconet" master controls the changing topologies of the network. It also controls data flow between devices, which can support direct connections between devices. As equipment moves unpredictably, the dynamic topology requires that these networks are reconfigured on fly. The Bluetooth routing protocol allows the master to set up and maintain these shifting networks.

## 10.15 Summary

The chapter discusses wireless networks that can be connected without any physical connection by multiple devices. The development of the Wireless LAN group which connects devices and networks through an access point. Wireless LAN's various factors include frequency and data rates, architecture of IEEE 802.11, components, scope and benefits. The security issues, the implementation of wireless LAN and the risks and threats associated with wireless LAN security are to be explored further.

## 10.16 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings

## 10.17 Activities

- Describe the difference between wireless and wired network,
- Explain the following terms – signal loss and fading, multipath distortion, shared airwaves,
- Differentiate between the various WLAN components,
- Distinguish among the various types of wireless networks,
- Differentiate between VPN and MAC.

## 11.1 Introduction

The quality of service network (QoS) is a new term, defined as: "the ability to control network traffic management mechanisms to meet the service needs of certain applications and users subject to network policies." QoS networks must have mechanisms for controlling the resource allocation between applicants in order to provide the measurement and control capabilities required by each definition. The concept of QoS was developed to respond to the new demands made by modern applications, in particular multimedia real time applications, on network performance. These applications required limitations to be defined as an acceptable delay when routing data across a network

## 11.2 Unit Objectives

- Draw the attention of the term QoS,
- Explain the requirements for QoS,
- Offer a broad overview of Network QoS,
- Highlight the techniques for achieving QoS,
- Give a brief apercu of each techniques.

## 11.3 Quality of Service (QoS)

Process for the reliable or better delivery of data than conventional. The network's ability to supply data based on traffic classification and priority management that focuses on the management of traffic. Capability in a network to provide assurance of resources and services. QoS is also a range of techniques that give priority to one type of traffic or program operating across a network connection rather than using only the best effort. However, with the growth of multimedia networking, often these ad hoc measures are not enough. Serious attempts at guaranteeing Quality of Service through network and protocol design are needed.

## 11.4 Requirements

A stream of packets is called a flow from source to destination. All packets belonging to a flow follow the same route in a connection-oriented network. They can follow different routes in a connected network. Four primary parameters can characterize the needs of each parameter:

- Reliability
- Delay
- Jitter and
- Bandwidth

Together these determine the QoS (Quality of Service) the flow requires.

The Most Important Among the Four Parameters? – Bandwidth Has a significant impact on other QoS parameters. There would be no congestion and, therefore, no loss if there were enough bandwidth available. The availability of bandwidth reduces delay and jitter. Basic bandwidth means: low data loss, low delay, low jitter, and QoS systems aim to meet bandwidth requirements by guaranteeing availability for applications bandwidth

## 11.5 Network QoS

Network QoS means the ability to provide: Minimal data loss, Minimal delay, Consistent delay characteristics/ jitter, Capability to determine the most efficient use of network resources or maximum bandwidth. Non Time-Sensitive and Time-Sensitive Applications include the following:

**Non-Sensitive Applications**

- Adaptive to increased delay
- Also called elastic applications
- Lost packets can be retransmitted
- Major requirement: **complete data transmission**
- Examples: Telnet, FTP, E-mail, WWW

**Time-Sensitive Applications**

- Applications with strong timing requirements
- Sensitive to loss, delay and jitter
- Examples: Voice/Video Streaming, Voice/Video Conference

## 11.6 Techniques for Achieving Good Quality of Service

### 11.6.1Overprovisioning

Overprovisioning is an easy way to provide a high level of router capacity, buffer space and bandwidth to allow packets to easily travel. The downside is that implementing this solution is expensive. In future, this technique can even become practical if designers have a better idea of how far it is enough. Example of the system over-supplied: The telephone system is to some extent an over-supplied system. A telephone is seldom collected and not dialed immediately. There is just so much capacity that demand can always be fulfilled.

### 11.6.2 Buffering

With the buffering technique, flows can be buffered on the receiving side before being delivered. Buffering them does not affect the reliability or bandwidth. It increases the delay but it smooths out the jitter. For audio and video on demand, jitter is the main problem, so this technique helps a lot. In Figure 11.1, Packet 1 is sent from the server at t = 0 sec and arrives at the client at t = 1 sec. Packet 2 undergoes more delay and takes 2 sec to arrive. As the packets arrive, they are buffered on the client machine

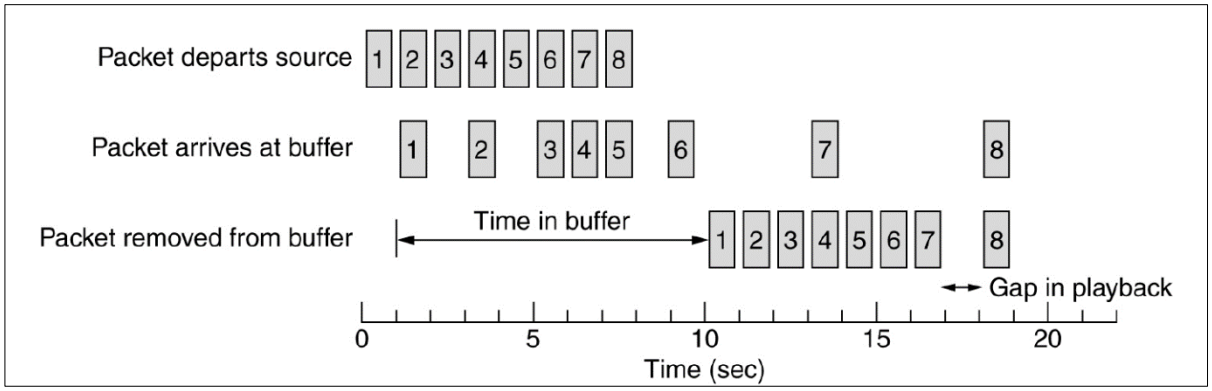



**Figure 11.1 - Buffering**

Playback starts at t = 10 sec. Packages 1-6 were buffered at this time so that they can be uniformly removed from buffer for a smooth play. Packet 8 has unfortunately been delayed so much that when its play slot arrives it's not available so that playing must stop until it arrives and creates an annoying gap in music or the film. The delay of the starting time can alleviate this problem further, although a greater buffer is also required. Note: Commercial Web sites with audio or video streaming all use players buffered approximately 10 seconds prior to starting playing.

### 11.6.3 Traffic Shaping

If a server (and hosts generally) were to transmit at a consistent rate, QoS would improve. Traffic design is a process that smoothes traffic on the server side instead of on the customer side. The shaping of traffic involves regulating the average data transmission (and bursting). When a connection is set, a particular route pattern (i.e. the shape) is agreed between the user and the subnet (i.e. customer and carrier). This is known as a service level contract (SLA). As long as the host fulfills its share of the deal and sends only packages under the agreed agreement, the carrier undertakes to deliver them in a timely manner.

**How does Traffic Shaping work?** *At the source: it r*ecalls that bursts → congestion, Smooth out the traffic at the source, Regulate average rate and bustiness, Service Level Agreements (SLAs) and a Contract between the user and the carrier

**How does the carrier tell if the user is following the SLA?**

It monitors the flows and networks (traffic monitoring) the income traffic flows as well as the shaping of traffic to ensure that a packet stream meets certain parameters. Networks may form their traffic before it is transferred to another network. It must be noted. This is shown in Figure 11.2

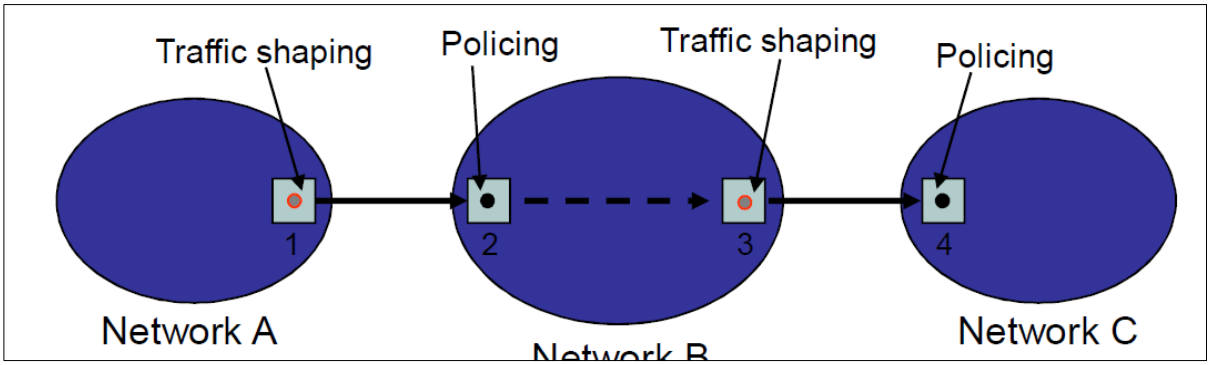



**Figure 11.2 – Traffic Shaping**

The advantage is to reduce congestion by forming traffic and thereby assist the carrier to fulfill its promise. SLAs do not matter so much for file transfers, but are important for real-time data such as audio and video connections with strict quality standards.

## 11.6.4 The Leaky Bucket Algorithm

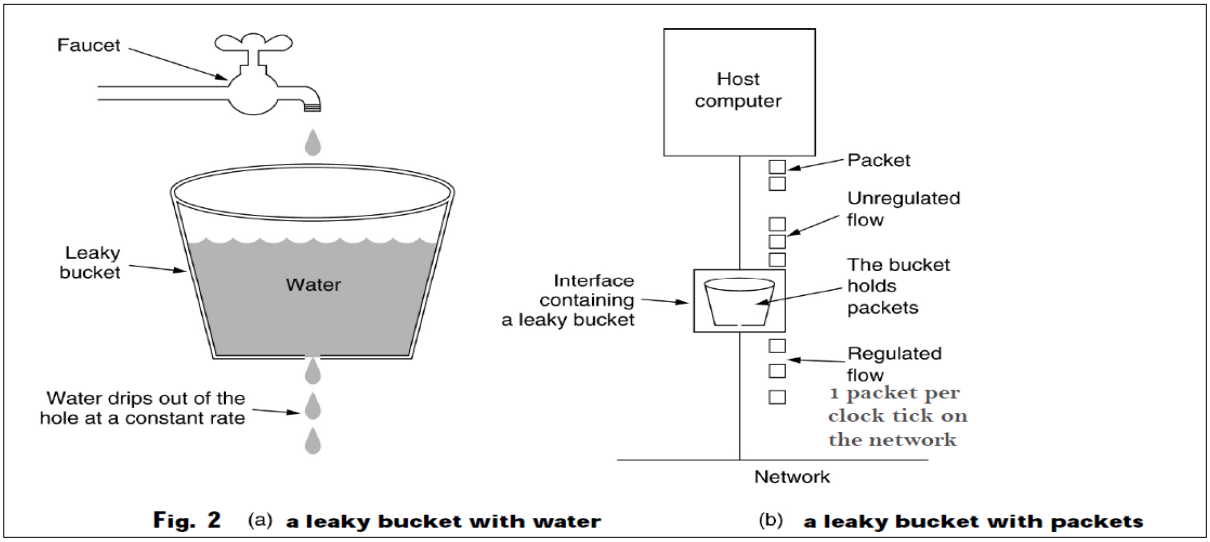



Figure 11.3 – Leaky Bucket

A water-leaked bucket: Think of a bucket with a small hole in the base, as Figure 2 shows (a). Regardless of the rate at whatever water enters the seal, the outflow rate is constant, ¨, provided there is water in the seal and zero if the seal is empty. Furthermore, once the bucket is full, any further water enters the bucket, which falls over the sides and is lost. The Leaky Bucket algorithm looks like a leaky packet analogy: As shown in Figure 2 the same idea is applicable to packets (b).

Each host is connected by a leaky bucket interface, i.e. a finite indoor queue, to the network. Indeed, the leaky bucket is a limited queue. When a packet arrives, the queue will be filled; otherwise, the packet will be discarded if the queue is full. One packet is transmitted at each clock tick (unless the queue is empty). In other words, if the new packet is abruptly discarded if one or more processes in the host try to send out a packet if the maximum number is already queued. This system can be built into the hardware interface or simulated using the host operating system. In fact, it is nothing other than a single-server queueing system with constant service time. The host can put a packet on the network each clock (this can be enforced by the interface card or by the operating system). This mechanism turns an uneven packet flow from host user processes into an even packet flow onto the network, lightens explosions and greatly reduces congestion chances.

This algorithm can be used efficiently when the packets are all the same size (e.g. ATM cells). But this algorithm may not produce the desired results in an IP network where variable-sized packets are used! Solution: Allow a fixed byte per tick instead of only one packet. Therefore, if the rule is 1024 bytes per tick, one packet of 1024 bytes, two

packets of 512 bytes OR 4 packets of 256 bytes etc can be admitted on the tick. The next packet has to wait until the next tick if the remaining byte count is too low.

### 11.6.5 The Token Bucket Algorithm

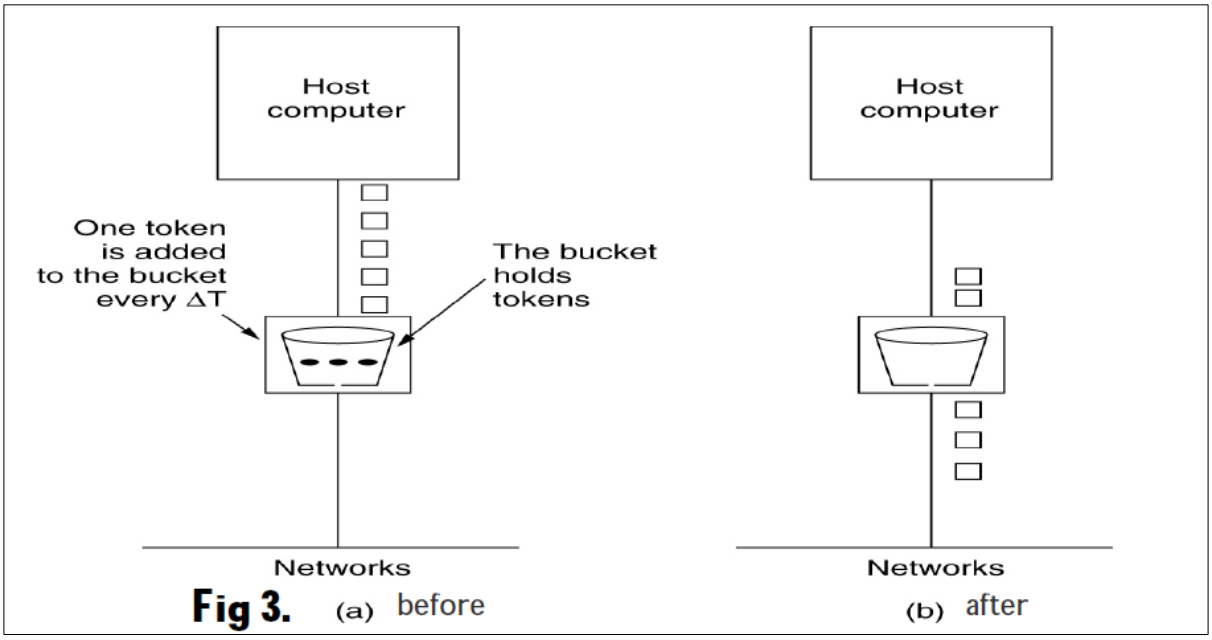



**Figure 11.4 – Token Bucket**

The leaky bucket algorithm enforces the average rigid output pattern; however, explosive the traffic is. In most applications, the output can be speeded up a bit if there are large explosions, so a more flexible algorithm, which preferably does not lose data, is needed. The token bucket (Figure 11.4) algorithm is one such algorithm. The leaky bucket has tokens in this algorithm, which are produced at one token per clock, all of which are T sec. Figure 3(a) shows a bucket with three tokens and five packets waiting for transmission. It must capture and destroy one token for a packet to be transmitted. Figure 3(b) shows that three of the five packets were passed, but the other two still wait to produce two more tokens. The host can stop sending a token bucket that regulates a host when the rules say so. If a router stops sending while its input flows, data may be lost. The use of the basic token bucket algorithm is only a tokens variable. When a packet is sent, the counter is augmented by one each way and decreased by one. No packets can be sent when the counter hits zero.

Maximum-speed burst of length S seconds, i.e, MS is given by:

Maximum-speed burst of length S seconds, i.e, MS is given by:

$$MS = C + \rho S$$

$$\text{that is, } MS - \rho S = C \text{ or } S(M - \rho) = C$$

$$\text{Therefore, we get } S = C/(M - \rho)$$

where S = burst length (in seconds); C = token bucket capacity (in bytes); M= burst rate (in bytes/second); ρ = token arrival rate (in bytes per second).

It must capture and destroy one token for a packet to be transmitted. Figure 3(b) shows that three of the five packets were passed, but the other two still wait to produce two more tokens. The host can stop sending a token bucket that regulates a host when the rules say so. If a router stops sending while its input flows, data may be lost. The use of the basic token bucket algorithm is only a tokens variable. When a packet is sent, the counter is augmented by one each way and decreased by one. No packets can be sent when the counter hits zero. The token bucket algorithm throws away tokens (i.e., transmission capacity) when the bucket fills up but never discards packets. In contrast, the leaky bucket algorithm discards packets when the bucket fills up.

### 11.6.6 Resource Reservation

The QoS guarantee is a good start to be able to control the form of the offered traffic. Use this information effectively implicitly, however, means that all flow packets have to follow the same route. It is difficult to guarantee anything by sending them over routers at random. As a result, something similar to a virtual system needs to be configured and all packets of the flow must follow this route from source to destination. When we have a particular route for a flow, resources can be reserved along this route to ensure that the necessary capacity is available.

Three different kinds of resources can potentially be reserved:

- Bandwidth.
- Buffer space.
- CPU cycles.

**Bandwidth:** If a flow requires 2 Mbps and the outgoing line has a capacity of 5 Mbps, trying to direct three flows through that line is not going to work. Thus, reserving bandwidth means not oversubscribing (overflowing) any output line.

**Buffer Space:** The supply of buffer space is often lacking. Usually, a packet will be placed by the hardware itself on the network interface card. The router must then copy it in a memory buffer (RAM) and queue the buffer on the selected output line for transmission. If there is no buffer, the packet needs to be dropped as there is no place to put it in. Some buffers may also be reserved for a certain flow in order to make it difficult for the flow to compete with other buffers. If the flow needs one, up to a maximum there will always be a buffer available.

**CPU cycles:** They are a scarce resource as well. Router CPU time is needed for processing a packet and only a number of packets can be processed by the router every second. To ensure a timely processing of each packet the CPU is not overloaded.

### 11.6.7 Admission Control

Now, we are at the point where the incoming traffic from certain flows is well formed and can possibly travel along a single route, where routers can reserve their capacity in advance. If such a flow is provided to a router, it needs to decide whether the flow is accepted or disallowed, based on its capacity and its commitments to other flows. Control of admission is based on a decision to accept or dismiss traffic flow. We have to find out if the resources are enough for the incoming flow (bandwidth, buffer, CPU-cycles). The decision to accept or reject a flow is not simply a question of comparing the excess flow capacity of the router with those three dimensions (bandwidth, buffers, cycles). Since many parties (sender, receiver and all routers along the path between them) can take an interest in flow negotiations, flows must be accurately described according to the specific parameters negotiable. The flow specification is a set of such parameters. The sender (for example, a video server) generates a flow specification which provides the parameters it wants to use. As the specification propagates along the route, each router examines it and may even modify the parameters as need be.

### 11.6.8 Proportional Routing

It split the traffic over multiple paths. It can be done **locally only.** Router normally do not have complete overview of the whole network-wide traffic! The approach is that it divides traffic equally over outgoing/output paths and also divides traffic in proportion to the link capabilities

### 11.6.9 Packet Scheduling

It discusses: how to put the packet in the queue and which packet should be sent out of the queue. It has a machine Enabled Mechanism for forwarding: Place incoming packets in a queue, take each packet and look at its header for the next hop. Then put the packet in the queue for the relevant exit interface. The algorithm of tradition: First-Come First-Serve is used where a single queue for all the flows is used and incoming packets are placed in the queue. Every flow is fair: every flux is treated in equal measure. No hunger, packets are honored in the order they are received. Fair to every packet; Therefore, later packages need to wait in the queue for just a few times.

## 11.7 Summary

The chapter described how VoIP is about multimedia (audio, video, text, graphics, etc.) transmission over IP networks. The main differences between VoIP and dial up networks are the signalling protocols and real time transmission. SIP is a dominant signalling protocol together with SDP in VoIP. The unit also shows how conversion is done from denary to binary and in hexadecimal. Furthermore, a binary number can be represented in exponent and mantissa. The final part described the shift unit, range and accuracy.

## 11.8 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 11.9 Activities

- Describe the techniques for achieving good QoS,
- Elaborate on the four parameters in achieving QoS.

## 12.1 Introduction

Traditional IP network intradomain routing systems or internal gateway protocols compute routes on the basis of algorithms which maximize paths based on a single scalar metric. This is done in a single scalar. For example, the minimum number of hops could be so high that a shortest path through a network can be calculated. This is how it calculates what is considered the shortest way by the Route Information Protocol (RIP). RIP calculates the fastest path using the Bellman-Ford algorithm and reduces path calculation based on a vector distance algorithm. RIP may be used in smaller networks, but in moderate networks, intrinsic problems related to routing loops and the time needed to converge on the solution are found. For this reason, OSPF and IS-IS have been selected for use in medium to large intranets (but not the Internet). This chapter provides an in-depth detail of these concepts.

## 12.2 Unit Objectives

- Draw the attention of Intra domain routing,
- Explain the different interior and exterior gateway protocol,
- Offer a broad overview on Routing Information Protocol,
- Highlight the need for Open Shortest Path First (OSPF),
- Give a brief apercu of Enhanced Interior Gateway Routing Protocol (EIGRP),
- Be able to distinguish between the different Open Shortest Path First (OSPF) concepts,
- Identify the need for Open Shortest Path First (OSPF) router classifications,
- Have an idea of the Border Gateway Routing Protocol (the Exterior Gateway Routing Protocol),
- Understand concept of Operation of OSPF.

## 12.3 Routing

The routing of packets is an important function of the network layer. A routing algorithm is responsible for deciding on which packets are to be transmitted on the output line. If a network datagram: The choice of routing for every packet is new. Where a VC network: decision on routing for the VC application. Packets then follow the path that is established. The routing algorithms aim to be accurate, simple, robust, stable, fair and optimal. Methods of routing include: Dijkstra (algorithm of link state routing), Fluting, Bellman-Ford (algorithm of distance vectors), Random

## 12.4 Intra-domain Routing

Intra-domain routing is also known **as Intra-AS Routing. Autonomous System (AS) -** An autonomous system is a collection of hosts/routers under administration control. It may consist of multiple LANs. Figure 12.1 depicts intra-domain routing.

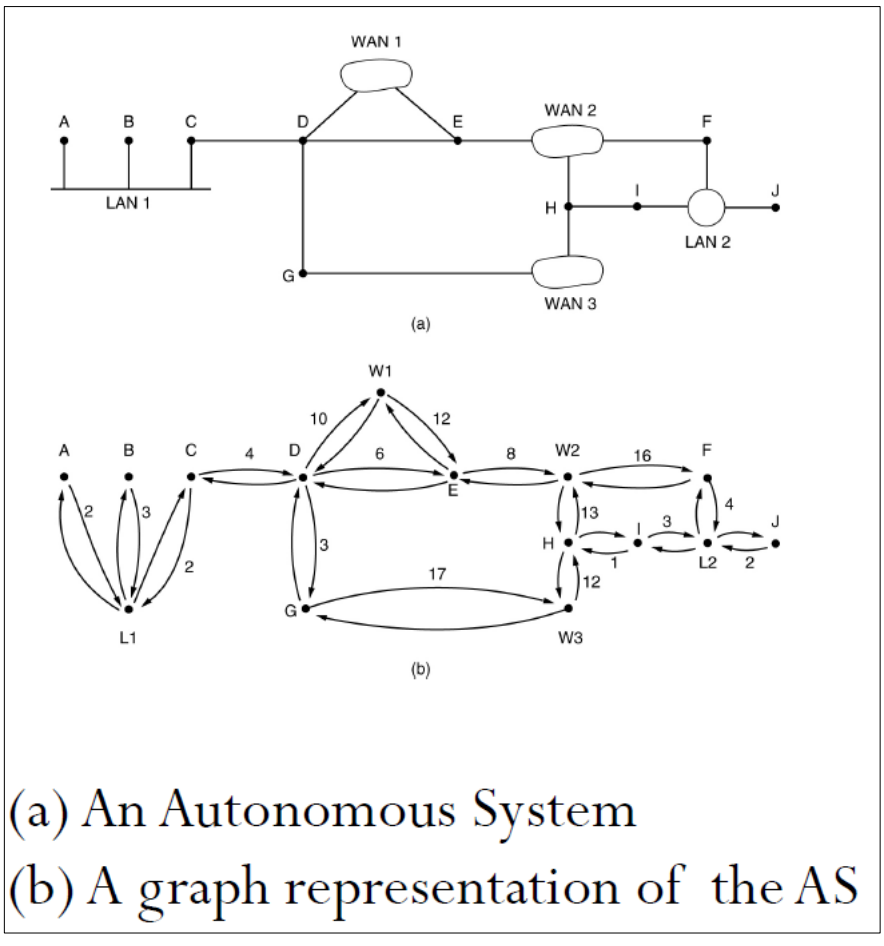



Figure 12.1 – Intra domain routing

A large number of autonomous systems are available on the Internet. The each AS has its own routing algorithm inside and is operated by a different organization. For example, if all three of them are on the Internet, the internal networks of X, Y and Z could be considered as three ASs. All three can internally use various routing algorithms. An internal gateway protocol is called a routing algorithm within an AS (intra-AS). An external gateway protocol is referred to as a routing algorithm for routing between ASs (inter-AS). The routing tables are set up and maintained within an AS. Also called internal protocols gateway (IGP). Three protocols have been historically used for routing:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protcol (EIGRP), which is Cisco's propriety

### 12.4.1 Routing Information Protocol (RIP)

One of the first intra-domain protocols was RIP. Still in use, popular because BSD Unix has been included. There are two versions: original and 2. It is based on a Bellman Ford algorithm, the distance vector protocol: neighboring routers every 30 seconds exchanges messages. RIP response message called message RIP response (or RIP advertisement). The cost metric is the hop-count in the original version. In small systems, RIP worked well, but it was less as well as ASs. RIP suffered from the problem of counting to endlessness (may take a long time to converge). RIP had no subnet addressing knowledge. RIP used the metric number of hop (other variables not taken into account). RIP was replaced by a link state protocol – its successor called **Open Shortest Path First (OSPF)**.

## 12.4.2 Open Shortest Path First (OSPF)

The RIP succeeding. In 1990, OSPF became a norm. Now OSPF is supported by most router vendors. It has therefore become the principal protocol of the interior gateway. OSPF is another protocol for intra-domain routing. It is a 0-pen protocol, a public domain and a link-state protocol, Dijkstra algorithm used for SPF, which is the main characteristic of the project.

In a hierarchy OSPF can function. It is the AS that is the most important entity. AS is split into area (will be explained in subsequent slides). Every area will work with the routing algorithm. OSPF can divide an AS into areas. Areas are not exhaustive but do not overlap. Topology and details are unknown outside an area. The area is the widespread subnet process. Each router must have the same link-state and run the same SPA within an area and must have the shortest path to any other router within its area.

### There is various router classification:

- Internal routers: routers located within (inside) an area.
- Area border routers: routers that connect outside of area (within AS), that is, connects two (or more) areas.
- AS boundary routers: routers that connect to other Autonomous Systems, that is routers that can communicate with routers in other ASs.

When a router boosts it will send HELLO messages to the group of all other routers on all its dotted lines and multi-taste them on the LANs. With WANs, it needs certain settings to know who to contact. Every router knows who its neighbors are from the answers. All neighbors are routers on the same LAN.

OSPF is a link-state routing protocol that requires Link State Advertises (LSAs) to be sent to all other router within the same hierarchy or the Autonomous System (AS). OSPF LSAs contains information about connected interfaces, used metrics and other variables. Independent Systems OSPF routers collect information from Link State. Then, they are calculating the shortest path to each node using the SPF algorithm first. Note 1: OSPF can function in a hierarchy as opposed to RIP. The autonomous system is the largest entity in the hierarchy (AS). An AS is a group of networks in a common management that share a common routing strategy. Note 2: OSPF is an intra-AS (interior gateway) routing protocol, although it is capable of receiving routes from and sending routes to other ASs.

By sending hello messages it determines neighbors: Hello, every ten seconds, the messages are multicast. If neighbor doesn't get hi 40 seconds, assume that link/neighbor has failed. In datagrams called Link State Advertises (LSAs), each router in the region distributes information about its local environment: Neighboring routers information (links and costs). LSAs are distributed through reliable floods (explicitly acknowledged, sequenced and time-stamped). If you discover a new neighbor or have a link failure or a cost change, refresh your situation at a certain interval. The shortest tree path can be established using this information.

Routers inform other routers in the area using reliable flooding. Then each router can build a graph and find the shortest paths. Backbone area is performing the same process – Backbone also accepts border router information. The best route from each backbone router to any other router can be determined. Information from the backbone sent to border area routers that advertise in their area. OSPF operates through information exchange between adjacent routers (not the same information as between adjacent routers!). Every router on a LAN talk to any router on the LAN is inefficient. Not adjacent neighboring routers do not exchange information. Every router regularly floods LINK STATE UPDATE messages to each of its adjacent routers during normal operation. This message provides the current status and cost of the topology database. The flood messages are recognized (to make them trustworthy!).

A router can see whether a new incoming LINK STATE UPDATE is older or newer than what it currently has. Each message has a sequence number Routers also send these messages when a line rises or falls, or changes its costs. The DATABASE DESCRIPTION messages provide all of the sender's current link status entries with sequence numbers. The recipient can determine who has the latest values by comparing his own values with the sender's. These messages are used especially when a line is raised. By using LINK STATE REQUEST messages, either partner can request link state information from the others. This algorithm results in each adjacent pair of routers checking who has the latest data and new information across the area. A designated router backup should crash and be replaced immediately, is always kept up to date to facilitate a transition. All of this is sent as raw IP packets.

Each router, through flooding, reports on its neighbors and costs to every other router in its area. Each router is able to build the graph and calculate the shortest path for its area(s) This information. This also happens in the backbone area. The backbone routers also accept information from the area border routers to calculate the best route from each backbone to each other. This information is spread back to the border routers in their areas, which advertise it. With this information, you can choose the best exit router to your backbone using an interface packet send router.

## 12.5 Inter-domain Routing: Border Gateway Routing Protocol (the Exterior Gateway Routing Protocol)

Within a single AS, the intra-domain (intra-AS) routing protocol called OSPF is generally used. However, routing between ASs (inter-domain or inter-AS routing) requires another routing protocol. As shown in Figure 12.1 this protocol is called an exterior gateway protocol. The main exterior gateway protocol is Border Gateway Protocol (BGP).

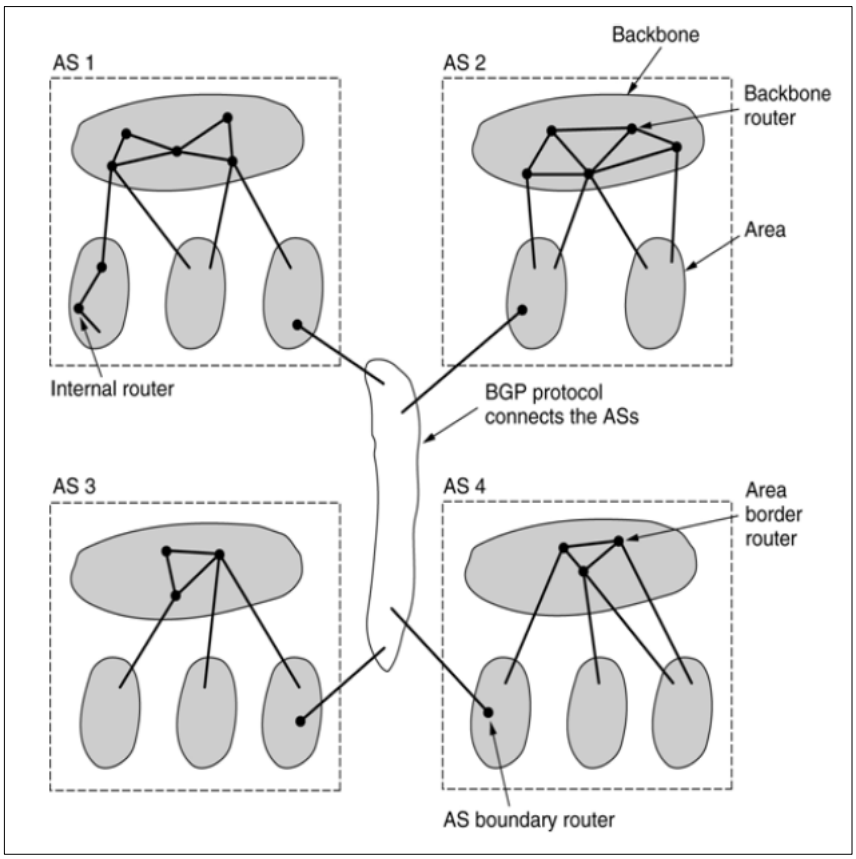



**Figure 12.1 – Border Gateway Routing Protocol**

A different protocol (BGP) is needed, since the goals are different as routing decisions are policy-based, routing based on who controls AS rather than cost or delay and there is a telco that accepts customer traffic, but not other telco traffic. BGP routers classify traffic either Local traffic, that is, traffic that originates or terminates in the AS. Otherwise, the traffic is termed as "transit".

BGP routers classify networks as:

- Stub networks - networks that have only one connection to the BGP graph (cannot be used to transit traffic).
- Multiconnected networks - networks that have multiple connections but refuse to transit traffic.
- Transit networks - networks that are willing to transmit third party traffic (backbone networks).

The Border Gateways Protocol (BGP) is a protocol used by routers in various Automous Systems to exchange routing information (ASs). The complete route to each destination includes BGP routing information. BGP uses routing information to maintain a network accessibility information database that is exchanged with other BGP systems. The network accessibility information is used by BGP to build an AS connectivity graph so that BGP can remove routing loops and implement AS level policy decisions. BGP permits policy-specific routing. Routing policies may be used to select and control the redistribution of the routing information between multiple paths to the destination. As its transport protocol, BGP uses the Transmission Control Protocol (TCP) to establish connections, using port 179. The need to implement updated fragmentation, transmission, acknowledgement and sequence is avoided by running a trusted transportation protocol.

The BGP router propagates path information using path vector routing algorithms (instead of cost). The exact path used is monitored (not just the next hop). Since complete paths are changed it is avoided to count to an endless problem. For Inter-AS internet routing, BGP is the de facto standard. The network access points is also used to connect (NAPs).

## 12.6 Link-state algorithm

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. But only the part of the routing table describing the state of its own links can be sent by each router. Each router generates an image in its routing tables in link-state algorithms of the whole network.

## 12.7 Distance vector algorithms

This is also known as Bellman Ford algorithms) to send each router, but only to its neighbors, all or part of its routing table. Essentially, link algorithms send updates to neighboring routers only, while vector algorithms send larger updates. Algorithms for distance vectors only know about neighbors.

## 12.8 Summary

In this chapter, the focus is on determining optimal link weight systems for designing and traffic engineering of shortest-path routing networks which is faced in Internet intra-domain routing environment running OSPF and IS-IS. Different mechanisms were introduced and explain.

## 12.9 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings


## 12.10 Activities

- Describe the Border Gateway Routing Protocol (the Exterior Gateway Routing Protocol),
- Explain the different BGP routers.
- State how the path vector routing algorithm works,
- Using a diagram explain the intra domain routing.

## 13.1 Introduction

The ultimate aim of the transportation layer is to provide its users with efficient, reliable and economical service, usually processes in the application layer. The transport layer uses the services provided through the network layer to achieve this objective. The transport entity is the hardware and/or software that performs the work. The carrier can locate in a separate user process, a library package linked into network applications, or plausibly on the network interface card in the operating system kernel. Transport network services have two types: connections and connectionless, and transport services of two types. In many ways, the connection-based transport service is similar to the connection-based network service. In addition, transport without connection is also very similar with the network without connection. This chapter also introduces concepts of Internet Transport Control Protocol.

## 13.2 Unit Objectives

- Draw the attention of TCP,
- Explain the need for a port,
- Offer a broad overview on TCP Connection as a Byte Stream,
- Highlight the need for The Silly Window Syndrome,
- Give a brief apercu of TCP Congestion Control,
- Be able to distinguish between Wireless TCP and UDP,

## 13.3 TCP - UDP

UDP is a simple protocol and has many uses: interactions between clients and servers and multimedia. However, reliable, sequenced delivery is required for most Internet applications. Unable to provide this, UDP requires another protocol. It is known as TCP and is the backbone of the Internet. TCP was designed specifically to provide the byte stream of an unreliable end-to-end stream. An internet system varies from a single network, because the topologies, bandwidths, delays, packet sizes and other parameters in different areas may differ uncontrolled. TCP is designed to dynamically adapt and be robust against many types of failures to the properties of the Internet.

## 13.4 Ports (Port Numbers)

65,535 ports are available. Ports below 1024 (that is: 0-1023) are known ports and reserved for standard services. Ports below 1024 If a process wants to establish a TCP connection to a remote process, it connects on its own machine to an unused TCP port. The source port is called. The process also provides a target port to indicate the remote side of the packets. Every process that wants to connect to a host for the transfer of a file using FTP can, for example, connect to port 21 of the target host to contact their FTP daemon. All TCP connections include duplex and point-to-point connections. Full duplex means that both directions can be covered simultaneously. Point-to-point means that there are two 5 end points for each connection. Multicasting or broadcasting is not supported in TCP.

## 13.5 TCP Connection as a Byte Stream

A TCP connection is a byte stream and not a message stream. Message boundaries are not preserved end to end. For example, if the sending process does four 512-byte writes to a TCP stream, these data may be delivered to the receiving process as four 512-byte chunks, two 1024-byte chunks, one 2048-byte chunk or some other way. There is no way for the receiver to detect the unit(s) in which the data were written.

Four 512-byte segments sent as separate IP datagrams as shown in Figure 13.1. The 2048 bytes of data is delivered to the application in a single READ call.

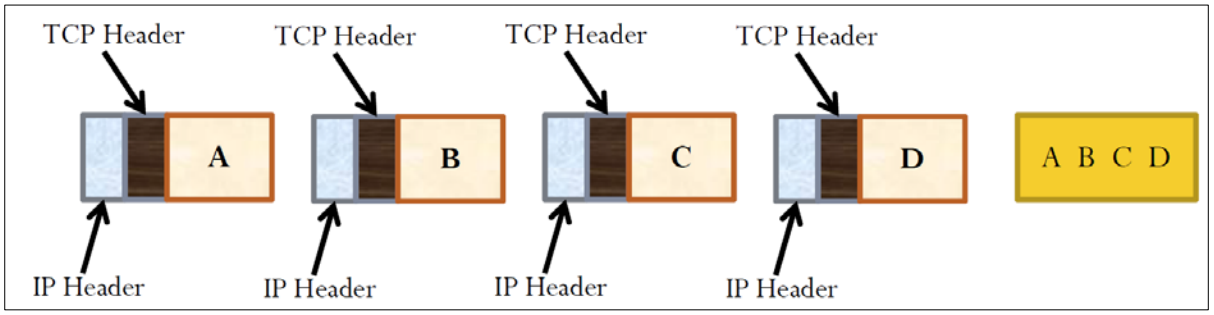



Figure 13.1 – TCP Headers

## 13.6 The TCP Service Model: Sockets and Ports

TCP service is obtained by both the sender and receiver creating end points, called sockets. Each socket has a socket number (address) consisting of:

- The IP address of the host and
- a 16-bit number local to that host, called a port.

For a TCP service to be obtained, a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine. The socket calls are listed in the table 10.1

| Port | Protocol | Use |
|---|---|---|
| 21 | FTP | File transfer |
| 23 | Telnet | Remote login |
| 25 | SMTP | E-mail |
| 69 | TFTP | Trivial file transfer protocol |
| 79 | Finger | Lookup information about a user |
| 80 | HTTP | World Wide Web |
| 110 | POP-3 | Remote e-mail access |
| 119 | NNTP | USENET news |

Table 10.1 – Sockets and Ports

A socket may be used for multiple connections at the same time. In other words, two or more connections may terminate at the same socket. Connections are identified by the socket identifiers at both ends, for e.g., (socket1, socket2). No virtual circuit numbers or other identifiers are used. How is a Socket Address formed? Consider Figure 13.2

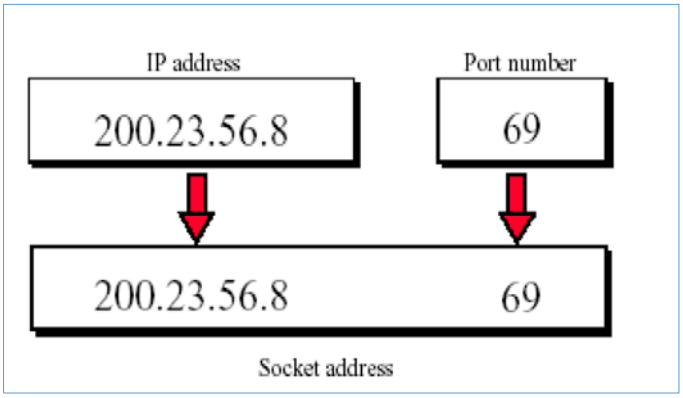



**Figure 13.2 - Socket**

## 13.7 Internet Connections

Clients and servers communicate by sending streams of bytes over connections. As pointed out, TCP connections (Figure 13.3) are point-to-point, full-duplex (2-way communication) and reliable. The layout s depicted in Figure 13.4

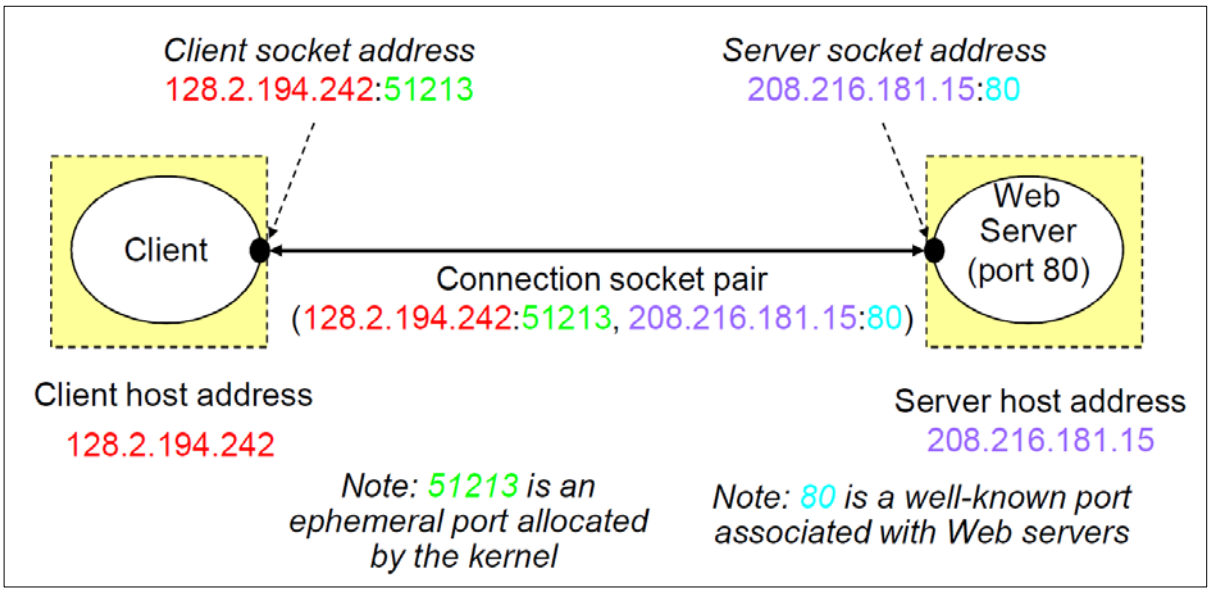



Figure 13.3 – TCP Connections

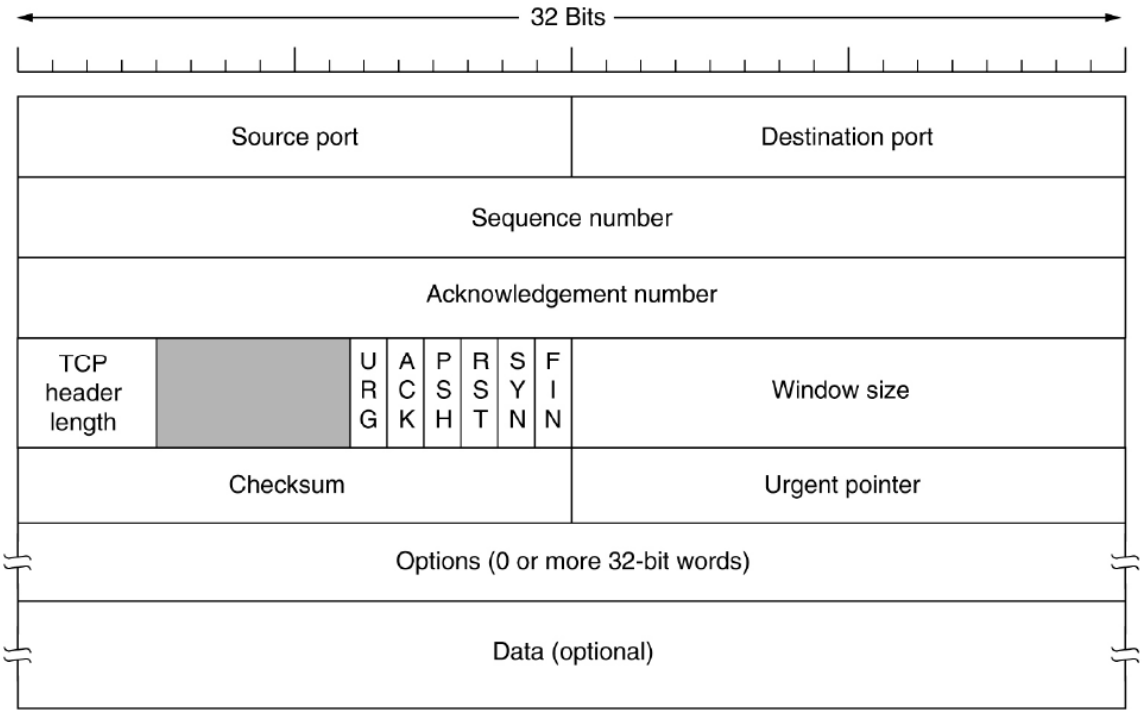



Figure 13.4 – TCP Segment Header

Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options. After the options, if any, up to 65,535 - 20 - 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages.

The fields Source Port and Destination Harbor identify the local connection endpoints. A 48-bit single end point is a port plus an IP address for its host. The connection is identified in the source and destination end points. The sequence and number fields accreditation perform their usual functions. Note that the number of acknowledgement specifies the next expected byte rather than the last byte received correctly. The length of the TCP header indicates how many 32-bit words the TCP header contains. The ACK bit is set to 1 so that the ACK number is valid. When ACK is 0, there is no recognition in this segment, so the field Recognition is ignored. The RST bit is used to reset a link that is confused because of a host accident or another. It also rejects or rejects attempts to open a connection in an invalid segment. To connect, the SYN bit is used. For a connection, the FIN bit is used. The sender no longer has to transmit data. A variable sliding window is used to control flow under TCP. The field of window size indicates the number of bytes to be sent from the byte.

The basics of a simple transport service are like a server application and a range of remote customers. The server first runs a primitive LISTEN, by calling a library procedure that will block the server by calling a system call before a client appears. If a client wants to communicate with the server, it runs a primitive CONNECT. This is done by the transport entity, which blocks the caller and sends the packet to the server. The message of the transportation layer for the server carrier is encapsulated in the payload of this packet. The CONNECT call of the client causes a CONNECTION REQUEST TPDU to be sent to the server. The transport entity checks when it arrives to see if a server on a LISTEN is blocked (i.e., is interested in handling requests). It then unblocks the server and returns to the client a CONNECTION ACCEPTED TPDU. The client is unblocked and the connection is established when this TPDU arrives. The SEND and RECEIVE primitive data can now be exchanged. Both parties can receive a (block) to expect the other party to make a SEND. SEND. The receiver is unblocked when the TPDU arrives. Then the TPDU can be processed and a response sent. This system works well as long as both sides are able to track whose turn it is to send.

## 13.8 TCP's Connection Establishment: 3-way handshake

This set-up protocol does not require either side to begin to send the same sequence number, so that it can be used for other than the global clock methods of synchronization. The normal configuration procedure is shown in host 1. Host 1 selects the number of the sequence (x) and sends a CONNECTION REQUESTTPDU to host 2. Host 2 answers with an ACK TPDU which recognizes x and announces a number of its own first series, y. Host 1 also acknowledges that the first TPDU-data host 2 has chosen an initial sequence number. In the presence of delayed duplicate control TPDUs, 3-way handshake works. This TPDU reaches host 2 without the knowledge of host 1. Host 2 reacts to this TPDU by sending host 1 with the ACK TPDU, asking that host 1 actually attempt to establish a new connection. When host 1 rejects a connection attempt from host 2, host 2 realizes that it has been tampered with a delayed double and leaves the connection. Thus there is no damage to a delayed duplicate. Figure 13.5 depicts all scenarios.
Together in the subnet there is a retarded CONNECTION REQUEST and an ACK. Host 2 receives and answers a delayed CONNECTION REQUEST. It is important to realize at this point that Host 2 has proposed the use of y for Host 2, as the initial sequence number, to host 1, knowing perfectly well that there are no TPDUs with sequence number y or y admissions. The fact that z has been recognized instead of telling host 2 that this too is an old duplicate, if the other late TPDU is host 2. The important thing is that there are no combinations of old TPDUs that can fail the protocol and have an accidentally established connection when it does not exist.

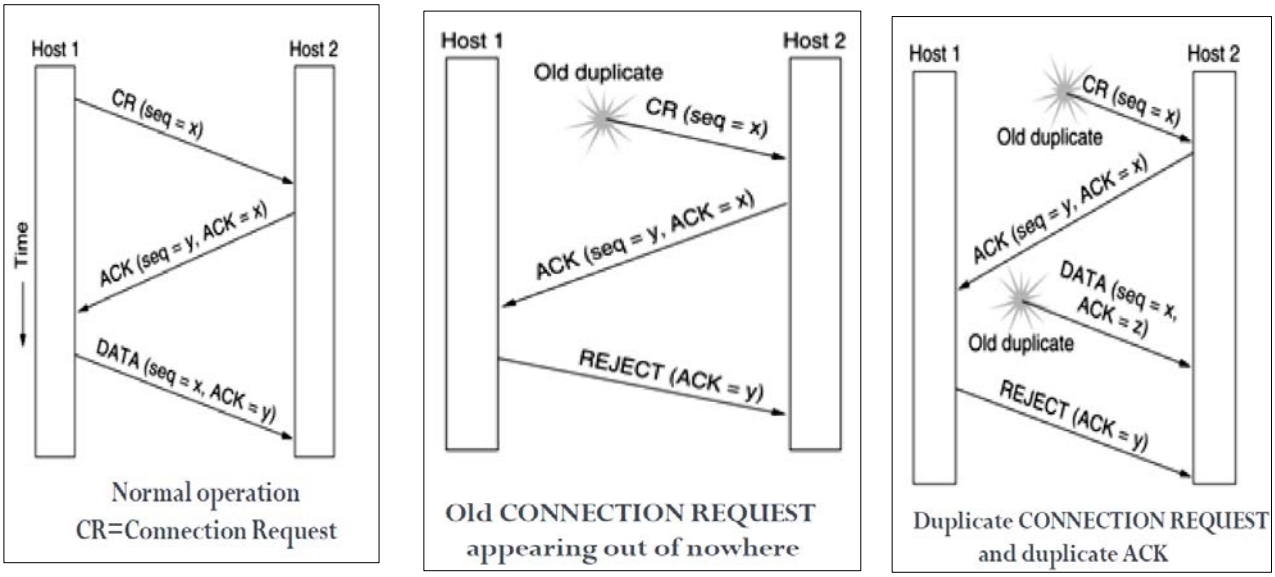



**Figure 13.5 - TCP's Connection Establishment: 3-way handshake**

## 13.9 TCP Connection Release

Two ways to end a connection: asymmetric release and symmetrical release in which the asymmetrical release is the way that the telephone system operates. Symmetric release considers the connection to be two separate one-way connections and requires that each one is separately released. Asymmetric releases are abrupt and can lead to loss of data. Host 1 sends a TPDU to host 2, once the connection is established. Host 1 then sends an additional TPDU. Sadly, before the second TPDU arrives, host 2 issues a DISCONNECT. This results in the release of the connection and the loss of data. Figure 13.6 shows this.

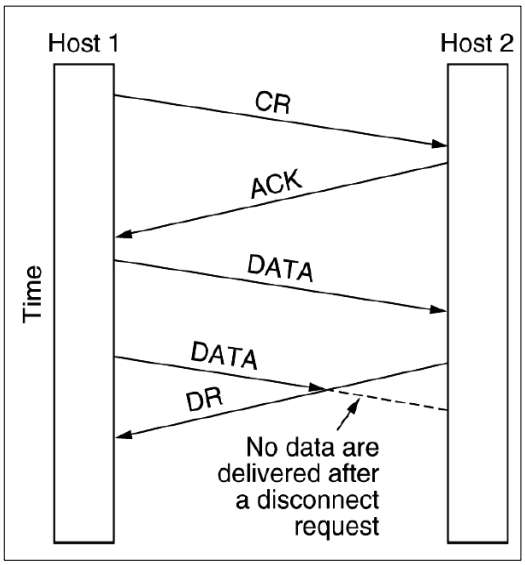



Figure 13.6 - Asymmetric release: abrupt disconnection with loss of data

The normal case in which one of the users sends a DR (DISCONNECTION REQUEST) TPDU to initiate the connection release. When it arrives, the recipient sends back a DR TPDU, too and starts a timer, just in case its DR is lost. When this DR arrives, the original sender sends back an ACK TPDU and releases the connection. Finally, when the ACK TPDU arrives, the receiver also releases the connection. Releasing a connection means that the transport entity removes the information about the connection from its table of currently open connections and signals the connection's owner (the transport user). Figure 13.6 depicts the scenario.

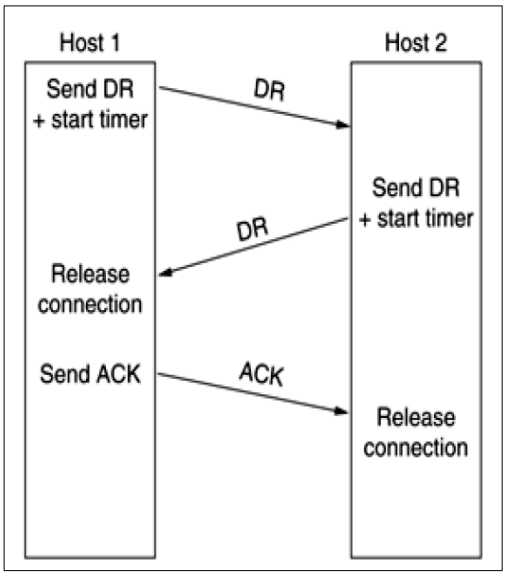



Figure 13.7 - **Connection release: Normal case of a three-way handshake**

## 13.10 TCP Transmission Policy: WINDOW

Two ways to end a connection: asymmetric release and symmetrical release in which the asymmetrical release is the way that the telephone system operates. Symmetric release considers the connection to be two separate one-way connections and requires that each one is separately released. Asymmetric releases are abrupt and can lead to loss of data. Host 1 sends a TPDU to host 2, once the connection is established. Host 1 then sends an additional TPDU. Sadly, before the second TPDU arrives, host 2 issues a DISCONNECT. This results in the release of the connection and the loss of data. Figure 13.6 shows this. The sender cannot send segments, with two exceptions, normally when the window is 0. The first thing to do is to send urgent data, for instance, to allow the operator to kill the remote process. Secondly, the transmitter can send a 1-byte section to re-annunciate the next expected byte and window size. This option, if a window advert is ever lost, is explicitly provided by the TCP standard.

## 13.11 Degradation of TCP's Performance: The Silly Window Syndrome

The problem with Silly Window Syndrome occurs when information is transferred to the transmitting TCP entity in large blocks, but an interactive application reads data 1 byte at a time on the receiving side. At first, the reception side TCP buffer is complete and the sender knows that (i.e., has a window of size 0). Then a character from the TCP stream is read by the interactive application. This action makes the receiver TCP, so it sends the sender a window update saying 1 byte is OK. The transmitter shall send and obligate 1 byte. The buffer is now complete so that the recipient recognizes the 1-byte segment but sets the window to 0. This conduct can continue forever. Figure 13.7 depicts this scenario.

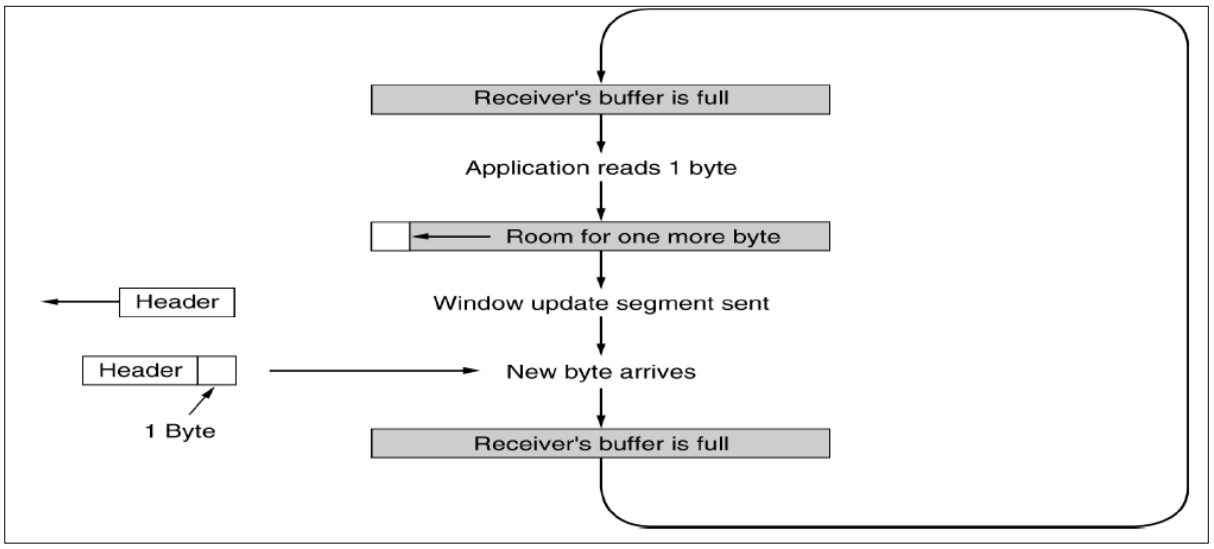



**Figure 13.7 – Silly window syndrome**

## 13.12 TCP Congestion Control

When there is more load than it can handle for any network, congestion increases. No exception is the Internet. Although the network layer also attempts to manage congestion, TCP does most of the heavy lifting because a real way to reduce the sender data rate is to reduce the congestion layer. In theory the use of a principle borrowed from physics can address congestion: the law on the preservation of packets: The idea is not to inject a new packet into the network until an old packet leaves (i.e., a packet sent before is delivered). By dynamically manipulating the window size, TCP is trying to achieve this goal. Two potential problems exist on the Internet - network capacity and receiver capacity. Each has to be dealt with each of them separately.

Each sender holds two windows for this purpose: the receiver's window and the congestion window, the second. Each of the bytes that the sender can transmit is a reflection. The minimum number of bytes to be sent is two windows. The effective window is therefore the minimum that the transmitter believes to be OK and the recipient believes to be OK. Example: if the recipient says "Send eight KB" but the recipient is aware of the network congested by bursts of more than four KB, it sends out four KB. If, instead, the sender knows, that bursts of up to 32 kB are completed effortlessly and the recipient says "send 8 kb',' 23 it sends the complete 8 kb requested.

## 13.13 The Internet Transport Protocol: UDP

In the transport layer, the internet has two main protocols: a connected Protocol and a connection-oriented Protocol. The UDP protocol is connected. The protocol that connects is TCP. Basically, UDP is only an IP with a short header. UDP offers applications the opportunity to send and send encapsulated IP datagrams without a connection. UDP sends segments consisting of an 8-byte header and the payload. Figure 13.8 displays the header.

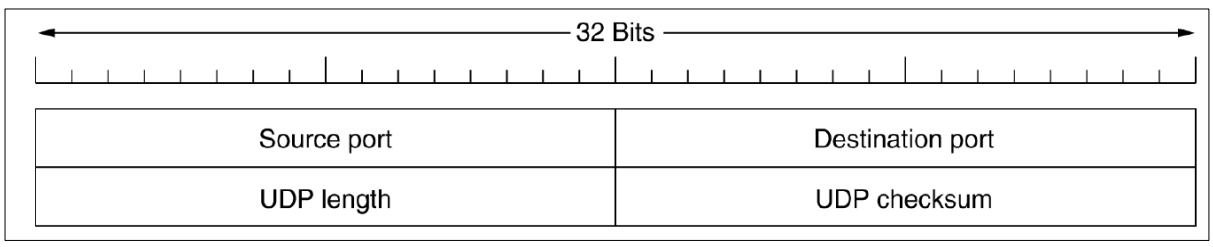



**Figure 13.8 – UDP header**

Both ports identify the final points on the source and destination machines. When a UDP packet arrives, its payload is transferred to the destination port process. In fact, adding sources and destination ports is the main value of UDP when you just use raw IP. The transport layer wouldn't know what to do with the packet without the port fields. It delivers segments properly with them! When a reply must be returned to the source, mainly the source port is needed. The sending process of the answer can specify on the sending machine, by copying the source port field from the incoming segment to the final port area of the outgoing segment. The 8-byte header and data are provided in the UDP length field. Optional is the UDP checksum and saved as 0 un calculated (a true computed 0 is stored as all 1s). It's stupid if the quality of the data isn't important (e.g., digitized speech).

UDP does NOT: flow control, error check or transfer when a bad segment is received. These can be handled by user processes. UDP does: provide an IP protocol interface with the additional feature to DE multiplex multiple ports processes. UDP deployment: In client-server applications, it is particularly useful. The client often sends a brief request and awaits a quick answer back to the server. If either the request or the answer is lost, the customer can just try again. The code is not only simple, but fewer messages (one in each direction) than a protocol that needs to be initialized are required (like TCP).

## 13.14 Wireless TCP and UDP

Theoretically, transport protocols should be separate from the underlying network layer's technology. TCP should not in particular bother if IP is running on fiber, UTP, 10Base2 or using radio waves. In practice, it is important because most of the TCP implementations have been carefully optimized on the basis of hypotheses that apply to wireless networks but fail to do so. Ignoring the characteristics of Wi-Fi can lead to the logically correct but terrible TCP implementation. The main problem: is the algorithm for congestion control. Almost every TCP implementation nowadays assumes that delays are caused by congestion and not lost packages. As a result, TCP slows and sends less vigorously (for example, the slow start algorithm of Jacobson, if a timer is removed). The idea is to reduce the network load and thereby reduce the congestion. Wireless transmission connections are highly unreliable – packets are constantly lost. The right way to deal with lost packets is to send them as quickly as possible. It just makes things worse by slowing down. If a sender is sending 100 packets/sec when 20% of all packets are lost, then the throughput amounts to 80 packets/sec. If the sender slows to 50 packets per second, the transmission will decrease to 40.

The sender should slow down if a packet is lost in a cabled network. The sender should try again if someone is lost on a wireless network (and harder). It is difficult to take the right decision if the sender doesn't know what the network is (as in a wireless network). The track is often heterogeneous from sender to recipient. Although a wired network may be the first 1000 km, the last 1 km may be wireless. It is now even harder to decide the correct timeout because where the problem has arisen it matters. As shown in Figure 13.9, a solution is to divide the TCP connection into two separate connections. The first connection is to the base station from the sender.

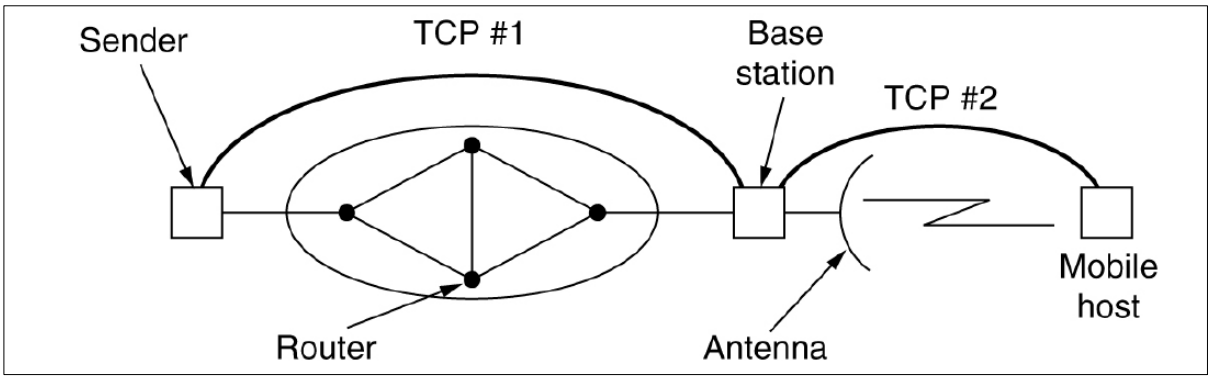



**Figure 13.9 –Wireless UDP & TCP**

This scheme has the advantage of being homogeneous in both connections. Wired connection times can decelerate the sender, while wireless connection timeouts can accelerate the sender. The downside of the scheme: it breaches TCP's semantics. Since each part of the connection has a complete TCP connection, the base station usually recognizes every TCP segment. It is only now that the sender is receiving an acknowledging that the receiver has received the segment but the base station has received it.

## 13.15 Summary

The chapter described the transport code runs entirely on the users' machines, but the network layer mostly runs on the routers, which are operated by the carrier (for e.g., in a WAN). What happens if the network layer offers inadequate service? Suppose that it frequently loses packets? What happens if routers crash from time to time or the link is down? If, in a connection-oriented subnet, a transport entity is informed halfway through a long transmission that its network connection has been abruptly terminated, with no indication of what has happened to the data currently in transit, it establishes a new network connection to the remote transport entity. Using this new network connection, it can send a query to its peer asking which data arrived and which did not and then pick up from where it left off.

## 13.16 Additional Reading


- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *Olivier Bonaventure, "Computer Networking : Principles, Protocols and Practice* Release 0.25," Open Educational Resource (OER) - Unsyiah Library, accessed January 27, 2021, http://uilis.unsyiah.ac.id/oer/items/show/2621.
- *"Computer Networking, 7th Edition"*. Jim Kurose, W. Ross
- *"Computer Networks, A system approach 4th Edition"*. Larry, Peterson Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Networks, 5th Edition"*. Tanenbaum, Wetherall Publisher : Pearson ISBN: 978-0-13-212695-3.
- *"Computer Science, 2nd Edition"*. Langfield, Duddell Publisher : Cambridge International.
- *"Principles of Communication Networks, 6th Edition"*. Zorsi,
- *"Principles of Networks and System Administration, 6th Edition"*. Burgess,
- *"Computer Science, 3rd Edition"*. Watson, Williams Publisher : Cambridge International.
- Computer Networks by Tanenbaum, latest edition
- Data Communication, Computer Networks and Open Systems by Halsall
- Local Networks, An Introduction by William Stallings

## 13.17 Activities

- Describe the different concepts in the transport layer,
- Differentiate between UDP and TCP,
- What are ports?
- Explain the TCP Service Model using Sockets and Ports
- Elaborate on the Primitives for a Simple Transport Service
- Using diagram explain the TCP's Connection Establishment: 3-way handshake