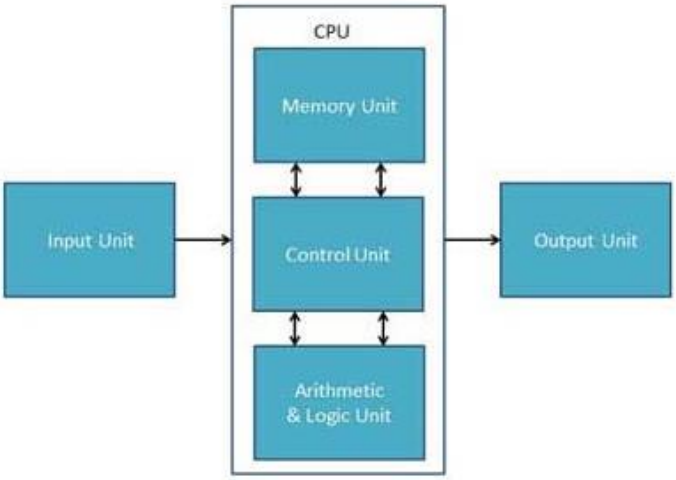
AWS Solution Architect Associate Certification Training – Module 1

1. Basics of Computer and Networking

Introduce Computers and Components

An electronic data processing device, which requires input raw data for processing and generates the output in desired form. It stores the data in its memory which can be accessed any number of times for reference from its memory, it is made up of a lot of electronics, software and mechanical parts.



A computer is divided into three basic units namely:

1. Input Unit
2. Central Processing Unit
3. Output Unit

These units are defined as below:

1. Input unit

As the name suggests, this unit contains devices with the help of which the data is entered into the computer. This unit is a basic requirement for computer system. The input devices are of many types such as keyboard, mouse, joy stick, microphone, camera etc. Input devices give different set of input values converted into a form understandable to the computer.

2. Central Processing Unit (CPU)

Central Processing Unit (CPU) is known as the brain of the computer. It performs all types of data processing operations as required by the programmer. It stores all the data, intermediate results and instructions as given by the programmer in the form of codes (program). Central Processing Unit controls the operation of each part of the computer.

It has the following three components:

I. Arithmetic Logic Unit (ALU)
II. Memory Unit
III. Control Unit

3. **Output Unit**

   The devices with the help of which we get the information from the computer are known as the output devices. Output unit is an interface between the computer and the user. Output devices notify the information displayed into a form which is understandable by the computer user.

Functions of a Computer

1. Data is entered into the computer using Input Devices.
2. Data or Instructions are stored in the computer in its memory and processed or uses them as and when required.
3. Data is processed and converted into useful information.
4. Output is generated as per format.
5. Control Mechanism is established for controlling all the functions.

We can divide computer in Hardware and Software:

1. **Hardware:** Keyboard, mouse, joy stick, microphone, camera, printer, monitor, Hard disk, CD, DVD, CPU, motherboard, RAM etc. are known as Hardware
2. **Software:** System Software and Application Software

Advantages of Computers

A Computer has a very High Speed of Processing i.e., can perform large amount of data very quickly. Computers are very accurate. Computers are very fast devices. Once the correct input is given to the computers, the output is 100% accurate. It has a large memory capacity. It can store a given large amounts of information for a large time. It is a reliable device.

Uses of Computers

Nowadays it is used in every walk of life. It has an important role industrial automation. Computers are playing very important role in Medical science, Engineering, General Education, Government and Private organizations, Film and Entertainment. It is at the top of making DIGITAL INDIA.

Introduce Networking Models and Concepts, IPV4, LAN, WAN, Subnets, Switches and Routers

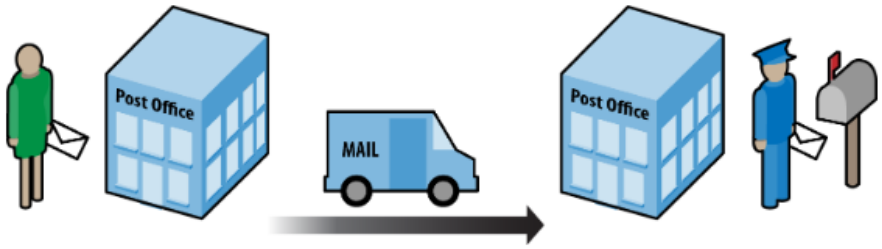
Networking Models:

Basic network architecture and construction is a good starting point when trying to understand how communication systems function, even though the topic is a bit dull. Architectures are typically based on a model showing how protocols and functions fit together. Historically, there have been many models used for this purpose, including, but not limited to, Systems Network Architecture (SNA-IBM), AppleTalk, Novell Netware (IPX/SPX), and the Open System Interconnection (OSI) model. Most of these have gone the way of the dodo due to the popularity of TCP/IP. TCP/IP stands for *Transmission Control Protocol/Internet Protocol* and represents a suite of protocols used on almost all modern communication systems. As the name suggests, this is the language of the Internet. This chapter focuses on the practical TCP/IP model, using the OSI model as a reference point.

What is a model?

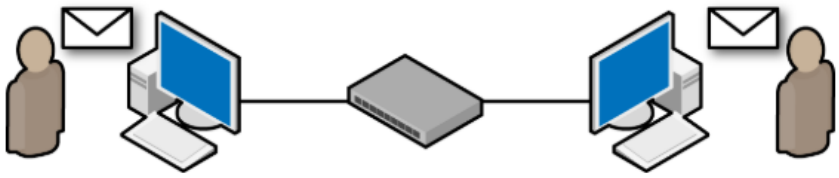
A *model* is a way to organize a system's functions and features to define its structural design. A design can help us understand how a communication system accomplishes tasks to form a protocol suite. To help us wrap our heads around models, communication systems are often compared to the postal system. Imagine writing a letter and taking it to the post office. At some point, the mail is sorted and then delivered via some transport system to another post office. From there, it is sorted and given to a mail carrier for delivery to the destination. The letter is handled at several points along the way. Each part of the system is trying to accomplish the same thing—delivering the mail. But each section has a particular set of rules to obey. While in transit, the truck follows the rules of the road as the letter is delivered to the next point for processing. Inspectors and sorters ensure the mail is metered and safe, without much concern for traffic lights or turn signals.

Postal system



A communication system is not much different, since messages created on a computer are processed and delivered, with each piece of equipment involved performing some function and obeying certain rules for transmission. The below figure depicts a typical scenario in which two computers are connected by their network cards via a networking device. Two people are communicating using an application such as an instant messaging or email program. At some point, we have to decide exactly how to handle this communication. After all, when you mail that letter, you cannot address the envelope in some arbitrary language or ignore zip codes, just as the mail truck driver cannot drive on the wrong side of the road.

Small communication network



So, how is the job of each device or connection determined? An application at the user level should not be responsible for choosing the encoding sequence or the signal type used between the client and server. The letter doesn't decide to go by air or boat. Similarly, the network interface card (NIC) is not in the business of message header construction, just as the mail sorting system doesn't care if you use pen or pencil when writing a letter. Models are routinely organized in a hierarchical or layered structure. Each layer has a set of functions to perform. Protocols are created to handle these functions, and therefore, protocols are also associated with each layer. The protocols are collectively referred to as a *protocol suite*. The lower layers are often linked with hardware, and the upper layers with software. For example, Ethernet operates at Layers 1 and 2, while the File Transfer Protocol (FTP) operates at the very top of the model. This is true for both the TCP/IP and OSI models. Network traffic can also be viewed in terms of these layers, many of which can actually be seen using a packet capture tool like Wireshark. In below figure, the major layers of the TCP/IP model are displayed in a message going to a web server.

Packet showing layers

```
Ethernet II, Src: WesternD_89:ba:fa (00:00:c0:89:ba:fa), Dst: Cisco_2c:0c:80 (00:11:21:2c:0c:80)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.254 (192.168.1.254)
Transmission Control Protocol, Src Port: optima-vnet (1051), Dst Port: http (80), Seq: 1, Ack: 1, Len: 336
Hypertext Transfer Protocol
```

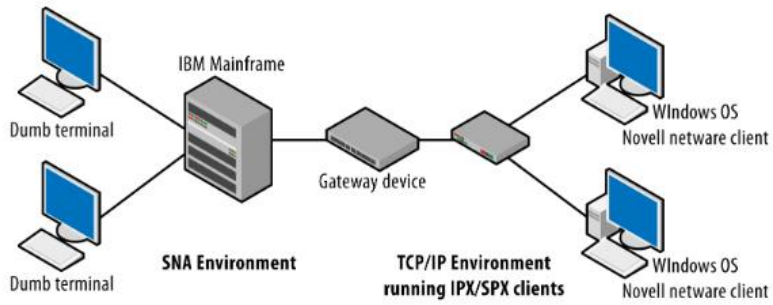
Why Use a Model?

Before we go too far, let's do a little reality check. A model describes the entire structure. At the beginning of the chapter, I stated that many networking models "have gone the way of the dodo." There may have been good ideas in each, but everyone ended up using one model in particular—TCP/IP. For example, both Apple and IBM initially developed their own protocol suites, but converted to TCP/IP due to its popularity. This section explains the historical use of models and provides a more modern viewpoint.

Even a simple communication system is a complicated environment in which thousands or even millions of transactions occur daily. Interconnected systems are considerably more complex. A single electrical disturbance or software configuration error can prevent completion of these transactions.

Models provide a starting point for determining what must be done to enable communication or to figure out how systems using different protocols might connect to each other. They also help in troubleshooting problems. For example, how would a Novell NetWare client running IPX/SPX communicate with an IBM AS/400 over a TCP/IP-based network? Below figure depicts a scenario in which several different platforms might be required to interact with each other. Windows nodes are based on the TCP/IP protocol suite but, if required, can run Novell NetWare client software for network authentication. Novell developed internetworking and transport protocols called IPX and SPX. At the other end of the network, the IBM mainframe communicates via the protocols used in the SNA model. Imagine the programming and extra effort required to maintain all of the transactions between these separate architectures.

Mixed architecture topology



Another example is a network of Apple computers running AppleTalk while connecting to a network of Windows machines running TCP/IP.

As I've said, TCP/IP is the prevalent architecture today. The complexities of interplatform communication are dramatically reduced with TCP/IP. Protocol systems such as AppleTalk, NetWare, and SNA are considered legacy. However, understanding protocol layers on a particular communications device or how processes might interact on the network are still critically important ideas. When troubleshooting standard problems or potential security threats, the models and their associated layers offer logical reference points to begin the process. One would not start looking at the routing protocols if the link light was dark.

OSI Model

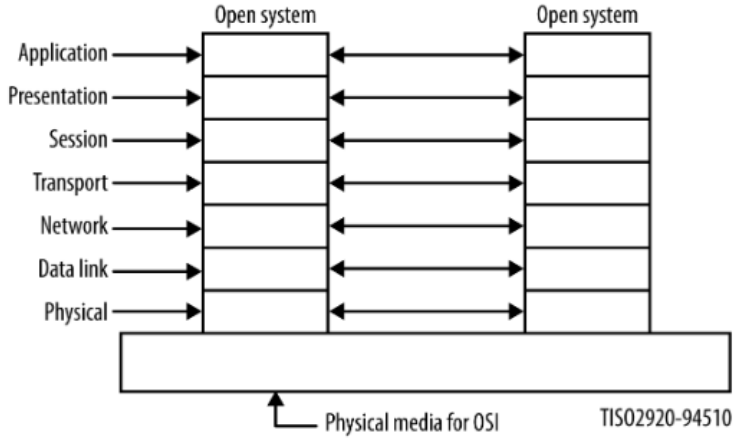
The OSI model is called a *reference model*. This means this particular model provides a method by which standards and protocols can be compared in order to assist in connectivity and consistency. Developers can use a reference model to understand how transmissions are framed and create methods to translate between systems.

The OSI basic model is standardized in ISO/IEC (International Standards Organization/International Electro technical Commission) 7498, which includes most of the definitions used here. These two organizations have actually created a Joint Technical Committee (JTC) that handles the issues associated with information technology. This model was developed in collaboration with the ITU-T and has also been printed as ITU-T Recommendation X.200. The ITU-T is the International Telecommunications Union—Telecom sector. Now that we've had our fill of acronyms, on to the standard.

The first version of ISO/IEC 7498 was written in 1984. This was replaced in 1994 by version 2, with additional corrections after that date. ISO/IEC 7498 has four parts:

- Part 1—The Basic Model
- Part 2—Security Architecture
- Part 3—Naming and Addressing
- Part 4—Management Framework

The OSI layers



A) The Physical Layer

- The Physical Layer is the bottom most layer and is associated with electrical, mechanical and functional aspects of the transmission media for information and receiving over internet.

B) The Data Link Layer

- The Data Link Layer is second from bottom and comes under the lower layer category. It ensures that the data must be synchronized, error detection and control are enabled.

C) The Network Layer

- The Network Layer is third from bottom in OSI model and is responsible for establishing data communication channel between multiple networks or devices or hosts or nodes.

D) The Transport Layer

- Transport Layer is the middle most layer in OSI model and it acts as Network Independent Layer. It has no idea about the functioning of lower layer i.e. physical, data link and network layers.

E) The Session Layer

- Session Layer is the fifth layer of OSI model and it provides appropriate sessions between users and entities, where user interacts. This layer can be used on the basis of resources available and it can be skipped too if not required.
- For example: Login Sessions in online banking.

F) The Presentation Layer

- This is the sixth layer of OSI model and it provides appropriate representation of data through various data presentation techniques.

G) The Application Layer

- Application Layer is the topmost layer of the OSI model and has the responsibility for providing interface between various users and application.

Introducing TCP/IP

The Internet and almost all networks in use today have standardized on the TCP/IP model. It is often referred to as the language of the Internet, because applications are typically built around this protocol suite. Below figure shows the TCP/IP model and some of the more well-known protocols and

corresponding layers. At Layer 4 (the Transport Layer), there are actually two protocols present—TCP and UDP. While this model shares its name with the former, many operations are based on UDP, so Layer 4 is shared by the two protocols. Layers 1 and 2 are governed by the local area network protocol, but Layer 3 belongs to IP, with Internet Control Message Protocol (ICMP) and Internet Group Membership Protocol (IGMP) components of IP-based operations.

The TCP/IP model and protocols

Application	FTP, Telnet, email, games, printing, HTTP
Transport	Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
Internet (Internetwork)	Internet Protocol (IP), ICMP, IGMP
Link (Network)	Ethernet, 802.11
Physical	Ethernet, 802.11

Comparing the TCP/IP and OSI models, it can be said that the functions are the same but the structure is different. Figure 1-10 shows a side-by-side comparison of the OSI and TCP/IP model layers. Layers 5–7 of the OSI model map to Layer 5 of the TCP/IP model.

The TCP/IP and OSI networking models

Application	7	Application
	6	Presentation
	5	Session
Transport	4	Transport
Internet	3	Network
Link/Network	2	Data Link
Physical	1	Physical

Basic Networking Concepts

a) Introduction

- A network can be defined as a group of computers and other devices connected in some ways so as to be able to exchange data.
- Each of the devices on the network can be thought of as a node; each node has a unique address. Addresses are numeric quantities that are easy for computers to work with, but not for humans to remember. Example: 204.160.241.98
- Some networks also provide names that humans can more easily remember than numbers. Example: www.javasoft.com, corresponding to the above numeric address.

Domain Name System (DNS): Mnemonic textual addresses are provided to facilitate the manipulation of internet addresses. DNS servers are responsible for translating mnemonic textual Internet addresses into hard numeric Internet addresses.

Ports: An IP address identifies a host machine on the Internet. An IP port will identify a specific application running on an Internet host machine. A port is identified by a number, the port number. The number of ports is not functionally limited, in contrast to serial communications where only 4 ports are allowed. There are some port numbers which are dedicated for specific applications

Applications	Port numbers
HTTP	80
FTP	20 and 21
Gopher	70
SMTP (e-mail)	25
POP3 (e-mail)	110
Telnet	23
Finger	79

Data Transmission:

Data Transmission -In modern networks, data are transferred using packet switching. Messages are broken into units called packets, and sent from one computer to the other. At the destination, data are extracted from one or more packets and used to reconstruct the original message. Each packet has a maximum size, and consists of a header and a data area. The header contains the addresses of the source and destination computers and sequencing information necessary to reassemble the message at the destination.

packet

header	data
1001….101	00010000111…000000110001100

Types of Networks:

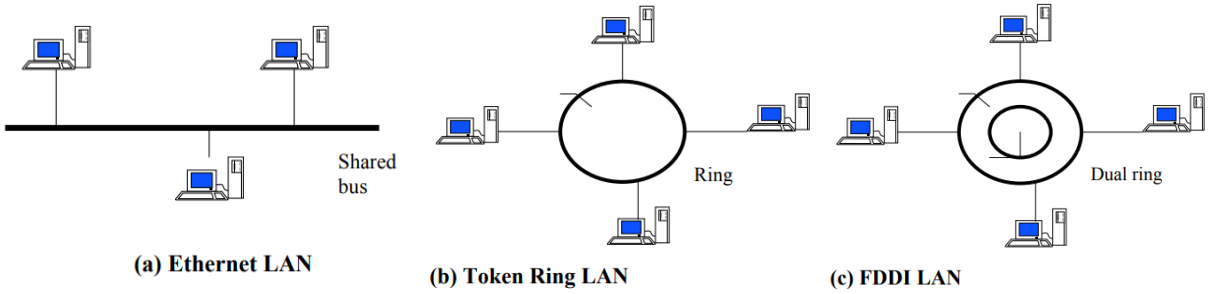
There are two principle kinds of networks: Wide Area Networks (WANs) and Local Area Networks (LANs).

WANs

- Cover cities, countries, and continents.
- Based on packet switching technology
- Examples of WAN technology: Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN)

LANs:

- Cover buildings or a set of closely related buildings.
- Examples of LAN technology: Ethernet, Token Ring, and Fiber Distributed Data Interconnect (FDDI).
    - ✓ Ethernet LANs: based on a bus topology and broadcast communication
    - ✓ Token ring LANs: based on ring topology
    - ✓ FDDI LANs: use optical fibers and an improved token ring mechanism based on two rings flowing in opposite directions.



(a) Ethernet LAN (b) Token Ring LAN (c) FDDI LAN

Interconnection

- Networks of low capacity may be connected together via a backbone network which is a network of high capacity such as a FDDI network, a WAN network etc. \
- LANs and WANs can be interconnected via T1 or T3 digital leased lines.
- According to the protocols involved, networks interconnection is achieved using one or several of the following devices:
    - Bridge: a computer or device that links two similar LANs based on the same protocol.
    - Router: a communication computer that connects different types of networks using different protocols.
    - B-router or Bridge/Router: a single device that combines both the functions of bridge and router.
    - Gateway: a network device that connects two different systems, using direct and systematic translation between protocols

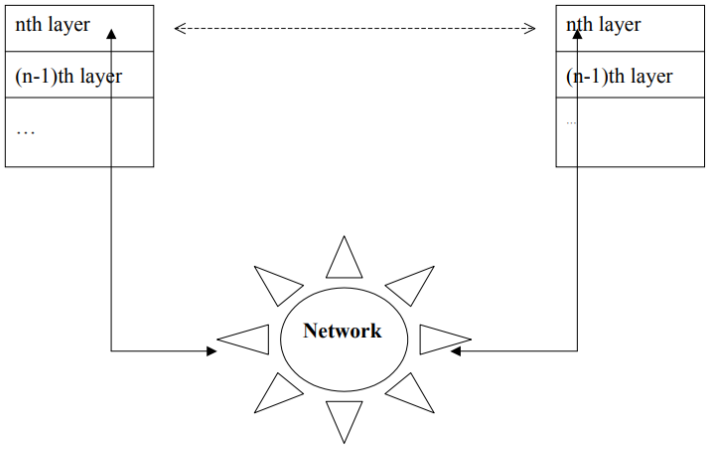
Network Topology Diagram

The specification of the network topology diagram requires the definition of the characteristics and entities underlying the network

- Geographical locations of the different components or subnets involved in the network.
- Description of the LAN topology
- Description of the WAN topology
- Description of the network connectors such as routers, bridges, repeaters, and gateways.

b) Protocols

- Define the rules that govern the communications between two computers connected to the network.
- Roles: addressing and routing of messages, error detection and recovery, sequence and flow controls etc.
- A protocol specification consists of the syntax, which defines the kinds and formats of the messages exchanged, and the semantic, which specifies the action taken by each entity when specific events occur.
- Example: HTTP protocol for communication between web browsers and servers.
- Protocols are designed based on a layered architecture such as the OSI reference model.
- Each entity at a layer n communicates only with entities at layer n-1.
- The data exchanged, known as Protocol Data Unit (PDU), goes back and forth through the layers, each layer adds or removes its own header and vice-versa. Therefore a layer n PDU may become a layer n-1 data.



c) Networks Interconnection/Internet

Concept of Network Interconnection

- First implemented in the Defense Advanced Research Project Agency Network (Arpanet), in 1966 in USA.
- Consists of connecting several computer networks based on different protocols.
- Requires the definition of a common interconnection protocol on top the local protocols.

- The Internet Protocol (IP) plays this role, by defining unique addresses for a network and a host machine.

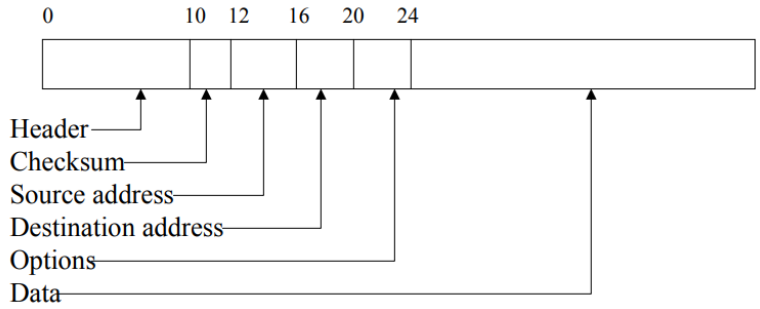
Internet Protocol (IP)

Overview

- The IP protocol provides two main functionality:
  - Decomposition of the initial information flow into packets of standardized size, and reassembling at the destination.
  - Routing of a packet through successive networks, from the source machine to the destination identified by its IP address.
- Transmitted packets are not guaranteed to be delivered (datagram protocol).
- The IP protocol does not request for connection (connectionless) before sending data and does not make any error detection. Functions.
- Decompose the initial data (to be sent) into datagrams.
- Each datagram will have a header including, the IP address and the port number of the destination.
- Datagrams are then sent to selected gateways, e.g IP routers, connected at the same time to the local network and to an IP service provider network. 23 Sender Receiver packet1 packet2 Routers.
- Datagrams are transferred from gateways to gateways until they arrived at their final destination.

Structure of an IP packet

- The fields at the beginning of the packet, called the frame header, define the IP protocol's functionality and limitations.
- 32 bits are allocated for encoding source and destination addresses (32 bits for each of these address fields).
- The remainder of the header (16 bits) encodes various information such as the total packet length in bytes.
- Hence an IP packet can be a maximum of 64Kb long.



Internet Application Protocols

On top of TCP/IP, several services have been developed in order to homogenize applications of same nature

- **FTP** (File Transfer Protocol) allows the transfer of collection of files between two machines connected to the Internet.
- **Telnet** (Terminal Protocol) allows a user to connect to a remote host in terminal mode.
- **NNTP** (Network News Transfer Protocol) allows the constitution of communication groups (newsgroups) organized around specific topics.
- **SMTP** (Simple Mail Transfer Protocol) defines a basic service for electronic mails. -SNMP (Simple Network Management Protocol) allows the management of the network.

Addressing

IP Address:

An IP address, or simply an "IP," is a unique address that identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected via the Internet protocol. There are two primary types of IP address formats used today — IPv4 and IPv6.

The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of 20. The bit just to the left of that holds a value of 21. This continues until the left-most bit, or most significant bit, which holds a value of 27. So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

```
  1   1   1   1 1 1 1 1
128  64  32  16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

Here is a sample octet conversion when not all of the bits are set to 1.

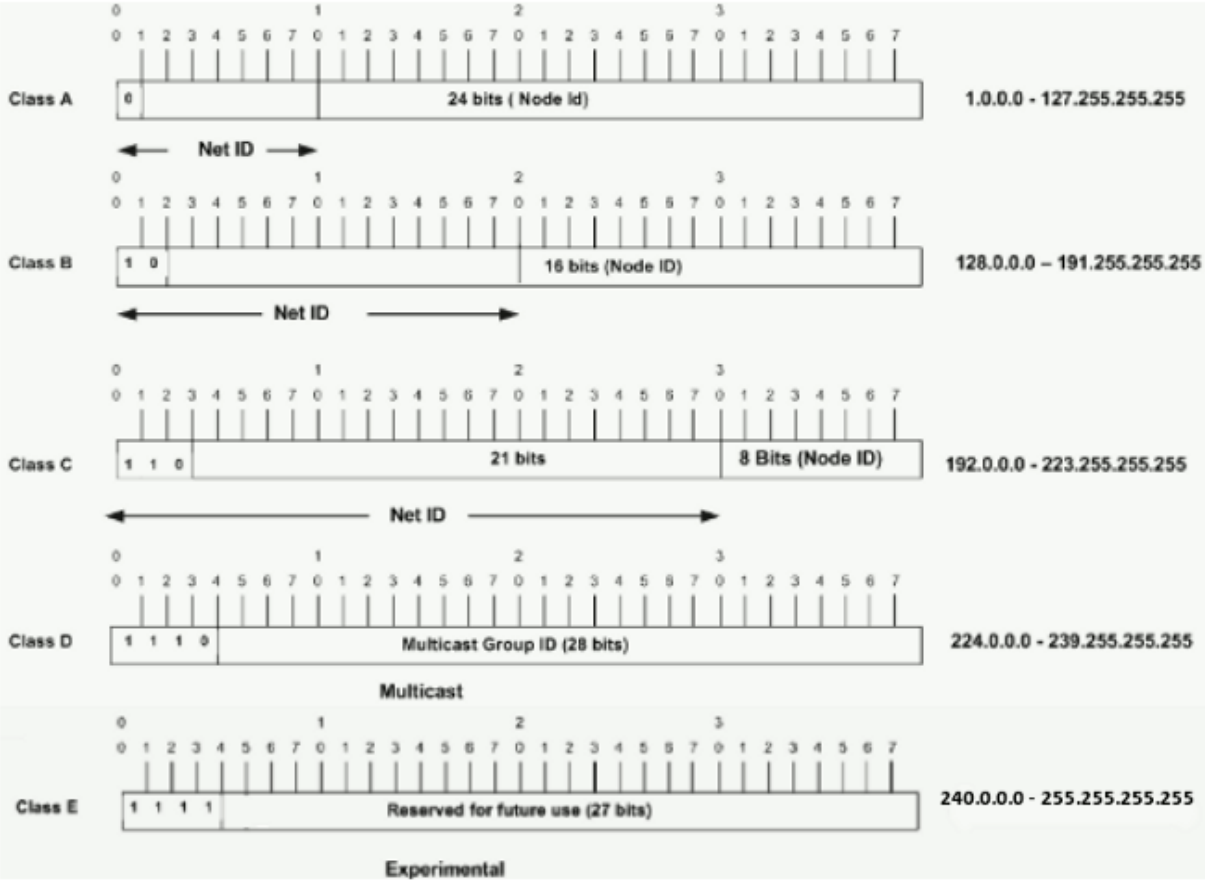
```
0   1 0 0 0 0 0 1
0  64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

And this sample shows an IP address represented in both binary and decimal.

```
       10.       1.      23.      19 (decimal)
00001010.00000001.00010111.00010011 (binary)
```

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E. This document focuses on classes A to C, since classes D and E are reserved and discussion of them is beyond the scope of this document.

Given an IP address, its class can be determined from the three high-order bits (the three left-most bits in the first octet). Below figure shows the significance in the three high order bits and the range of addresses that fall into each class. For informational purposes, Class D and Class E addresses are also shown.



IPv4

An IPv4 address consist of four sets of numbers from 0 to 255, separated by three dots. For example, the IP address of TechTerms.com is 67.43.14.98. This number is used to identify the TechTerms website on the Internet. When you visit http://techterms.com in your web browser, the DNS system automatically translates the domain name "techterms.com" to the IP address "67.43.14.98."
There are three classes of IPv4 address sets that can be registered through the InterNIC. The smallest is Class C, which consists of 256 IP addresses (e.g. 123.123.123.xxx — where xxx is 0 to 255). The next largest is Class B, which contains 65,536 IP addresses (e.g. 123.123.xxx.xxx). The largest block is Class A, which contains 16,777,216 IP addresses (e.g. 123.xxx.xxx.xxx).

The total number of IPv4 addresses ranges from 000.000.000.000 to 255.255.255.255. Because 256 = 28, there are 28 x 4 or 4,294,967,296 possible IP addresses. While this may seem like a large number, it is no longer enough to cover all the devices connected to the Internet around the world. Therefore, many devices now use IPv6 addresses.

IPv6

The IPv6 address format is much different than the IPv4 format. It contains eight sets of four hexadecimal digits and uses colons to separate each block. An example of an IPv6 address is: 2602:0445:0000:0000:a93e:5ca7:81e2:5f9d. There are 3.4 x 1038 or 340 undecillion) possible IPv6 addresses, meaning we shouldn't run out of IPv6 addresses anytime soon.

Subnets

A subnet is a logical partition of an IP network into multiple, smaller network segments. It is typically used to subdivide large networks into smaller, more efficient sub networks.

The internet is composed of many networks that are run by many organizations. In turn, each organization's network can be composed of many smaller networks, or subnets. Each subnet allows its connected devices to communicate with each other, and routers are used to communicate between subnets. The size of a subnet depends on the connectivity requirements and the network technology employed. A point-to-point subnet allows two devices to connect, while a data center subnet might be designed to connect many more devices.

Router

A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation.

Switch

A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it.

What is the difference between a switch and a router?

A switch is designed to connect computers within a network, while a router is designed to connect multiple networks together.

In a home network, a single router is usually all that is required for connecting devices to the Internet. All devices within a home, such as computers, tablets, and smartphones can connect to the router via a wired or wireless connection. As the name implies, the router routes all connected devices to a cable or DSL modem.

Switches are most often used in large networks, such as those found in business and school environments. They connect many computers together within a single local area network, or LAN. A large network may include multiple switches, which connect different groups of computer systems

together. These switches are typically connected to a router that allows connected devices to access the Internet.