./

Learning Report – Networking



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be approved By** | **Remarks/Revision Details** |
| 1 |  | Name/PS No | Name/PS No | Module Owner Name | Comments |
| 2 | 15/02/21 |  |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Document History**

1. **NETWORKING CONCEPTS**
   * + *Network types - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 5*
     + *Network Topologies- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 9*
     + *Wired Networks- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 14
     + *Wireless Networks- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 15
     + *Queuing- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 16*
     + *Network Scheduling- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -- - - - -* 18
2. **NETWORK SECURITY**
   * + *Stack Overflow and Heap Overflow- - - - - - - - - - - - - - - - - - - - - - - - - - -* 20
     + *Cryptography- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 22
     + *Encryption- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 23*
     + *SSH, TLS and MTLS- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 24
3. **COMPONENTS**
   * + *Hub- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 25*
     + *Switches- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 25
     + *Routers- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 26
     + *Repeaters- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 26
     + *Bridge- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 27
     + *Gateways- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 27
     + *Access Points- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -28*
4. **PROTOCOLS**
   * + *OSI Layers- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -- - - - - -* 28
     + *TCP Header Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 36*
     + *UDP Header Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 38
     + *IP Header Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 39
     + *L2 Protocols- - - - - - - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - - - - - - - - -39*
     + *L3 Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*41
     + *WLAN Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 42
     + *BGP Protocols- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -44*
5. **IP ADDRESS**
   * + *IPV4 Address- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 45
     + *IPV6 Address- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 46
     + *IPV4 Subnetting- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -* 48
6. **NETWORK TOOLS**
   * + *Packet Tracer- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 52*
     + *Wireshark- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 49*

**Network:**

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

**Type of Networks:**

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.

* **Personal Area Network** (**PAN**)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

****

* **Local Area Network(LAN)**

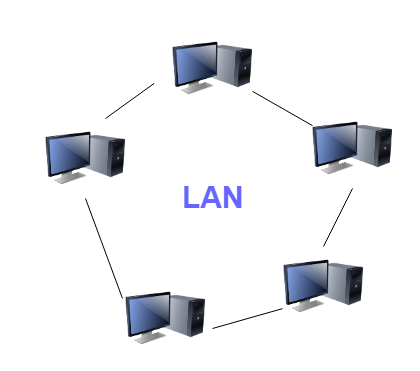
Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) their size,

(2) their transmission technology,

(3) their topology.

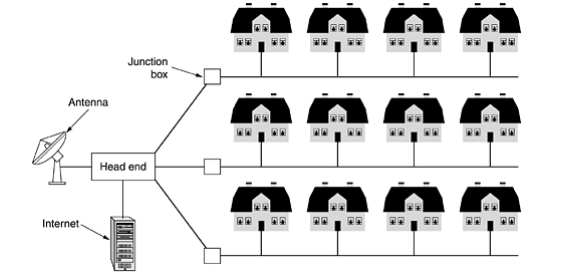
LANs are restricted in size.



* **Metropolitan Area Networks(MAN)**

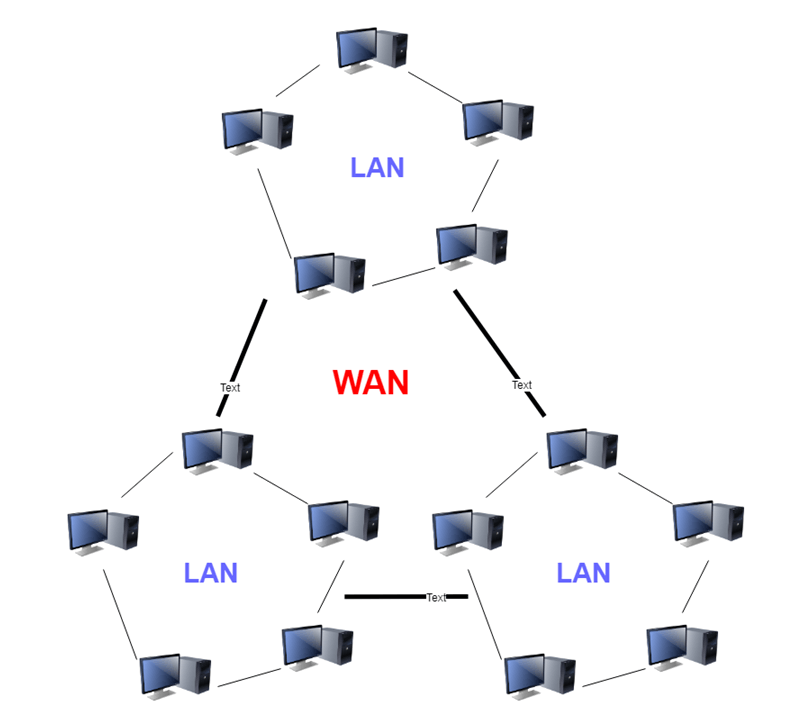
A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

* A metropolitan area network based on cable TV

****

* **Wide Area Networks**:

1. A wide area network, or WAN, spans a large geographical area, often a country or continent.
2. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
3. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.
4. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.



## **Network Topologies:**

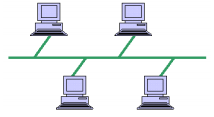
* Topology - Physical and logical network layout
* Physical: actual layout of the computer cables and other network devices
* Logical: the way in which the network appears to the devices that use it.

**Common topologies:**

* Bus, ring, star, mesh and wireless

**Bus topology:**

* Uses a trunk or backbone to which all the computers on the network connect
* Systems connect to this backbone using T connectors or taps
* Coaxial cablings (10Base-2, 10Base5) were popular options years ago.

. 

**Advantages:**

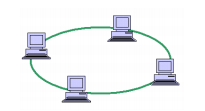
* Cheap and easy to implement
* Require less cable
* Does not use any specialized network equipment.

**Disadvantages:**

* Network disruption when computers are added or removed
* A break in the cable will prevent all systems from accessing the network.
* Difficult to troubleshoot

**Ring Topology:**

* Meaning that data travels in circular fashion from one computer to another on the network.
* Typically FDDI, SONET or Token Ring technology are used to implement a ring network.
* Ring networks are most commonly wired in a star configuration.
* Token Ring has multi-station access unit (MSAU), equivalent to hub or switch. MSAU performs the token circulation internally.

****

**Advantages:**

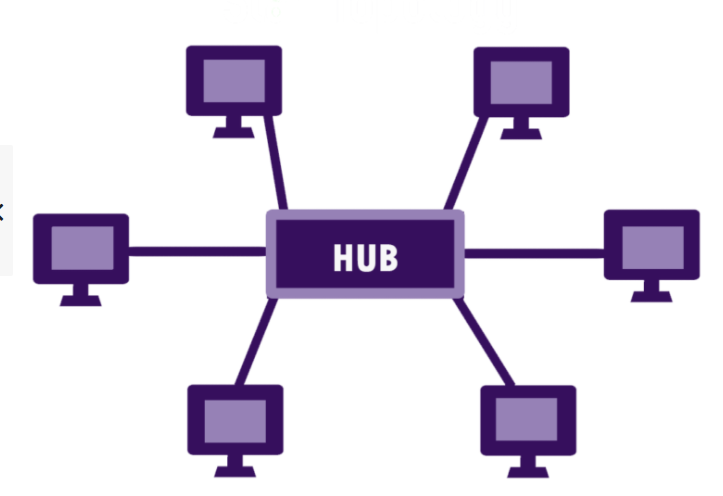
* Cable faults are easily located, making troubleshooting easier.
* Ring networks are moderately easy to install.

**Disadvantages:**

* Expansion to the network can cause network disruption.
* A single break in the cable can disrupt the entire network.

# Star Topology:

* All computers/devices connect to a central device called hub or switch.
* Each device requires a single cable.
* point-to-point connection between the device and hub.
* Most widely implemented.
* Hub is the single point of failure.

****

**Advantages:**

* Easily expanded without disruption to the network.
* Cable failure affects only a single user.
* Easy to troubleshoot and isolate problems.

**Disadvantages:**

* Requires more cable.
* A central connecting device allows for a single point of failure.
* More difficult to implement.

**Mesh Topology:**

* Each computer connects to every other.
* High level of redundancy
* Rarely used.

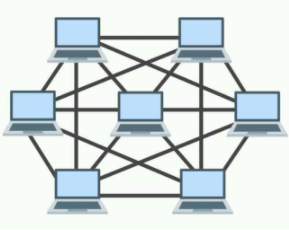
– Wiring is very complicated

– Cabling cost is high

– Troubleshooting a failed cable is tricky

– A variation hybrid mesh

– create point to point connection between specific network devices, often seen in WAN implementation.

****

**Advantages:**

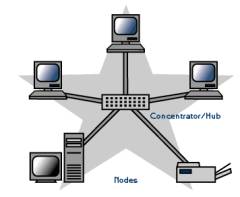
* Provides redundant paths between devices.
* The network can be expanded without disruption to current uses.

**Disadvantages:**

* Requires more cable than the other LAN topologies.
* Complicated implementation.

**Wired Networks:**

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second to 100Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today.



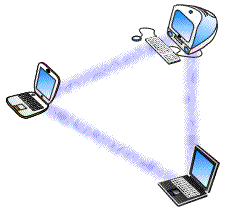
Some of the Ethernet standards are:

* 802.3 – It is a 10BASE5 thick coax, which has data rate of 10Mbps and operates on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) process
* 802.3a – It is a 10BASE2 thin coax, which has data rate of 10Mbps.
* 802.3i – It is a 10BASET twisted pair cable, which has data rate of 10Mbps.
* 802.3j - 10Base-F (fiber optic)
* 802.3u – It is a 100BASET twisted pair cable, which has data rate of 100Mbps.
* 802.3x - Full duplex
* 802.3ae - 10-Gigabit Ethernet
* 802.3ba - 40Gbps & 100Gbps Ethernet

**Wireless Networks**

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.



**Some wireless networking standards are:**

* 802.11a - 802.11a applies to wireless local area networks and supports a maximum a maximum connect rate of 54Mbps throughput in the 5GHz band.
* 802.11b - 802.11b applies to wireless local area networks and supports a maximum connect rate of 11Mbps with fallback to 5.5, 2, and 1Mbps in the 2.4GHz ISM band
* 802.11n- This standard works on both the 2.4 GHZ and 5 GHZ bands, its net data ranges from 54Mbits/s to 600Mbits/s.

### Queuing, Scheduling:

**Queuing:**

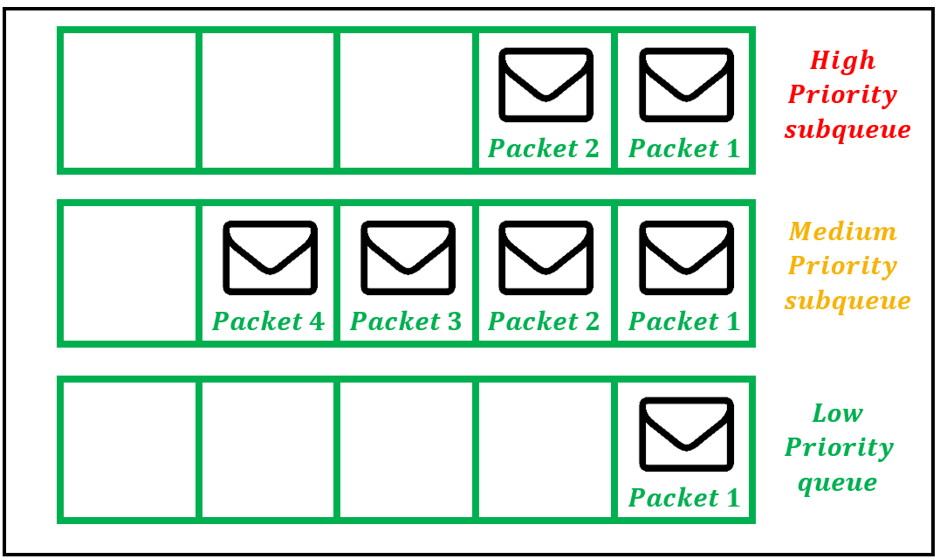
Regardless of how simple or how sophisticated the rest of the resource allocation mechanism is, each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted. The queuing algorithm can be thought of as allocating both bandwidth (which packets get transmitted) and buffer space (which packets get discarded). It also directly affects the latency experienced by a packet by determining how long a packet waits to be transmitted. This section introduces two common queuing algorithms first-in, first-out (FIFO) and fair queuing (FQ)—and identifies several variations that have been proposed.

**FIFO:**

Regardless of how simple or how sophisticated the rest of the resource allocation mechanism is, each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted. The queuing algorithm can be thought of as allocating both bandwidth (which packets get transmitted) and buffer space (which packets get discarded). It also directly affects the latency experienced by a packet by determining how long a packet waits to be transmitted. This section introduces two common queuing algorithms—first-in, first-out (FIFO) and fair queuing (FQ)—and identifies several variations that have been proposed.

**Priority Queuing(PQ):**

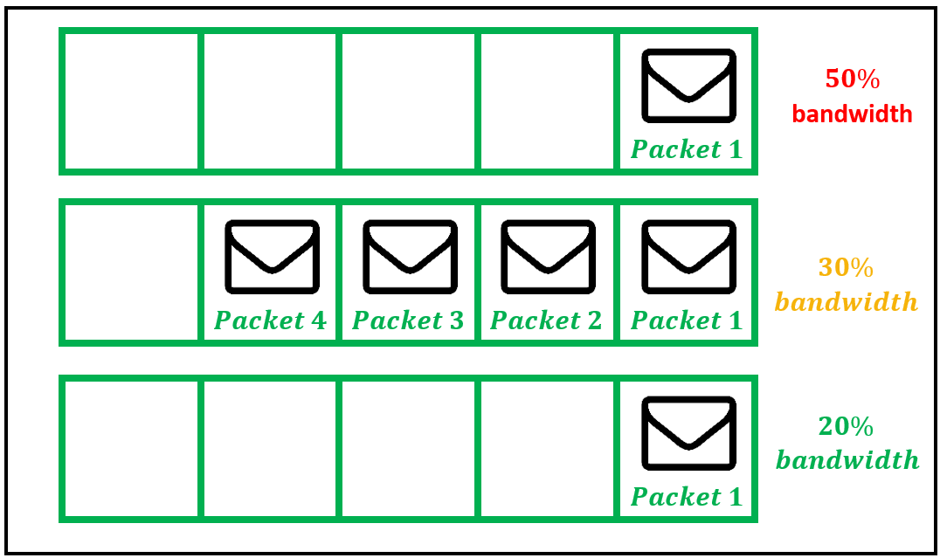
In Priority Queuing, instead of using a single queue, the router bifurcates the memory into multiple queues, based on some measure of priority. After this, each queue is handled in a FIFO manner while cycling through the queues one by one. The queues are marked as High, Medium or Low based on priority. Packets from the High queue are always processed before packets from the Medium queue. Likewise, packets from the Medium queue are always processed before packets in the Normal queue, etc. As long as some packets exist in the High priority queue, no other queue’s packets are processed. Thus, high priority packets cut to the front of the line and get serviced first. Once a higher priority queue is emptied, *only then* is a lower priority queue serviced.



**Weighted Fair Queuing(WFQ):**

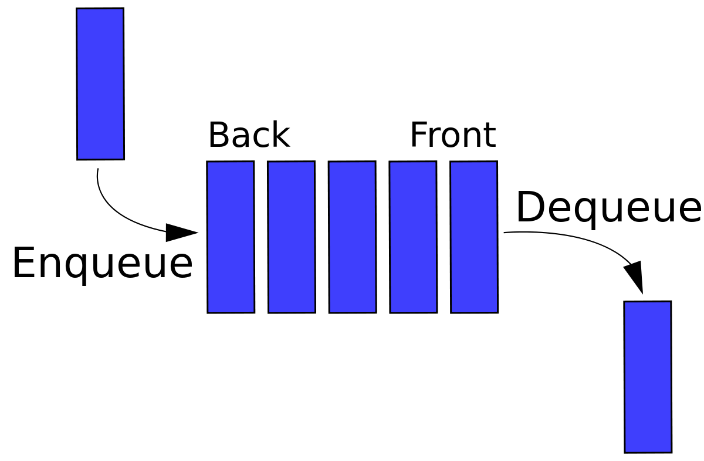
Weighted Fair Queuing (WFQ) dynamically creates queues based on traffic flows and assigns bandwidth to these flows based on priority. The sub-queues are assigned bandwidths dynamically. Suppose 3 queues exist which have bandwidth percentages of 20%, 30%, and 50% when they are all active. Then, if the 20% queue is idle, the freed-up bandwidth is allocated among the remaining queues, while preserving the original bandwidth ratios. Thus,

the 30% queue is now allotted (75/2) % and the 50% queue is now allotted (125/2) % bandwidth.



**Scheduling:**

In computing, **s**cheduling is the method by which work is assigned to resources that complete the work. The work may be virtual computation elements such as threads, processes or data flows, which are in turn scheduled onto hardware resources such as processors, network links or expansion cards



**NETWORK SECURITY**

How do we keep them from impersonating us, or from listening in to our conversations or downloading our data? Computer security problems are in the news on almost a daily basis. In this chapter and the next we take a look at just a few of the issues involved in building secure networks.

For our limited overview here, we will divide attacks into three categories:

1. Attacks that execute the intruder’s code on the target computer

2. Attacks that extract data from the target, without code injection

3.Eavesdropping on or interfering with computer-to-computer communication.

More technical forms of attack may involve a virus, a buffer overflow Stack Buffer Overflow and Heap Buffer Overflow, some other software flaw The Morris Worm.

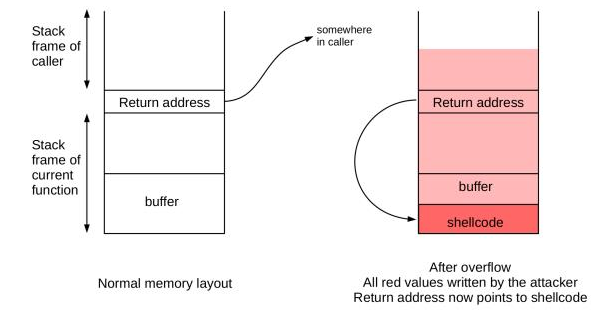
**stack overflow**

The stack buffer overflow is perhaps the classic way for an attacker to execute a short piece of machine code on a remote machine, thus compromising it. Such attacks are always due to an implementation flaw. A server application reads attacker-supplied data into a buffer, buf, of length buflen. Due to the flaw, however, the server reads more than buflen bytes of data, and the additional data is written into memory past the end of buf, corrupting memory. In the C language, there is no bounds checking with native arrays, and so such an overflow is not detected at the time it occurs.

A common goal for the attacker is to supply an overflowing buffer that does two things:

1. It includes a shellcode - a small snippet of machine code that, when executed, does something bad (traditionally but not necessarily by starting a shell with which the attacker can invoke arbitrary commands).

2. It overwrites the stack return address so that, when the current function exits, control is returned not to the caller but to the supplied shellcode.



**Heap Overflow**

As with stack overflows, heap overflows all rely on some software flaw that allows data to be written beyond the confines of the designated buffer. A buffer on the heap is subject to the same software-failure overflow prospects as a buffer on the stack. An important difference, however, is that buffers on the heap are not in clear proximity to an obvious return address. Despite that difference, heap overflows can also be used to enable remote-code-execution attacks.

Perhaps the simplest heap overflow is to take advantage of the fact that some heap pages contain executable code, If the page with the overflowable buffer is pointed to by p, and the following page in memory pointed to by q contains code, then all an attacker must do is to have the overflow fill the q page and a shellcode. When at some point a call is made to the code pointed to by q, the shellcode is executed instead. A drawback to this attack is that the layout of heap pages.

**Cryptography**

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it.

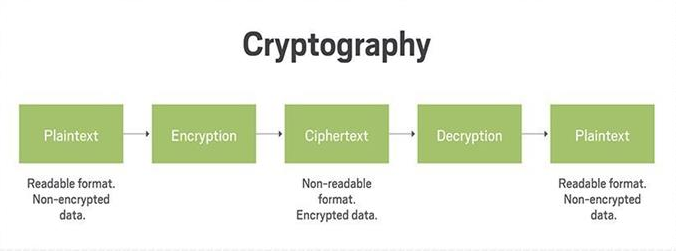
"crypt-" means "hidden" or "vault" -- and the suffix " - graphy " stands for "writing."

To protect packet contents. Different techniques address different issues; three classic goals are the following:

1. Message confidentiality: eavesdroppers should not be able to read the contents.

2. Message integrity: the recipient should be able to verify that the message was received correctly, even in the face of a determined adversary along the way.

3. Sender authentication: the recipient should be able to verify the identity of the sender



**Encryption:**

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

The process of encrypting and decrypting messages involves keys. The two main types of keys in cryptographic systems are symmetric-key and public-key (also known as asymmetric-key).

**Types:**

**Symmetric key**

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication. The German Enigma Machine utilized a new symmetric-key each day for encoding and decoding messages.

**Public key**

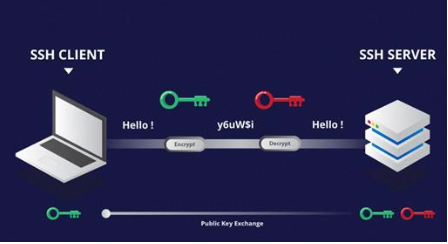
Illustration of how encryption is used within server Public key encryption.

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read. Public-key encryption was first described in a secret document in 1973, beforehand, all encryption schemes were symmetric-key (also called private-key).

​

**SSH**

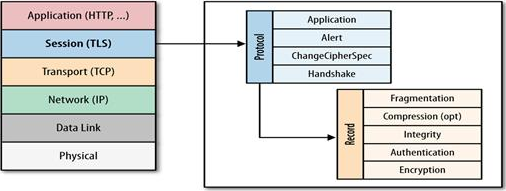
SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.



​

**TLS**

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security



​

**MTLS**

Mutual authentication is a desired characteristic in verification schemes that transmit sensitive data, to ensure data security. Mutual authentication can be accomplished with two types of credentials: usernames and passwords, and public key certificates.

**COMPONENTS OF NETWORK**

**Repeater:**

• A repeater operates at the physical layer.

• The job is to regenerate the signal over the same network before the signal becomes too weak

or corrupted to extend the length to which the signal can be transmitted over the same

network.

• These repeaters do not amplify the signal. When the signal becomes weak, they copy the

signal bit by bit and regenerate it at the original strength. It is a 2 port device.

**Hub:**

• Hub is a very simple network connecting device.

• It is also known as a Multiport Repeater Device.

• A Hub is a layer-1 device and operates only in the physical network of the OSI Model.

There are mainly two types of Hub, they are:

1. **Active Hub:** An Active hub is also known as Concentrator. It requires a power supply and

can work as a repeater.

2. **Passive Hub**: A passive hub does not need any power supply to operate. It only provides

communication between the networking devices and does not amplify the transmission

signals.

3. **Intelligent Hub:** It works like active hubs and include remote management capabilities. They

also provide flexible data rates to network devices.

**Bridge**:

• A bridge operates at data link layer.

• A bridge is a repeater; with add on the functionality of filtering content by reading the MAC

addresses of source and destination.

• It is also used for interconnecting two LANs working on the same protocol.

• There are two types of bridges as follows:

**Switch:**

• A switch is a multiport bridge with a buffer and a design that can boost its efficiency (many ports imply less traffic) and performance.

• A switch is a data link layer device.

• The switch can perform error checking before forwarding data, that makes it very efficient as it

does not forward packets that have errors and forward good packets selectively to correct port

Only

**Gateway:**

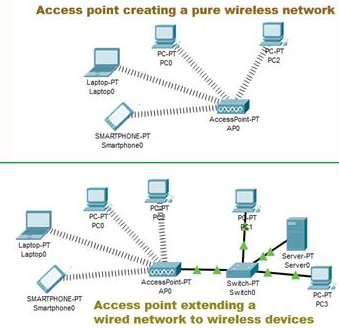
• A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.

• They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

• Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router

**Access Point:**

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. For example, if you want to enable Wi-Fi access in your company's reception area but don’t have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room



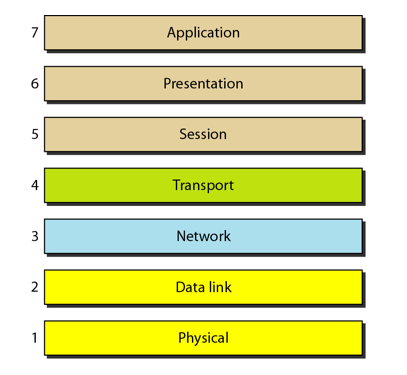
**OSI**

**Open System Interconnection:**

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Introduction:

OSI (Open Systems Interconnection) is used to understand how data is transfer from one device to another. It has 7 layers. It is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other.

****

* Application, Presentation, Session layer are the software layers
* Transport Layer is the heart of the OSI layer
* Network, Datalink, Physical layers are the hardware layers

Layer 7: The Application Layer:  
  
The top layer of an OSI model (layer seven) is the application layer that delivers network services or protocols that comply with an end-user’s data to the end-user. It provides protocols that allow software to send and receive information and present meaningful data to users.  
  
Examples of Layer 7 applications include web browsers such as Google Chrome or Firefox, as well as apps such as Office, Outlook, and Skype. The services provided by each of these applications permit the application layer to supply and receive data from the Presentation layer.  
  
A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).  
  
**Layer 6: Presentation layer:**  
  
Presentation layer get the data from the Application layer. The data is in the form of numbers and characters. Presentation layer convert that characters and numbers to machine understandable binary format

* Example conversion of ASCII to EBCDIC (Extended Binary Coded Decimal Interchange Code)
* This process is known as translation. Before the data is transmitted to the presentation layer reduces the number of bits that are used to represent the original data.
* This bit reduction process is called data compression and it can be Lossy or Lossless.
* To maintain the integrity of data, before transmission data is encrypted at the sender side and data is decrypted at the receiver side.
* Here SSL (Secure Sockets Layer) protocol is used for encrypting and decrypting the data.
* Some of the protocols used in presentation layer are SSH, IMAP, MPEG, JPEG

**Layer 5: Session Layer:**

Session layer helps in setting up and managing connections enabling sending and receiving of data followed by termination of connections or sessions

* Session layer has its helpers called APIs (Application Programming interfaces)
* NETBIOS (Network Basic Input Output System) is an example of APIs which allows applications of different computers to communicate with each other. Just before a session or connection is established with the server.
* Server perform a function called authentication. It is a process of verifying who you are.
* For this server uses a username and password. Once the username and password are matched the session or a connection is established between your computer and the server
* After the authentication session layer check for authorization
* This process is determined if you have permission to access a file. If not you will get a message saying you are not authorized to access this page.
* These are the two functions authentication and authorization are performed by the session layer

**Layer 4: Transport Layer:**

Transport layer controls the reliability of communication through Segmentation, Flow control, Error control.

* + Segmentation:
    - In segmentation, the data received from the session layer is divided into small data units called as segments.
    - Each segment contains a source and destination port number and a sequence number.
    - Port number help to direct each segment to the correct application
    - Sequence number helps to reassemble the segments in correct order to form correct message at the receiver.
  + Flow Control:
    - In flow control the transport layer controls the amount of data being transmitted.
    - For example, a mobile is connected to a server, Here server can transmit data maximum at 100Mbps and our mobile can process data maximum at 10Mbps. Now we are downloading the file from the server. Server start sending the file at 50Mbps which is greater than the rate our mobile can process.
    - So, the mobile phone tells the transmission layer to slow down the data transmission rate up to 10Mbps so that no data can get lost. Like this wise versa.
* Error Control:
* Transport layer also help in error control, if some data does not arrive the destination. Transport layer uses automatic repeat request scheme to retransmit the lost or corrupted data.
* A group of bits called checksum is added to each segment by the transport layer to find out the received corrupted segment
* Protocols for transport layer:
* Transmission Control protocol (TCP)

1. TCP is the connection oriented transmission
2. It provided feedback that data delivered or not.
3. Lost data can be recovered in TCP

* User Datagram Protocol (UDP)

1. UDP is the connectionless transmission it is faster than the
2. It doesn’t provide any feedback where it delivered data or not
3. Lost data can’t be recovered

**LAYER 3: Network Layer:**

1. Network layer work for the transmission of the received data segment from one computer to the another located in different networks.
2. Data units in network layer are called packets. It is the layer where routers to decide the function of network layer are logical addressing, routing and path determination.
3. IP addressing (IPv4, IPv6) done in network layer is called logical addressing.
4. Every computer in a network has a unique IP addressing
5. IP address is assigned to each data packet to ensure that data can reach the correct destination.
6. Routing is a method of moving the data packets from source to destination and it is based on the logical address format of IPv4 or IPv6.
7. Based on IP address and Mask routing decisions are made in a computer.

* Path Determination

A computer can be connected to internet server for a computer in many ways. Choosing the best delivery path for the data delivery from source to destination.

* Protocols used
* OSPF (Open Shortest path first border)
* BGP (Boarder Gateway protocol)
* IS-IS (Intermediate System to Intermediate)

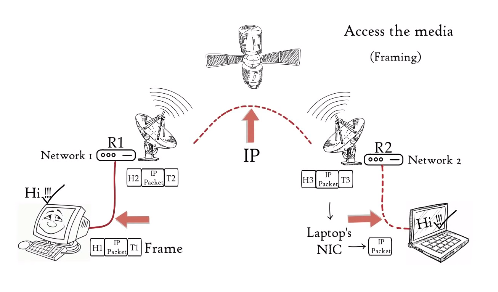
These are the protocols to determine the best path for data delivery.

**Layer 2: Data Link Layer:**

1. Data link layer receives data from the Network layer. data packets contain IP address of sender and receiver
2. There are 2 types of addressing

* Logical addressing: It is done at network layer where the segment is assigned with the sender and receiver IP address to form a data packet.
* Physical addressing: It is done at the data link layer where the data packets are assigned with the MAC address of sender and receiver and form a frame.
* Data unit in Data link layer is called frame

1. Example if we want to transfer the data from computer to the laptop here computer is connected to the router through an ethernet cable and laptop connects with the wireless network.
2. Data link layer add some data as head and tail to an IP packet form it as a frame and passes through the ethernet cable. The router de capsulate as a packet and encapsulate as a frame
3. At the other end router, de capsulate as a packet and encapsulate again as a frame.
4. The laptop receives this wireless data link frame de capsulate it and then forward IP packet to network layer.
5. Finally arrives application layer. Application layer protocol make the received data and visible on the computer screen.
6. Network layer and higher-level layers can transfer data over media with the help of Data link layer.
7. That is data link layer provides access to media for higher layer of OSI model

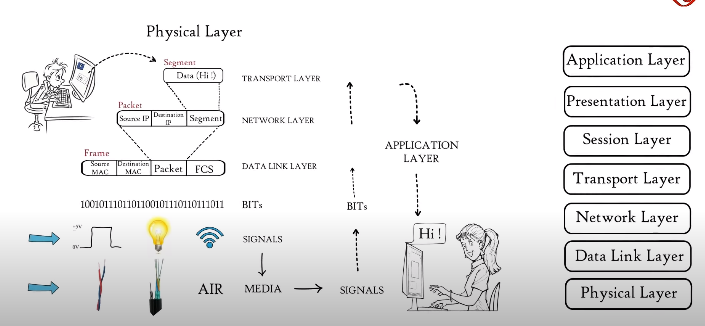
****

**Layer 1: Physical Layer:**

Physical layer converts the binary digits into signal and transmit over the local media.

1. It can be the electric signal in case of copper cable or LAN cable.
2. Light signal in case of optical fiber.
3. Radio signal in case of air

* At the receiver signal convert it to bits and pass it to data link layer as a frame. Frames is further de capsulate as the data move to higher layers finally data is moved to application layer.
* Application layer protocol makes the senders message visible in the application in the receiver’s computers screen.
* In this way, the OSI model is helping to transfer data between distant hosts.

****

#### TCP:

* The most common protocol used in the transport layer is TCP (Transmission Control Protocol). This is a connection oriented protocol. TCP offers reliable, peer-acknowledged, ordered, session-based connectivity between two hosts.
* All the features mentioned above are provided by the TCP layer itself. This means, that it may operate with other, unreliable, protocols in the lower layers and that this shouldn't affect the communication from the application layer perspective.

##### TCP Reliability:

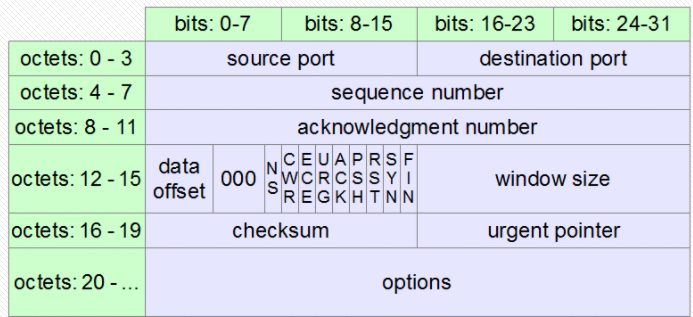
* During sending data, TCP assures that data has been provided to the recipient.
* The receiver checks if the received packet was intact during transmission (by checking the checksum of the data) and, if so, the receiver confirms it by sending an acknowledgement to the sender.
* If the sender doesn't receive the acknowledgement for a message within some period, it will resend the lost packet.
* After several unsuccessful attempts, TCP assumes that the receiver is unreachable and informs the application layer that the transmission has failed.

##### TCP Ordering:

* The TCP header contains a field with the message sequence number. The sequence number is incremented by one for every message sent.
* During receiving data, TCP rearranges incoming packets and put them in the right order. Thanks to that, the application layer doesn't need to care about the ordering of network packets.

##### TCP Header:

* The TCP header consists of 20 or more bytes. The size depends on the fact whether the optional *options* field is used. The maximum size of the *options* field is 40bytes, thus the maximum size of the whole header is 60 bytes.



**The TCP header structure:**

* Two applications need to establish a session to exchange data. TCP requires three messages to create the session.
* **SYN** - the first application (the client) sends a *synchronize* packet to the host. The message contains a random sequence number, which has been set by the client.
* **SYN-ACK** - the host responds to the client. It increases the sequence number from the client by one and sends it back in the message as an acknowledgement number. Also, the response message contains another sequence number chosen randomly by the host.
* **ACK** - the client sends an acknowledgement message to the host. The message contains both received numbers increased by one.

When the transmission is completed, the session should be terminated. Each side can terminate the session. The second side is supposed to acknowledge that.

**TCP Usage:**

TCP is widely used by protocols and applications that require high reliability. It is not as fast as UDP but, if configured properly, it still provides quite good speed together with high quality of transmitted data.

There are a lot of application layer protocols that are most mostly used together with TCP. Some of the most popular ones are:

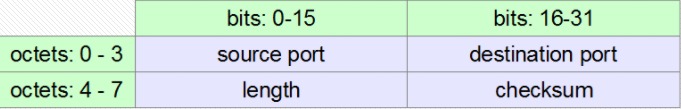
* HTTP, HTTPS
* FTP
* SMTP
* Telnet

#### UDP (User Datagram Protocol):

* The second popular protocol that is used in the transport layer is UDP (User Datagram Protocol or Universal Datagram Protocol), a simpler, connectionless protocol. One program just sends some packages to another, without creating any kind of relation between them.
* Due to its simplicity UDP is faster than TCP. On the other hand, it doesn't provide such reliability as TCP.
* There is no guarantee that the messages would reach the receiver. UDP doesn't deliver packets in the same order that they were sent.
* It is up to the application to check that the received messages are intact and to deal with data in the correct order.

##### UPD Header:

* The UDP header is 8-byte long. It is much shorter and simpler than the corresponding TCP header.



##### UDP Usage:

* UDP is preferred if unimportant data is transmitted or the communication has to be really fast. For example, UDP is used for DNS requests (because of a huge number of clients sending many short messages to relatively few DNS servers). Similarly, during audio and video transmission the loss of some packets is not so damaging to the receiver.
* There are a lot of application layer protocols that use UDP, for example:
* DNS
* DHCP
* TFTP
* SNMP
* RIP
* VOIP

**L2 layer protocol:**

• The **data link layer**, or **layer 2**, is the second layer of the seven-layer OSI model of computer

networking.

• This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer.

• The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer.

• Some of the L2 layer protocols are as follows:

• Ethernet

• ARC net Attached Resource Computer Network

• ARP Address Resolution Protocol

• ATM Asynchronous Transfer Mode

• CHAP Challenge Handshake Authentication Protocol

• CDP Cisco Discovery Protocol

• DCAP Data Link Switching Client Access Protocol

• Distributed Multi-Link Trucking

• Distributed Split Multi-Link Trucking

• DTP Dynamic Trucking Protocol

Detailed explanation of a protocol:

**ARP (Address resolution protocol):**

**ARP:**

1. ARP stands for Address Resolution Protocol.

2. It is the protocol used by Internet Protocol (IP) specifically IPv4.

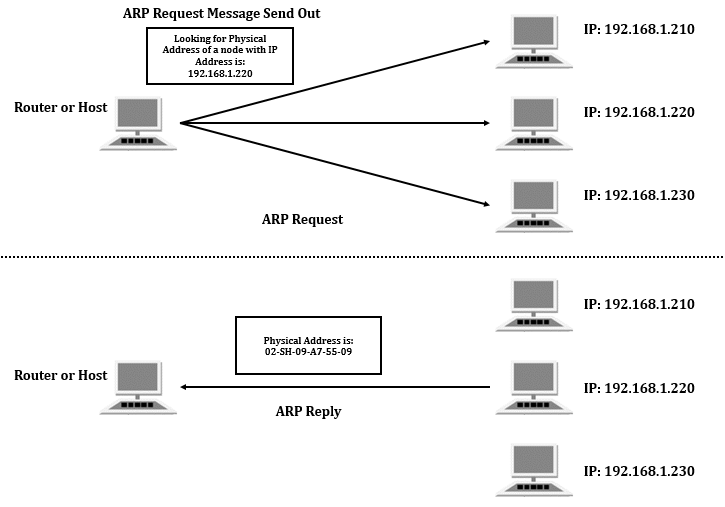
3. This protocol operates below the network layer as a part of the interface between the OSI

network and OSI link layer.

4. It is used to map Logical Addresses to the Physical Addresses used by a data link protocol.

5. ARP Simply Converts IP Address to Physical Address.

6. It is relatively simple Request-and-Reply Protocol.



**Figure 13: ARP Mechanism**

1. ARP maintains the mapping between IP address and MAC address in a table in memory called ARP cache.

2. The entries in this table are dynamically added and removed.

3. A host will update its ARP cache, only if the ARP request is for its IP address.

4. Otherwise, it will discard the ARP request.

5. Consider the above figure, in this a Host sends out the Request Message.

6. It is looking for the MAC Address of the node with IP Address 192.168.1.220.

7. The Node with the IP Address 192.168.1.220 sends out the Reply Message.

8. In reply message it sends its MAC Address to the Host.

**L3 layer protocol:**

• IP Internet Protocol

• ICMP Internet Control Message Protocol

• RIP Routing Information Protocol (v1 and v2)

• OSPF Open Shortest Path First (v1 and v2)

• IPSEC IP sec

**ICMP (Internet Control Message Protocol):**

• ICMP is a transport level protocol within TCP/IP which communicates information about

network connectivity issues back to the source of the compromised transmission.

• It sends control messages such as *destination network unreachable*, *source route failed*,

and *source quench*.

• It uses a data packet structure with an 8-byte header and variable-size data section.

• ICMP is used by a device, like a router, to communicate with the source of a data packet about

transmission issues.

• For example, if a datagram is not delivered, ICMP might report this back to the host with details

to help discern where the transmission went wrong.

• It's a protocol that believes in direct communication in the workplace.

• Ping is a utility which uses ICMP messages to report back information on network connectivity

and the speed of data relay between a host and a destination computer.

• It's one of the few instances where a user can interact directly with ICMP, which typically only

functions to allow networked computers to communicate with one another automatically

**WLAN:**

* WLAN is a local area network (LAN) that doesn’t rely on wired ethernet connections.
* A wireless local area network (WLAN) is a wireless distribution method for two or more devices.
* WLAN supports 54Mbps or above.
* WLANs use high-frequency radio waves and often include an access point to the Internet.
* A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

## **Types of WLAN Protocols**

IEEE 802.11 or WIFI has many variations, the main among which are −

* **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
* **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
* **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
* **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

**Border Gateway Protocol (BGP):**

• Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is

the protocol used between ISP which are different AS’s.

• The protocol can connect together any internetwork of autonomous system using an arbitrary

topology.

• The only requirement is that each AS have at least one router that is able to run BGP and that

does router connect to at least one other AS’s BGP router.

• BGP’s main function is to exchange network reach-ability information with other BGP systems.

• Border Gateway Protocol constructs an autonomous systems’ graph based on the information

exchanged between BGP routers.

**Characteristics of Border Gateway Protocol (BGP):**

• **Inter-Autonomous System Configuration:** The main role of BGP is to provide communication

between two autonomous systems.

• BGP supports Next-Hop Paradigm.

• Coordination among multiple BGP speakers within the AS (Autonomous System).

• **Path Information:** BGP advertisement also include path information, along with the reachable

destination and next destination pair.

• **Policy Support:** BGP can implement policies that can be configured by the administrator. For

ex: - a router running BGP can be configured to distinguish between the routes that are known

within the AS and that which are known from outside the AS.

• Runs Over TCP.

• BGP conserve network Bandwidth.

• BGP supports CIDR.

• BGP also supports Security.

## **IPv4 addresses:**

* An IP address (*internet protocol address*) is a numerical representation that uniquely identifies a specific interface on the network.
* IPv4 addresses are 32-bit binary numbers, consisting of the two sub addresses (identifiers), identify the network and the host to the network, with an imaginary boundary separating the two. An IP address is, as such, generally shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.
* For example, the address **168.212.226.204** represents the 32-bit binary number 10101000.11010100.11100010.11001100.
* The binary number is important because that will determine which class of network the IP address belongs to.
* An IPv4 address is typically expressed in dotted-decimal notation, with every eight bits (octet) represented by a number from one to 255, each separated by a dot.
* An example IPv4 address would look like this:192.168.17.22
* IPv4 addresses are composed of two parts. The first numbers in the address specify the network, while the latter numbers specify the specific host. A subnet mask specifies which part of an address is the network part, and which part addresses the specific host.
* A packet with a destination address that is not on the same network as the source address will be forwarded, or routed, to the appropriate network. Once on the correct network, the host part of the address determines which interface the packet gets delivered to.

## **IPv6 addresses:**

* To avoid the seemingly reoccurring issue in technology, where a specification’s limitation seems more than sufficient at the time, but inevitably becomes too small, the designers of IPv6 created an enormous address space for IPv6. The address size was increased from 32 bits in IPv4 to 128 bits in IPv6.
* The IPv6 has a theoretical limit of 3.4 x 1038 addresses.
* IPv6 addresses are represented by eight sets of four hexadecimal digits, and each set of numbers is separated by a colon.
* An example IPv6 address would look like this:

( 2DAB:FFFF:0000:3EAE:01AA:00FF:DD72:2C4A )

* With IPv6 addresses being so long, there are conventions to allow for their abbreviation. First, leading zeros from any one group of numbers may be eliminated. For example, :0033: can be written as :33:
* Any consecutive sections of zeros can be represented by a double colon. This may be done only once in any address.
* The number of sections removed using this abbreviation can be determined as the number required to bring the address back up to eight sections.
* Like in IPv4 certain address blocks are reserved for private networks. These addresses are not routed over the public internet. In IPv6, private addresses are called Unique Local Addresses (ULA). Addresses from the FC00 :: /7 block are ignored and not routed by default.
* In both IPv4 and IPv6, remembering the IP address of every device is not possible, except on the smallest of networks. Name resolution provides a way to lookup an IP address from an easier to use name.

**IPv4 subnetting:**

IPv4 allows for a variation of the network and host segments of an IP address, known as subnetting, can be used to physically and logically design a network. For example, an organization can have a single internet network address (NETID) that is known to users outside the organization, yet configure its internal network into different departmental subnets. Subnetwork addresses enhance local routing capabilities, while reducing the number of network addresses required.

There are basically 5 classes of subnets, out of which 3 are extensively used for the user use.

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts.

In Class B, first two octets are used as Network identifiers and rest of two octets are used to be assigned to Hosts.

In Class C, first three octets are used as Network identifiers and rest of the octet is used to be assigned to Hosts.

## **Steps for IPV4 Subnetting**

STEP 1: Convert the IP address and Subnet Mask values into Binary

STEP 2: Calculate the Subnet Address

STEP 3: Find Host Range

STEP 4: Calculate the Total Number of Subnets and Hosts Per Subnet

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | **1** | **2** | **4** | **8** | **16** | **32** | **64** | **128** | **256** |
| **Host** | **256** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| **Subnet Mask**  **Class A** | **/8** | **/9** | **/10** | **/11** | **/12** | **/13** | **/14** | **15** | **/16** |
| **Class B** | **/16** | **/17** | **/18** | **/19** | **/20** | **/21** | **/22** | **/23** | **/24** |
| **Class C** | **/24** | **/25** | **/26** | **/27** | **/28** | **/29** | **/30** | **/31** | **/32** |

**Class A:**

**100.101.103.104/10 ----- 4 networks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network ID** | **Subnet**  **Mask** | **Host ID Range** | **No of Hosts** | **Broadcast ID** |
| **100.0.0.0** | **/10** | **100.0.0.1 - 100.63.255.254** | **64** | **100.63.255.255** |
| **100.64.0.0** | **/10** | **100.64.0.1 - 100.127.255.254** | **64** | **100.127.255.255** |
| **100.128.0.0** | **/10** | **100.128.0.1 - 100.191.255.254** | **64** | **100.191.255.255** |
| **100.192.0.0** | **/10** | **100.192.0.1 - 100.255.255.254** | **64** | **100.255.255.255** |

**Class B:**

**140.14.16.17/18 ----- 4 networks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network ID** | **Subnet**  **Mask** | **Host ID Range** | **No of Hosts** | **Broadcast ID** |
| **140.14.0.0** | **/18** | **140.14.0.1 - 140.14.63.254** | **64** | **140.14.63.255** |
| **140.14.64.0** | **/18** | **140.14.64.1 - 140.14.127.254** | **64** | **140.14.127.255** |
| **140.14.128.0** | **/18** | **140.14.128.1 - 140.14.191.254** | **64** | **140.14.191.255** |
| **140.14.192.0** | **/18** | **140.14.192.1 - 140.14.255.254** | **64** | **140.14.255.255** |

**Class C: 193.186.16.15/26 ----- 4 networks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network ID** | **Subnet**  **Mask** | **Host ID Range** | **No of Hosts** | **Broadcast ID** |
| **193.186.16.0** | **/26** | **193.186.16.1 - 193.186.16.62** | **64** | **193.186.16.63** |
| **193.186.16.64** | **/26** | **193.186.16.65 - 193.186.16.126** | **64** | **193.186.16.127** |
| **193.186.16.128** | **/26** | **193.186.16.129 - 193.186.16.190** | **64** | **193.186.16.191** |
| **193.186.16.192** | **/26** | **193.186.16.193 - 193.186.16.254** | **64** | **193.186.16.255** |

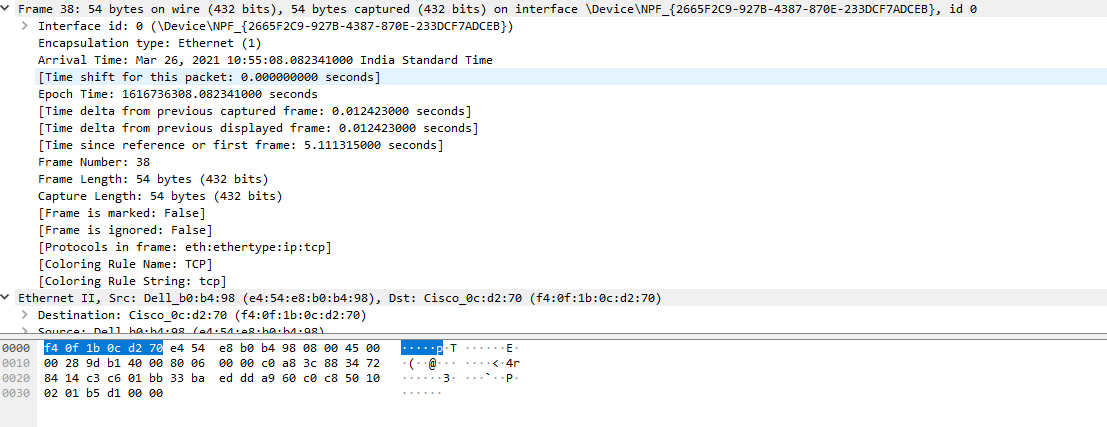
**Network Tools:**

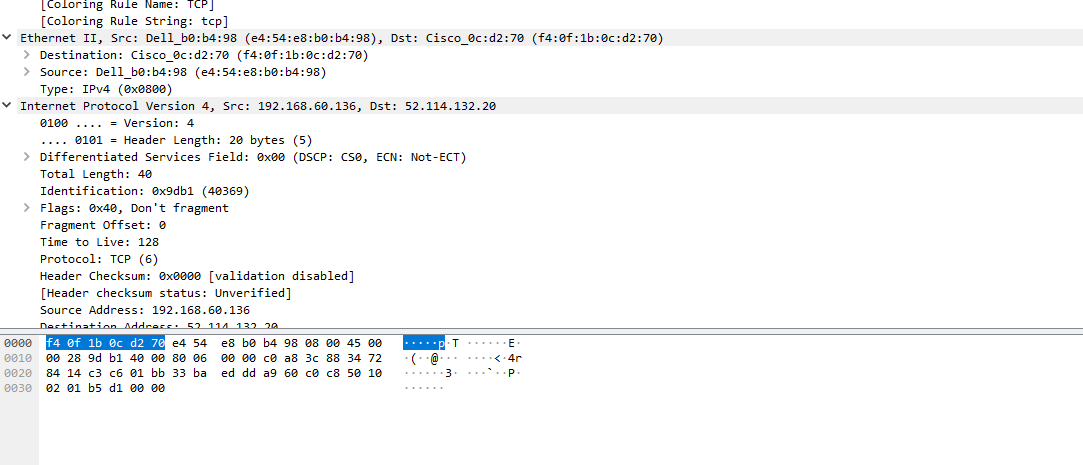
## **Wireshark**

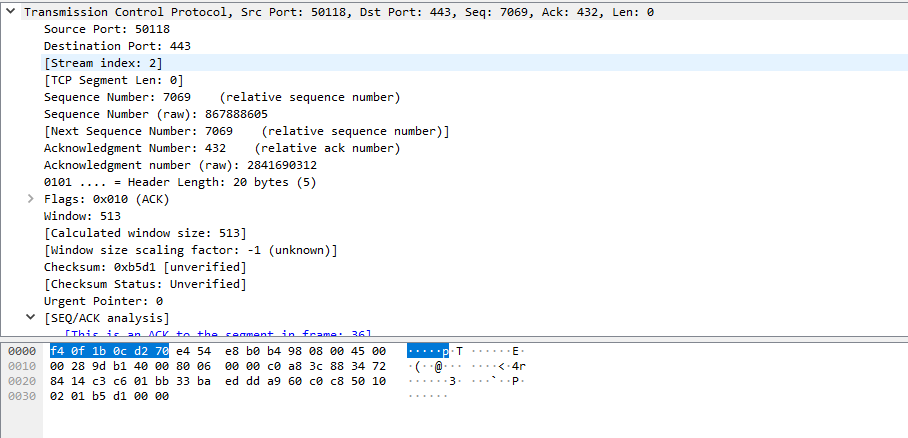
Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

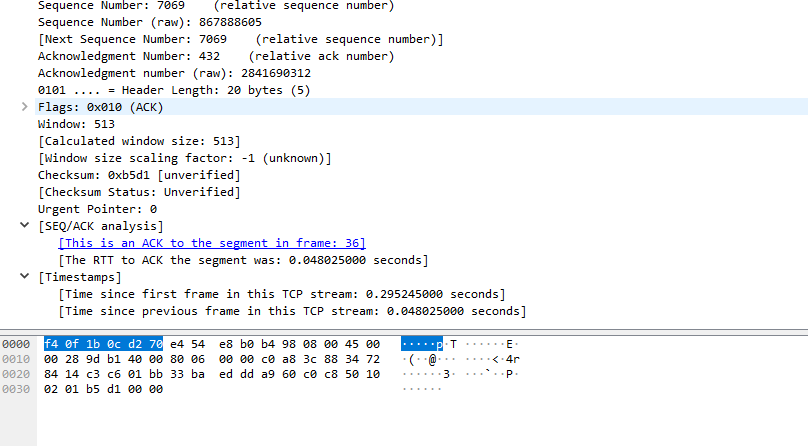
It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

**Wireshark Log analysis**

****

****

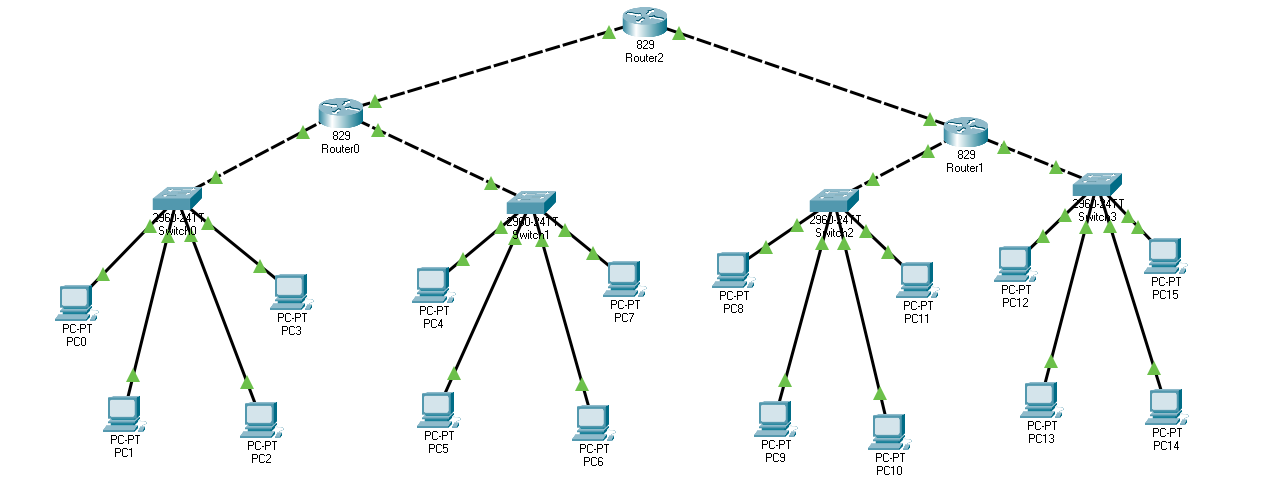
****

****

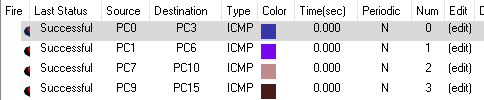
## **Packet Tracer**

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

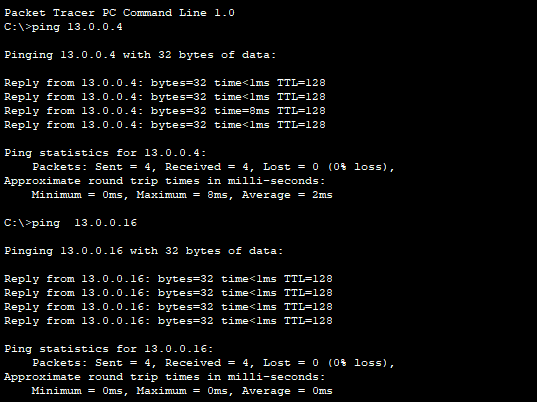
**Network**

****

**Message Acknowledgement**

****

**Pinging IP :**

****