

Network Fundamentals

NEWNF401

Apply Network Fundamentals

Competence

REQF Level: 4

Credits: 8

Sector: ICT

Sub-sector: Networking

Module Note Issue date: September, 2020

Learning hours:



Purpose statement

This core module describes the skills, knowledge and attitude required to describe the purpose and functions of various network devices and protocols. The learner will be able to select the components required to meet a network specification, Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network, describe the purpose and basic operation of the protocols in the OSI and TCP models, the components required for network and Internet communications, differentiate LAN/WAN operation and features. Explain the technology and media access control method for Ethernet networks, network segmentation and basic traffic management concepts, implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network, describe the operation and benefits of using private and public IP addressing. At the end the learner will have a strong foundation and an understanding of basic network functions, standards, and protocols.

Table of Contents

Elements of competence and performance criteria		Page No.
Learning Unit	Performance Criteria	
1. Learning Unit 1 Introduction to Network Concepts	LO 1.1 – Description of Network concepts and Technologies	3
	LO1.2. Description of Network topology	
	LO1.3. Identification of Network devices, Components and their Functions	
2. Learning Unit 2 Network protocols and communications	LO2. 1. Description of network protocols	23
	LO2.2. Description of Network standards	
	LO2.3. Identification and application of Network media and connectors	
3. Learning Unit 3 IP Addressing (IPv4&IPv6)	LO3.1 – Description of IP Addressing concepts	45
	LO3.2. Applying IP v4	
	LO3.3. Apply IPv6	

Total Number of Pages: 97

Learning Unit 1 Introduction to Network Concepts

LO 1.1 – Description of Network concepts and Technologies

- **Content/Topic 1: Description of Computer Network**

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

The nodes of a computer network may be classified by many means as personal computers, servers, networking hardware, or general purpose hosts. They are identified by hostnames and network addresses. Hos

tnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol

- **Elements of Network**

The modern data network has become a critical asset for many industries. Most basic data networks are designed to connect users and enable them to access various resources, like the Internet and other computers connected to the network. Networks are comprised of four basic elements: hardware, software, protocols and the connection medium.

- ✓ **Hardware**

The backbone of any network is the hardware that runs it. Network hardware includes network cards, routers or network switches, modems and Ethernet repeaters. Without this hardware, computers have no means of accessing a network. Network cards give computers direct access to network media and enable them to connect to other equipment, including routers, switches, modems and repeaters. Routers or switches allow a single network connection from a modem to be divided between several computers. Repeater refresh the network signal between Ethernet cable segments, allowing Category 5 cables to reach beyond their 300-foot maximum length without signal loss.

✓ **Software**

Network software is a foundational element for any network. This type of software helps administrators deploy, manage and monitor a network. The traditional networks are made up of specialized hardware, such as routers and switches that bundle the networking software into the solution.

Such type of software encompass a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. When the software like Defined Networking (SDN) emerged, software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

✓ **Protocols**

There are some defined rules and conventions for communication between network devices. These are called Protocols. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.

Protocols may be of 3 types:

1. Internet Protocols
2. Wireless Network Protocols
3. Network Routing Protocols

✓ **Transmission medium:**

The means through which we send our data from one place to another is known as Transmission medium.

Signals are used to represent data by computers and other telecommunication devices. The signals (i.e., data or information) are transmitted in the form of electromagnetic energy from one device to another. These signals travel through vacuum, air or other transmission mediums to move from one point to another (from sender to receiver).

Transmission medium is of two types:

(i) Wired or Guided: For example, Twisted Pair Cable, Coaxial Cable and Optical Fiber Cable.

(i) Wireless or Unguided: For example, Radio waves, Microwaves and Infrared.

- **Benefits of Network**

Setting up a computer network is a fast and reliable way of sharing information and resources within a business. It can help you make the most of your IT systems and equipment.

Advantages of computer networking

Main benefits of networks include:

- **File sharing** – you can easily share data between different users, or access it remotely if you keep it on other connected devices.
- **Resource sharing** – using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money.
- **Sharing a single internet connection** – it is cost-efficient and can help protect your systems if you properly secure the network.
- **Increasing storage capacity** – you can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

Networking computers can also help you improve communication, so that:

- staff, suppliers and customers can share information and get in touch more easily
- your business can become more efficient - eg networked access to a common database can avoid the same data being keyed multiple times, saving time and preventing errors
- staff can deal with queries and deliver a better standard of service as a result of sharing customer data

Cost benefits of computer networking

Storing information in one centralized database can also help you reduce costs and drive efficiency. For example:

- staff can deal with more customers in less time since they have shared access to customer and product databases
- you can centralize network administration, meaning less IT support is required
- you can cut costs through sharing of peripherals and internet access

You can reduce errors and improve consistency by having all staff work from a single source of information. This way, you can make standard versions of manuals and directories available to them, and back up data from a single point on a scheduled basis, ensuring consistency

- **Content/Topic 2: Classification of Network**

- ✓ **Classifying network by components roles**

Based on network components, there two classification of computer network which are the following:

Client-Server Network: This model is broadly used network model. In Client-Server Network, Clients and server are differentiated, specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized. In Client-Server Network, Server respond the services which is request by Client.

Peer-to-Peer Network: This model does not differentiate the clients and the servers, in this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover.

- ✓ **Classifying network by geographical area**

Local Area Network (LAN) –LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc.

Metropolitan Area Network (MAN) –MAN or Metropolitan Area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart

but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN) –WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

- **Content/Topic 3: Introduction to Network Technologies**

Networking technology allows for the exchange of data between large and small information systems used primarily by businesses and educational institutions. Network technicians, also known as network engineers or specialists, are responsible for the configuration, installation and troubleshooting of the technology used to transmit digital information, including audio, visual and data files. Through networking, end-users are able to transmit files, messages and other data through e-mail or various other channels, sharing information through Internet or Intranet connections, based on the needs of an organization.

- ✓ **IEEE802.3 Ethernet**

Ethernet Operation

Ethernet is the most widely used LAN technology used today.

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10,000 Mb/s (10 Gb/s)
- 40,000 Mb/s (40 Gb/s)
- 100,000 Mb/s (100 Gb/s)

Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. For the Layer 2 protocols, as with all 802 IEEE standards, Ethernet relies on the two separate sub layers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sub layers.

✓ IEEE 802.5 Token ring

The foundation of a token ring is the IEEE 802.5 network of the “Institute of Electrical and Electronics Engineers” from 1985, in which all participants of the “Local Area Network” (LAN) are connected to form a logical ring. Usually token ring topologies have a transmission speed of 4 or 16 Mbit/s, but in theory speeds of 100 Mbit/s or 1 Gbit/s are also possible.

A token ring works somewhat differently to other ring topologies, which is why it’s said that this technology is based only logically on a ring topology. The token ring topology uses **Multistation Access Units (MAUs)**, which allow a star-shaped connection of the connections involved. The distributor is a node that is connected to all computers on the network. There is no direct connection between the individual computers.

Nevertheless, there is still a logical ring involved, which is due to the **physical star structure**, because the data transmission takes the form of a ring – on an abstract level. Although the data is repeatedly transported to the MAU, it is not sent from there to a specified subscriber, but simply to the next computer in the fixed sequence.

Token passing

To avoid chaos, the token passing procedure is used. This method ensures that not all participants send data to the network at the same time. Only computers that are currently in possession of the token have the right to send data packets to the network. This token is passed on in a ring – even if no participant requires a transmission permit, the token continues to circulate. A token is an empty frame of 3 bytes in size, each byte having a separate task:

- **Third byte** – start delimiter (SD): The first 8 bits of the frame indicate the beginning of the token. The structure is based on the differential Manchester code, which allows a clear assignment.
- **Second byte** – access control (AC): The access control contains the token bit. If this is set to 0, the token is free, 1 indicates that it is busy.
- **First byte** – end delimiter (ED): The design of the end delimiter is similar to the start delimiter and makes it clear that the frame is complete.

If a participant receives the frame and does not want to send any information, they simply pass it on to the next in the row. However, if the computer wants to send something, it changes the token bit and **attaches the data package to the token**.

✓ IEEE802.8 Fiber optic

This is the technology of IEEE that introduced the use of Fiber Optic cable that enables an Internet service provider to provide higher bandwidth speeds and support more services such as Internet, phone, and TV in large distance.

✓ IEEE802.11 Wireless

802.11 and 802.11x refers to a family of specifications developed by the IEEE for **wireless LAN (WLAN)** technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family:

- **802.11** — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11e** — a wireless draft standard that defines the **Quality of Service (QoS)** support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds

QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.

- **802.11g** — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
- **802.11n** — 802.11n builds upon previous 802.11 standards by adding **multiple-input multiple-output (MIMO)**. The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.
- **802.11ac** — 802.11ac, or Wi-Fi 5, builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beam forming capabilities by default to help achieve its higher wireless speeds.
- **802.11ac Wave 2** — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.
- **802.11ad** — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).
- **802.11ah** — Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.
- **802.11r** - 802.11r, also called Fast **Basic Service Set (BSS)** Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.
- **802.1X** — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.
- **802.11ax**, or Wi-Fi 6, improves on Wi-Fi 5 with more speed, bandwidth and security.

LO1.2. Description of Network topology

- **Content/Topic 1: Description of Network topology**

A network topology is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected. A topology of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others. Admins have a range of options when it comes to choosing a network topology, and this decision must account for the size and scale of their business, its goals, and budget.

- **Types of Network Topology**

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. Ask yourself a question “What is network topology?” This question can be answered with an explanation of the two categories in the network topology.

1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical** – The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Types of Physical Network Topology

There are six types of topology in computer networks:

1. **BUS Topology**

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

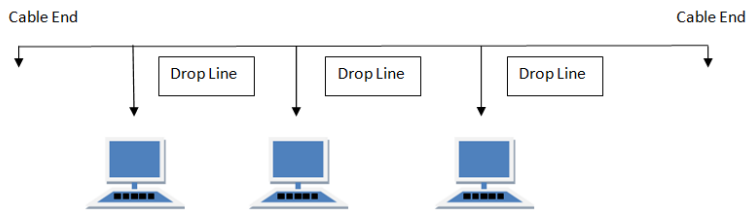


Fig.1: Bus topology

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

2. RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

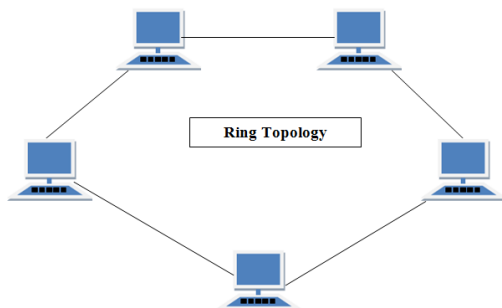


Fig.2: Star topology

Features of Ring Topology

- ✓ A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- ✓ The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
- ✓ In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- ✓ Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

- ✓ Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- ✓ Cheap to install and expand

Disadvantages of Ring Topology

- ✓ Troubleshooting is difficult in ring topology.
- ✓ Adding or deleting the computers disturbs the network activity.
- ✓ Failure of one computer disturbs the whole network.

1. STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

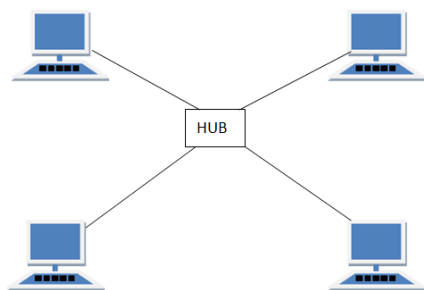


Fig.3: Star topology

Features of Star Topology

- ✓ Every node has its own dedicated connection to the hub.
- ✓ Hub acts as a repeater for data flow.
- ✓ Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

- ✓ Fast performance with few nodes and low network traffic.
- ✓ Hub can be upgraded easily.
- ✓ Easy to troubleshoot.
- ✓ Easy to setup and modify.
- ✓ Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

- ✓ Cost of installation is high.
- ✓ Expensive to use.
- ✓ If the hub fails, then the whole network is stopped because all the nodes depend on the hub.
- ✓ Performance is based on the hub that is it depends on its capacity

4. MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has $n(n-1)/2$ physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

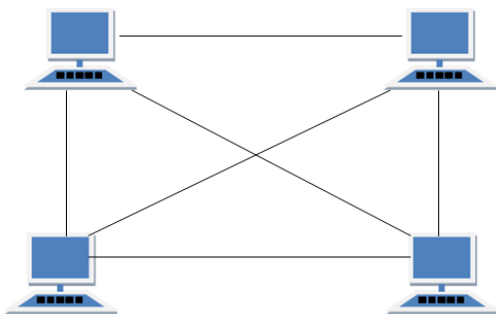


Fig.4: Mesh topology

Features of Mesh Topology

- ✓ Fully connected.
- ✓ Robust.
- ✓ Not flexible.

Advantages of Mesh Topology

- ✓ Each connection can carry its own data load.
- ✓ It is robust.
- ✓ Fault is diagnosed easily.
- ✓ Provides security and privacy.

Disadvantages of Mesh Topology

- ✓ Installation and configuration is difficult.
- ✓ Cabling cost is more.
- ✓ Bulk wiring is required.

5. TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

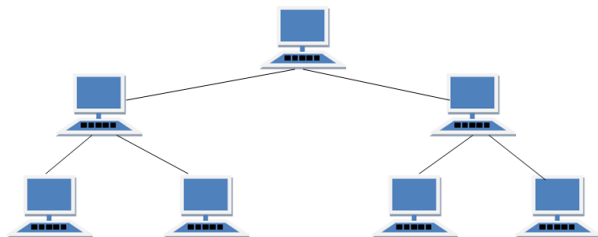


Fig.5: Tree topology

Features of Tree Topology

- ✓ Ideal if workstations are located in groups.
- ✓ Used in Wide Area Network.

Advantages of Tree Topology

- ✓ Extension of bus and star topologies.
- ✓ Expansion of nodes is possible and easy.
- ✓ Easily managed and maintained.
- ✓ Error detection is easily done.

Disadvantages of Tree Topology

- ✓ Heavily cabled.
- ✓ Costly.
- ✓ If more nodes are added maintenance is difficult.
- ✓ Central hub fails, network fails.

6. HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

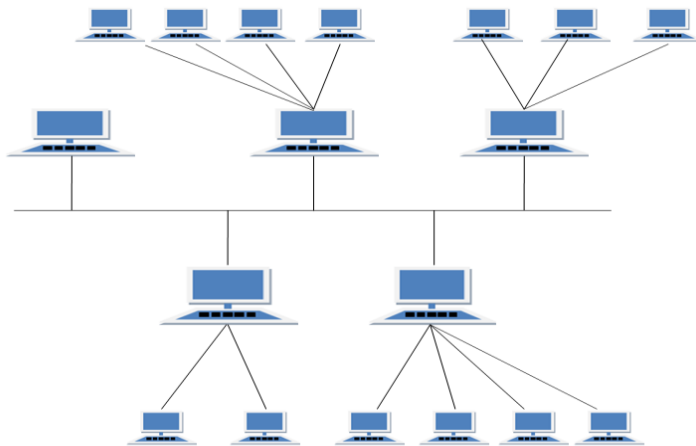


Fig.6: Hybrid topology

Features of Hybrid Topology

- ✓ It is a combination of two or more topologies
- ✓ Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

- ✓ Reliable as Error detecting and trouble shooting is easy.
- ✓ Effective.
- ✓ Scalable as size can be increased easily.
- ✓ Flexible.

Disadvantages of Hybrid Topology

- ✓ Complex in design.
- ✓ Costly.

LO1.3. Identification of Network devices, Components and their Functions

- **Content/Topic 1 Classification of Network Devices**

There are different types of electronic devices are used in networking which are known as network devices or network equipment. In a computer network, network devices are mainly used for transmitting and receiving the data quickly and securely in between computers, fax machines, printers, etc. These devices may be intra network or internetwork. There are three classes of network devices which are:

- Interconnection devices
- Access devices
- End devices
- ✓ **Interconnection devices**

Interconnection device is any device that can enable computers to exchange data on a network. The function of interconnection devices and examples of interconnection devices on networks are explained below:

Repeater

Repeaters are non-intelligent network devices that receive a signal through one port. They regenerate that signal and then transmit the signal again on all remaining ports. To extend the length of a network, repeaters can be used to connect network segments (a portion of a computer network) but they can't be used to connect different networks using different access methods. Repeaters reduce the loss of signal along a cable (known as attenuation) which in turn provides a more stable connection to the devices connected the repeater.

Bridge

Unlike repeaters, a bridge can extend the capacity as well as the length of a network because each port on a bridge has a MAC address. They are used to connect two or more LANs of the same type, e.g. Ethernet to Ethernet. When activating a bridge on an Ethernet network, they automatically start to capture and analyse addresses of incoming frames, building up a routing table and learning the topology of the network. Because bridges learn about the network, they are considered intelligent devices and can manage traffic, resulting in reduced bandwidth and a more efficient flow of data on a network.

Switch

The switch has replaced a lot of hubs and bridges in Local Area Networks as it's considered a more intelligent device, improving network performance and reducing the chances of errors occurring on a network. A switch keeps a record of all MAC address connected to it so it can then identify which device is connected to which port. When a frame is received, it then looks at the destination MAC address and knows exactly which port to send the data on to. It doesn't just send the data out on all ports like a hub does.

Switches also allocate full bandwidth to all ports so if a switch is 10/100Mbps, all ports are allocated 10/100Mbps speed. This is not the case with the hub where that bandwidth is shared across all ports. They can be used to link a number of end-user devices (e.g. workstations) or they can also interconnect multiple network segments.

Router

If a network has a number of sub-networks (segments) that use different networking protocols and architectures, it requires a sophisticated device to manage the data flow. This device is known as a router which determines how incoming packets get to destination networks in the most efficient way possible. Routers can communicate information about their network with routers on different networks and they store information in a routing table.

Routers are located at the edge of networks (known as gateways) which is the point at which two or more networks connect. For example, your home router connects to your ISP. Your home router manages traffic and devices in your home while simultaneously talking to your ISP and ensuring data is sent and received efficiently.

✓ Access devices

Network access device is any device that help a user (end device) to get connected on a network.

Network Interface Card (NIC)

A NIC is also known as a network adapter. Any device that wants to communicate and send / receive data must have a NIC installed. They are usually located in a computer's expansion slot, similar to how you'd see a graphics card or sound card installed. The NIC contains a transceiver which is a combination of a transmitter and receiver. This facilitates data transmission, enabling the device to

send and receive data. The NIC also contains a MAC address (also known as a hardware address) which is a unique, 48-bit identifier used by many networking protocols including Ethernet and 802.11 wireless. A MAC address looks something like this: 65:85:45: F2:C3:8E

Hub

Hubs are used in Ethernet networks to connect multiple Ethernet devices together, forming a network segment (group of computers that is a portion of a network). A hub, like a repeater has no intelligence so simply broadcasts all network data across all ports. However, most hubs can detect basic errors such as collision and because every computer connected to the hub has its own dedicated connection to the hub, this means that if there is a connection failure, it only affects a single device and not the entire hub and all of its associated connections / devices.

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.

✓ End devices

Network devices that people are most familiar with are called end devices. All computers connected to a network that participate directly in network communication are classified as hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are:

- computers (workstations, laptops, file servers, and web servers)
- network printers
- VoIP phones
- TelePresence endpoints
- security cameras

- Mobile handheld devices (smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners) sensors such as thermometers, weight scales etc...
- **Content/Topic 2: Description of network components**

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves. Network components are used to provide services and processes.

Here are the main categories of network components:

✓ **Media**

Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

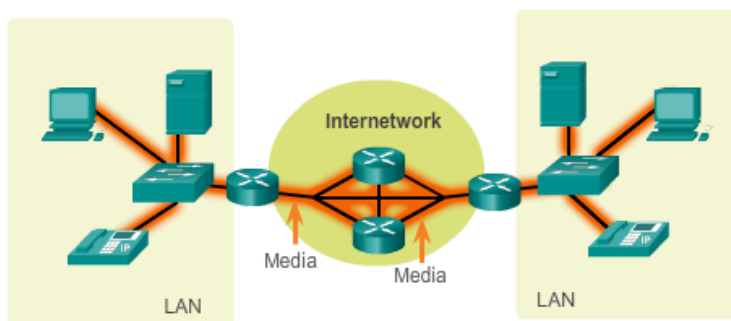


Fig.8: Network component/ Media

✓ **Message**

In general, a message is any grouping of information at the application layer (layer 7) of the Open Systems Interconnection (OSI) reference model that is exchanged between applications for various purposes.

✓ **Protocol**

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

✓ **Devices**

The devices which are used for communication between different hardware's used in the computer network are known as network devices. These devices are also known as physical devices, networking hardware, and network equipment otherwise computer networking devices. In a computer network, each network device plays a key role based on their functionality, and also works for different purposes at different segments.

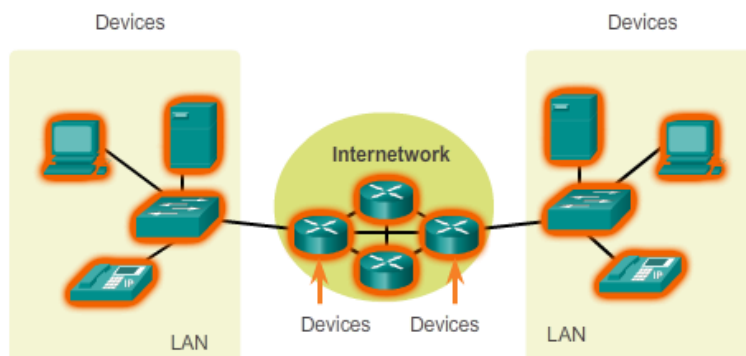


Fig.7: Network component/ Device

Here are the common network devices:

- **Router:** A network router is one kind of network device in a computer network and it is used for routing traffic from one network to another by using different network topologies. Routers are intelligent devices, and they store information about the networks they're connected to. Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing. This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.
- **Hubs:** Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.
- **Switch:** Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.
- **NIC:** A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface) is a computer hardware component that connects a computer to a computer network.
- **Repeater:** A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.
- **MAU:** A media access unit (MAU), also known as a multi-station access unit (MAU or MSAU), is a device to attach multiple network stations in a star topology as a token ring network, internally wired to connect the stations into a logical ring (generally passive i.e. non-switched and unmanaged; however managed token ring MAUs do exist in the form of CAUs, or Controlled Access Units).

- **Firewall:** A firewall is a security device such as computer hardware or software that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

- **Access points:** While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.
- **Antenna:** Also called an aerial, an antenna is a conductor that can transmit, send and receive signals such as microwave, radio or satellite signals. A high-gain antenna increases signal strength, where a low-gain antenna receives or transmits over a wide angle.
- **Gateways:** Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

Learning Unit 2: Network protocols and communications

LO2. 1. Description of network protocols

- **Content/Topic 1 Introduction to network protocols**

Just like in human communication, the various network and computer protocols must be able to interact and work together for network communication to be successful. A group of inter-related protocols necessary to perform a communication function is called a protocol suite. Protocol suites are implemented by hosts and networking devices in software, hardware or both.

One of the best ways to visualize how the protocols within a suite interact is to view the interaction as a stack. A protocol stack shows how the individual protocols within a suite are implemented. The protocols are viewed in terms of layers, with each higher level service depending on the functionality defined by the protocols shown in the lower levels. The lower layers of the stack are concerned with moving data over the network and providing services to the upper layers, which are focused on the content of the message being sent. As the figure shows, we can use layers to describe the activity occurring in our face-to-face communication example. At the bottom layer, the physical layer, we have two people, each with a voice that can say words out loud. At the second layer, the rules layer, we have an agreement to speak in a common language. At the top layer, the content layer, there are words that are actually spoken. This is the content of the communication.

Were we to witness this conversation, we would not actually see layers floating in space. The use of layers is a model that provides a way to conveniently break a complex task into parts and describe how they work.

At the human level, some communication rules are formal and others are simply understood based on custom and practice. For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. Networking protocols define a common format and set of rules for exchanging messages between devices.

- **The most common network protocols**
 - ✓ **NetBEUI**

NetBEUI stands for NetBIOS Extended User Interface, is a networking protocol developed by IBM and Microsoft in 1985 that is used for workgroup-size local area networks (LANs) with up to 200 stations. NetBEUI is an extension of the NetBIOS protocol.

NetBEUI was the primary protocol for LAN Manager and Windows for Workgroups. It is a fast and efficient protocol with low overhead that supports both connection-oriented communication (such as communication for mapping drives using the Net Use command and starting services remotely using the Net Start command) and connectionless communication (such as communication for sending datagrams, registering NetBIOS names, and performing NetBIOS name resolution).

✓ **AppleTalk**

It is Apple Computer's LAN protocol. It is built into every Macintosh computer and facilitates communications between a variety of Apple and non-Apple products linked on LANs. AppleTalk includes a number of features that allow local area networks to be connected with no prior setup or the need for a centralized router or server of any sort. Connected AppleTalk-equipped systems automatically assign addresses, update the distributed namespace, and configure any required inter-networking routing.

✓ **Transport Protocol**

Transmission Control Protocol (TCP) is the transport protocol that manages the individual conversations between web servers and web clients. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.

✓ **Internet Protocol**

IP is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them across the best path to the destination host.

✓ **Application Protocol**

Hypertext Transfer Protocol (HTTP) is a protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged

between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.

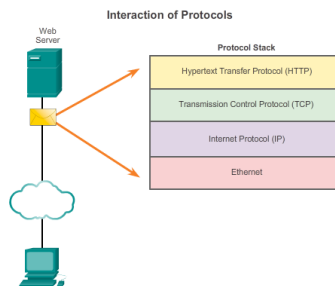


Fig.10: Interaction of protocols

Reference Models

A layered model, such as the TCP/IP model, is often used to help visualize the interaction between various protocols. A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction of protocols with the layers above and below each layer.

There are benefits to using a layered model to describe network protocols and operations. Using a layered model:

- Assists in protocol design, because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
- Fosters competition because products from different vendors can work together.
- Prevents technology or capability changes in one layer from affecting other layers above and below.
- Provides a common language to describe networking functions and capabilities.

There are two basic types of networking models:

- **Protocol model** - This model closely matches the structure of a particular protocol suite. The hierarchical set of related protocols in a suite typically represents all the functionality required

to interface the human network with the data network. The TCP/IP model is a protocol model, because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

- **Reference model** - This model provides consistency within all types of network protocols and services by describing what has to be done at a particular layer, but not prescribing how it should be accomplished. A reference model is not intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes involved.

The OSI model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

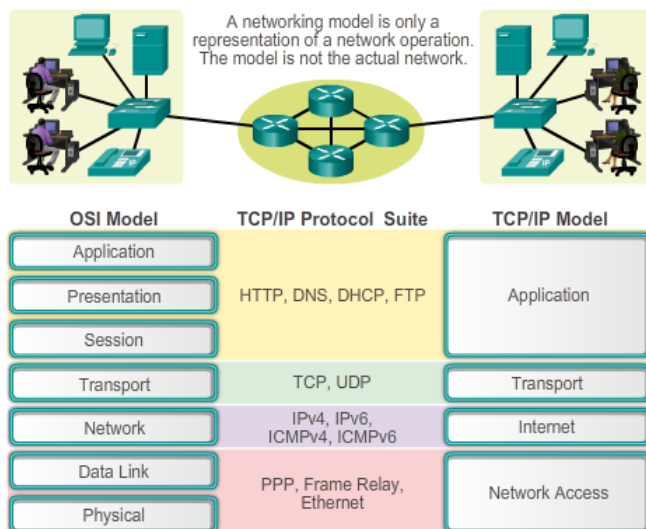


Fig .11: OSI and TCP/IP Models

As shown in the figure, the TCP/IP and OSI models are the primary models used when discussing network functionality. Designers of network protocols, services, or devices can create their own models to represent their products. Ultimately, designers are required to communicate to the industry by relating their product or service to either the OSI model or the TCP/IP model, or to both.

✓ **Novell netware(IPX/SPX)**

IPX is a Novell NetWare protocol used for routing packets from one network node to another throughout an internetwork. Internetwork Packet Exchange (IPX) is a network layer protocol and

provides connectionless datagram services for Ethernet, Token Ring, and other common data-link layer protocols. IPX is the commonly used local area network (LAN) protocol on legacy NetWare-based LANs but has recently been replaced with TCP/IP for NetWare 5.x.

- **Description of IP Terminologies**

IP Address is a key function of network layer protocols that enables data communication between hosts, regardless of whether the hosts are on the same network or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data. The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks.

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

LO2.2. Description of Network standards

- **Content/Topic 1: Importance of Network standard**

Standards are necessary in almost every business and public service entity. The primary reason for standards is to ensure that hardware and software produced by different vendors can work together. Without networking standards, it would be difficult, if not impossible, to develop networks that easily share information. Standards also mean that customers are not locked into one vendor. They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices. The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

- **Internet standards**

A **standard** is a set of rules or guidelines approved and monitored by an authorized organization. An internet standard (STD) is a specification that has been approved by the Internet Engineering Task Force (IETF). Such standard helps to promote a consistent and universal use of the internet worldwide. There are regulated standards such as those published by the International Telecommunication Union (ITU), the American National Standards Institute (ANSI), and the Institute of Electrical and Electronics Engineers (IEEE). There are also de facto standards, such as those put forth by network vendors, such as Cisco, and adopted over time by everyone else.

ITU (International Telecommunication Union)

The International Telecommunication Union (ITU) is made up of telecommunication policy makers and regulators, network operators, equipment manufacturers, hardware and software developers, regional standards-making organizations, and financing institutions. The activities, policies, and strategic direction of the ITU are determined and shaped by the industry it serves.

There are three sectors of the ITU which are Radiocommunication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D). Each of the three ITU sectors works through conferences and meetings at which members negotiate the agreements that serve as the basis for the operation of global telecommunication services. The activities of the ITU cover all aspects of telecommunication: setting standards that facilitate seamless interworking of equipment and systems on a global basis; adopting operational procedures for the vast and growing array of wireless services; and designing programs to improve telecommunication infrastructure in the developing world.

ANSI (American National Standards Institute)

American National Standards Institute (ANSI) serves as administrator and coordinator of the United States private-sector voluntary standardization system. ANSI was founded in 1918 by five engineering societies and three governmental agencies, and is a private, nonprofit membership organization. ANSI ensures each foot-long ruler is accurate in its dimensions, for instance, essentially using a ruler to measure a ruler. ANSI ensures that each inch on the ruler is in fact 1 inch, and that the foot-long ruler is in fact made up of 12 of these inches.

ANSI, like the ITU, regulates telecommunications standards; unlike the ITU, however, ANSI regulates standards in North America, whereas the ITU regulates standards in Europe. For example, ANSI

regulates the T1 telecommunications standard, whereas the ITU regulates the E1 telecommunications standard in Europe.

IEEE 802 Group

The Institute of Electrical and Electronics Engineers (IEEE, pronounced "eye-triple-E") is a nonprofit, technical professional association in 150 countries. The IEEE is a leading authority in technical areas ranging from computer engineering, to biomedical technology, to telecommunications, to electric power, to aerospace and consumer electronics. The IEEE produces 30 percent of the world's published literature in electrical engineering, computers, and control technology and has nearly 900 active standards with 700 under development.

Some of the best-known IEEE standards are as follows:

- IEEE 802.1 (LAN/MAN)
- IEEE 802.3 (Ethernet)
- IEEE 802.5 (Token Ring)
- IEEE 802.11 (Wireless LAN)

- **Types of standards**

De Facto standards: A format, or protocol that has become a standard not because it has been approved by a standards organization but because it is widely used and recognized by the industry as being standard. Examples of de facto standards include but not limited to: the QWERTY keyboard, the Windows operating system and breadcrumb trail technology; a navigation aid used when moving through a website that indicates the current page in relation to the website's remaining pages.

De Jure standards: De jure standards are those which have been approved by formal authorities like the Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO). These standards are critically assessed before being approved. An example of a de jure standard is the **ASCII** character set. Some de jure hardware standards include **USB**, **FireWire** and **HDMI**.

- **Content/Topic 2: Description of Standards organizations**

Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards.

Standards organizations include:

- ✓ **ISOC:** Short for International Organization for Standardization. Note that ISO is not an acronym; instead, the name derives from the Greek word iso, which means equal. Founded in 1946, ISO is an international organization composed of national standards bodies from over 75 countries. For example, ANSI (American National Standards Institute) is a member of ISO. ISO has defined a number of important computer standards, the most significant of which is perhaps OSI (Open Systems Interconnection), a standardized architecture for designing networks.
- ✓ **IEEE:** The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) is an organization within IEEE that develops global standards in a broad range of industries, including: power and energy, consumer technology and consumer electronics, biomedical and health care, learning technology, information technology and robotics, telecommunication and home automation, transportation, nanotechnology, information assurance, and many more. IEEE-SA has developed standards for over a century, through a program that offers balance, openness, fair procedures, and consensus. Technical experts from all over the world participate in the development of IEEE standards. IEEE-SA is not a body formally authorized by any government, but rather a community. ISO, IEC and ITU are recognized international standards organizations.

Some of the best-known IEEE standards are as follows:

- ✓ **ANSI:** American National Standards Institute is an organization that facilitates and governs the development of standards in many areas, including computing and communication. The American National Standards Institute (ANSI) was founded as a private sector voluntary standards association in 1918 and is a nonprofit, private association with almost 1400 member organizations.

Standards that are approved by ANSI are called ANSI Standards. Examples include the ANSI C/C++ programming language standards, ANSI-89 SQL standards, and ANSI character set.

- ✓ **ITU-Formally CCITT:** The standardization efforts of ITU started in 1865 with the formation of the International Telegraph Union (ITU). ITU became a specialized agency of the United Nations in 1947. The International Telegraph and Telephone Consultative Committee (French: Comité Consultatif International Téléphonique et Télégraphique, CCITT) was created in 1956, and was renamed ITU-T in 1993.

There are three sectors of the ITU which are Radio communication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D). Each of the three ITU sectors works through conferences and meetings at which members negotiate the agreements that serve as the basis for the operation of global telecommunication services. The activities of the ITU cover all aspects of telecommunication: setting standards that facilitate seamless interworking of equipment and systems on a global basis; adopting operational procedures for the vast and growing array of wireless services; and designing programs to improve telecommunication infrastructure in the developing world.

- ✓ **EIA:** Founded in 1924, the EIA is a U.S. organization of electronics manufacturers. The EIA has published a number of standards related to telecommunication and computer communication, and works closely with other associates such as ANSI and the ITU. The primary EIA standards for telecommunication define the serial interface between modems and computers. The most popular are the RS-232-C, RS-449, RS-422, and RS-423 serial interfaces. The physical layer specifications define 37-pin (DB-37), 25-pin (DB-25), and 9-pin (DB-9) connectors and associated cable, as well as electrical characteristics such as the type of signal used on each pin and the timing of those signals.
- ✓ **Telcordia:** Is a standard uses a series of models for various categories of electronic, electrical and electro-mechanical components to predict steady-state failure rates which environmental conditions, quality levels, electrical stress conditions and various other parameters affect.

LO2.3. Identification and application of Network media and connectors

- **Content/Topic1: Introduction to network media**

Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

- **Types of Network Media**

- ✓ **Logical (Wireless)**

The term logical media is used to refer to any type of electrical or electronic operation which is done without the use of “hard wired” connections. It is also referred to as Wireless or unbounded transmission media.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Signals transmitted through logical media:

- **Radio waves**

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3 KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

- **Microwaves**

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

- **Infrared**

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

✓ **Physical**

Physical media refers to the physical materials that are used to transmit information in data communications. These physical media are generally physical objects made of materials such as copper or glass. They can be touched and felt, and have physical properties such as weight and color.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

➤ Coaxial cable

Coaxial cable, or coax as it is commonly referred to, has been around for a long time. Coax found success in both TV signal transmission as well as in network implementations. Coax is constructed with a copper core at the center that carries the signal, plastic insulation, braided metal shielding, and an outer plastic covering. Coaxial cable is constructed in this way to add resistance to attenuation (the loss of signal strength as it travels over distance), crosstalk (the degradation of a signal caused by signals from other cables running close to it), and EMI (electromagnetic interference).

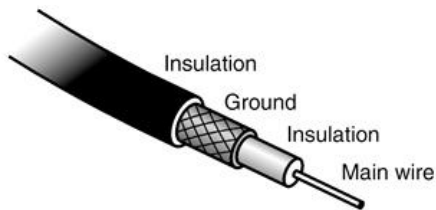


Fig.14: Construction of coaxial cabling

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantage: Single cable failure can disrupt the entire network

There are two types of coaxial cabling.

- **Thinnet** is used for short-distance. The maximum length of thinnet is 185 meters
 - **Thicknet**. It supports data transfer over longer distances than thinnet. The maximum length of thinnet is 500 meters
- **Twisted pair:** Twisted-pair cabling has been around a very long time. It was originally created for voice transmissions and has been widely used for telephone communication. Today, in addition to telephone communication, twisted pair is the most widely used media for networking.

The popularity of twisted pair can be attributed to the fact that it is lighter, more flexible, and easier to install than coaxial or fiber-optic cable. It is also cheaper than other media alternatives and can achieve

greater speeds than its coaxial competition. These factors make twisted pair the ideal solution for most network environments.

- **UTP:** stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference.

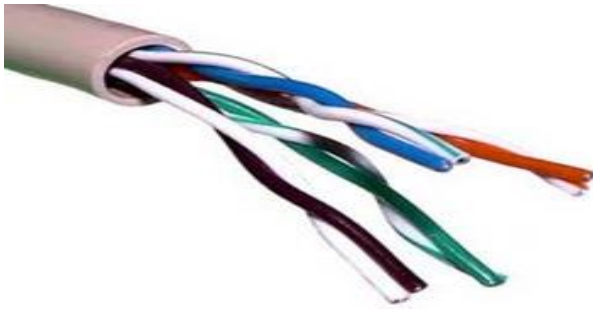


Figure: UTP Cable

- **STP:** Is a type of copper telephone wiring in which each of the two copper wires that are twisted together are coated with an insulating coating that functions as a ground for the wires. The extra covering in shielded twisted pair wiring protects the transmission line from electromagnetic interference leaking into or out of the cable. STP cabling often is used in Ethernet networks, especially fast data rate Ethernets.

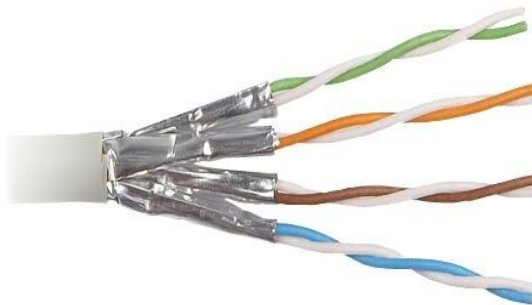


Fig.13: STP and UTP cables

- **ScTP:** Screened twisted-pair (ScTP) cabling is a hybrid of UTP and STP cable. ScTP cable typically consists of four pairs of 100 ohm, 24 AWG wire that are unshielded, but surrounded by a shield of foil and includes a single drain wire used for grounding.

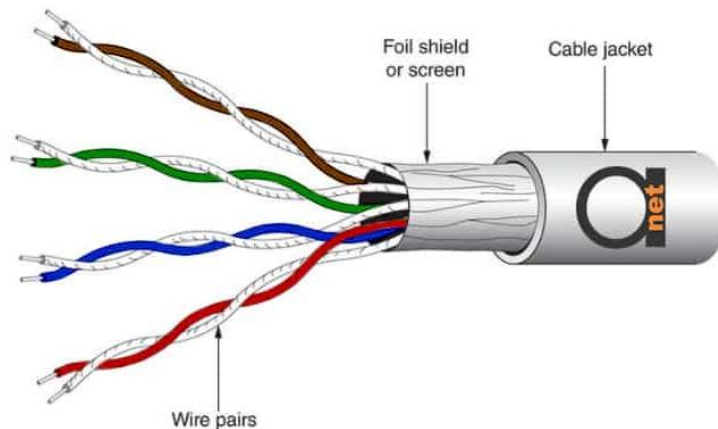


Figure: Screened twisted-pair (ScTP)

ScTP is therefore also called FTP (foil twisted-pair), as a foil shield surrounds the conductors. The foil shield is typically smaller than the woven copper braided jacket used by STP cabling systems. ScTP cable is basically STP cabling without the individual pairs being shielded. The shield is also often smaller than some types of STP cabling.

ScTP is less susceptible to noise because of the foil shield.

When implementing an effective ScTP system however, the shield's continuity should be kept through the whole channel, including wall plates, patch panels and patch cords.

Advantages:

- Cheaper and far easier to splice
- Less susceptible to electrical interference caused by nearby equipment or wires.
- In turn are less likely to cause interference themselves.
- Because it is electrically "cleaner", STP wire can carry data at a faster speed.

Disadvantages:

- STP wire is that it is physically larger and more expensive than twisted pair wire.

- STP is more difficult to connect to a terminating block.

➤ **Fiber optic**

A fiber-optic cable, also known as an optical-fiber cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed.

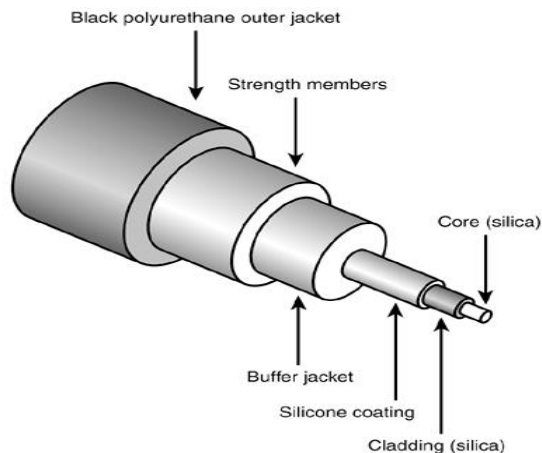


Fig.15: Composition of a fiber-optic cable

In many ways, fiber-optic media addresses the shortcomings associated with copper-based media. Because fiber-based media use light transmissions instead of electronic pulses, threats such as EMI, crosstalk, and attenuation become a nonissue. Fiber is well suited for the transfer of data, video, and voice transmissions. In addition, fiber-optic is the most secure of all cable media. Anyone trying to access data signals on a fiber-optic cable must physically tap into the media. Given the composition of the cable, this is a particularly difficult task.

Unfortunately, despite the advantages of fiber-based media over copper, it still does not enjoy the popularity of twisted-pair cabling. The moderately difficult installation and maintenance procedures of fiber often require skilled technicians with specialized tools. Furthermore, the cost of a fiber-based solution limits the number of organizations that can afford to implement it. Another sometimes hidden drawback of implementing a fiber solution is the cost of retrofitting existing network equipment. Fiber is incompatible with most electronic network equipment. This means that you have to purchase fiber-compatible network hardware.

Advantages:

- ✓ One single mode fiber can replace a metal of time larger and heavier.
- ✓ Multi-mode optical cable has a larger diameter and can be used to carry signal over short distance.

Disadvantages:

- ✓ Fiber optic versus metal cable is that it is difficult to make connections to fiber optic cable.
- ✓ The optical fiber must be highly polished to allow light to pass with little loss.

Types of fiber optic cable

▪ Single-Mode Fiber Optic Cable

Businesses that need to enhance their network's capability to perform long distance communication needs a single mode fiber optic cable. This cable has the smallest core and the thickest sheathing, specifically designed to carry a single signal source over great distances with a low chance of failure. Its small diametric core allows one mode of light to promulgate, causing the number of light reflections it creates to decrease. And as the light that passes through the core decreases, its attenuation lowers. Because of that, the signal this cable transmits is enabled to travel further, making it excellent for businesses that require long distance communication.

▪ Multimode Fiber Optic Cable

In contrast with the single-mode fiber optic cable, multimode fiber optic cables are capable of carrying multiple signals. Its large diametrical core is designed to enable multiple modes of light to promulgate. And, as it passes through the core, it creates more light reflections, unlike the single-mode cable. Although it can transfer data in a shorter distance, it enables the computer network to transfer more data at any given time. That being said, if your company needs to transmit more data, multimode fiber optic cable is what you need.

- **Content/Topic 2: Description of network connectors' types**

A variety of connectors are used with the associated network media. Media connectors attach to the transmission media and allow the physical connection into the computing device. It is necessary to identify the connectors associated with the specific media. The following sections identify the connectors and associated media.

BNC Connectors: BNC connectors are associated with coaxial media and 10Base2 networks. BNC connectors are not as common as they once were, but still are used on some networks, older network cards, and older hubs. Common BNC connectors include a barrel connector, T-connector, and terminators.



Fig.16: Two terminators (top and bottom) and two T-connectors (left and right)

RJ11connectors: RJ (Registered Jack) -11 connectors are small plastic connectors used on telephone cables. They have capacity for six small pins. However, in many cases, not all the pins are used. For example, a standard telephone connection only uses two pins, while a cable used for a DSL modem connection uses four.

RJ-11 connectors are somewhat similar to RJ-45 connectors, which are discussed next, though they are a little smaller. Both RJ-11 and RJ-45 connectors have small plastic flange on top of the connector to ensure a secure connection. Figure 5 shows two views of an RJ-11 connector.

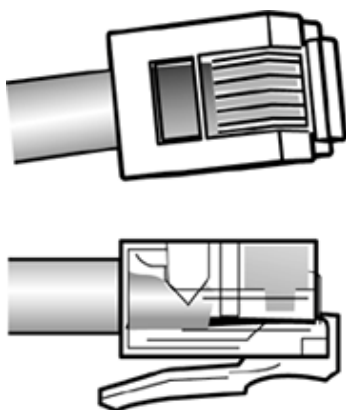


Fig.17:RJ-11 connectors

RJ-45 Connectors: RJ-45 connectors are the ones you are most likely going to encounter in your network travels. RJ-45 connectors are used with twisted-pair cabling, the most prevalent network cable in use today. RJ-45 connectors resemble the aforementioned RJ-11 phone jacks, but support up to eight wires instead of the six supported by RJ-11 connectors. RJ-45 connectors are also larger. Figure 6 shows the RJ-45 connectors.

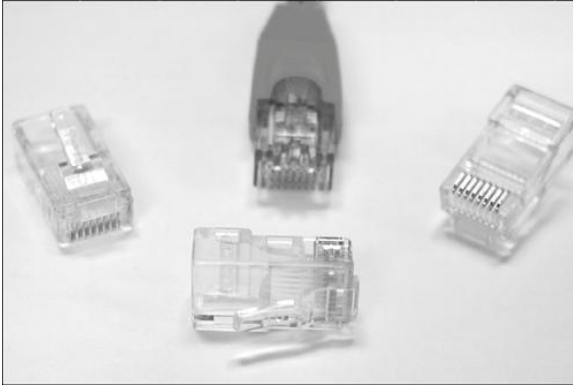


Fig.18: RJ-45 connectors

F-Type connectors: F-Type connectors are screw on connections used for attaching coaxial cable to devices. In the world of modern networking, F-Type connectors are most commonly associated with connecting Internet modems to cable or satellite Internet provider's equipment. However, they are also used for connecting to some proprietary peripherals.

F-Type connectors have a 'nut' on the connection that provides something to grip as the connection is tightened by hand. If necessary, this nut can be also being lightly gripped with pliers to aid disconnection.

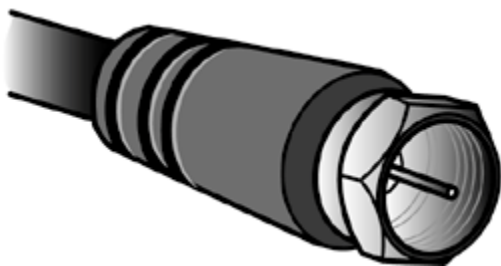


Fig.19: An example of an F-Type connector

Fiber Connectors: a variety of connectors are associated with fiber cabling, and there are several ways of connecting these connectors. These include bayonet, snap-lock, and push-pull connectors.

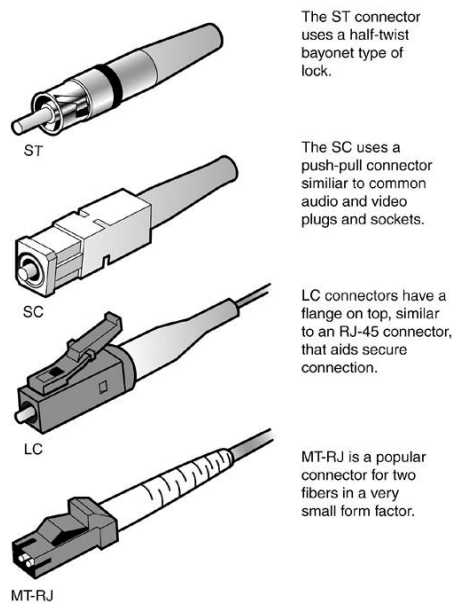


Fig.20: Different fiber connectors

VGA connector: A Video Graphics Array (VGA) connector is a standard connector used for computer video output. It is a three-row, 15-pin D-sub miniature connector referred to variously as DE-15, HD-15 or DB-15. DE-15 is the most accurate common nomenclature under the D-sub specifications: an "E" size D-sub connector, with 15 pins in three rows.

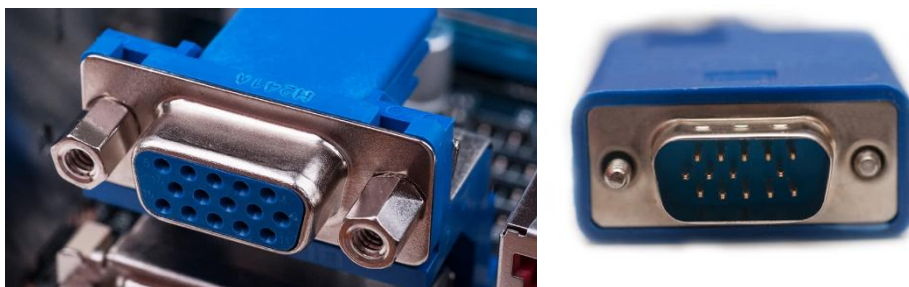


Fig.21: VGA Male and Female connectors

USB connector: A universal serial bus (USB) connector is a connector between a computer and a peripheral device such as a printer, monitor, scanner, mouse or keyboard. It is part of the USB interface, which includes types of ports, cables and connectors. The USB connector was developed to simplify the connection between computers and peripheral devices. Prior to the USB interface,

peripheral devices had a multitude of connectors. The USB interface provides various benefits, including plug-and-play, increased data transfer rate (DTR), reduced number of connectors, and addressing usability issues with existing interfaces.

Firewire Connectors: External connector, similar to a USB port, that provides a high-speed connection between a computer and peripheral devices. Firewire was developed by Apple, Inc. and is based off the standard IEEE 1394 high performance serial bus. Firewire ports are able to transfer data at a rate of up to 400 Mbps. This technology was once standard on computers manufactured by Apple, Inc., but has since been replaced by Thunderbolt ports and later versions of USB ports.



Fig.22: Different firewire connectors

Serial Port/Connector: A serial port is an interface that allows a PC to transmit or receive data one bit at a time. It is one of the oldest types of interfaces and at one time was commonly used to connect printers and external modems to a PC. Modern serial ports are used in scientific instruments, shop till systems such as cash registers and applications like industrial machinery systems.



Fig.23: Serial port

MT-RG

MT-RG Connector: **MT-RJ** stands for Mechanical Transfer Registered Jack. **MT-RJ** is a fiber-optic Cable **Connector** that is very popular for small form factor devices due to its small size. Housing two fibers and mating together with locating pins on the plug.

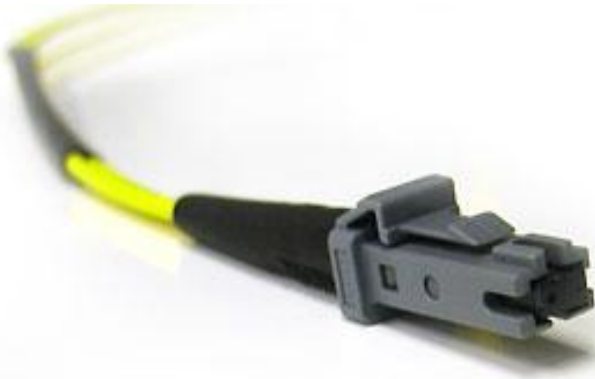


Figure: Fiber optic cable connector

RS-232

RS232 is a standard protocol used for serial communication, it is used for connecting computer and its peripheral devices to allow serial data exchange between them. As it obtains the voltage for the path used for the data exchange between the devices. It is used in serial communication up to 50 feet with the rate of 1.492kbps.

RS-232 Connector is a type of connector used for serial communication standard that provides asynchronous and synchronous communication capabilities.

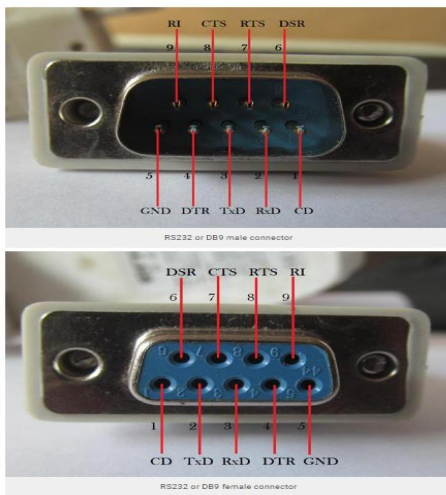


Figure: RS-232 Connector

- **Content/Topic 3: Introduction to Access Methods**

✓ CSMA/CD

CSMA/CD stands for **Carrier Sense Multiple Access / Collision Detection** is a network protocol for carrier transmission. It is operated in the medium access control layer. It senses if the shared channel is busy for broadcasting and interrupt the broadcast until the channel is free. In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped and a jam signal is sent by the stations and then station waits for a random time context before retransmission.

✓ CSMA/CA

CSMA/CD stands for **Carrier Sense Multiple Access / Collision Avoidance** is a network protocol for carrier transmission. Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD (that is effective after a collision) CSMA / CA is effective before a collision.

Table: The difference between CSMA/CA and CSMA/CD

No	CSMA / CD	CSMA / CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resend the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).

✓ **Token passing**

A communications network access method that uses a continuously repeating frame (the token) that is transmitted onto the network by the controlling computer. When a terminal or computer wants to send a message, it waits for an empty token that it fills with the address of the destination station and some or all of its message.

Every node on the network constantly monitors the passing tokens to determine if it is a recipient of a message, in which case it "grabs" the message and resets the token status to empty. Token passing uses bus and ring topologies.

Learning Unit 3: IP Addressing (IPv4&IPv6)

LO3.1 – Description of IP Addressing concepts

- **Content/Topic 1: Introduction to IP Address**

Addressing is a key function of network layer protocols that enables data communication between hosts, regardless of whether the hosts are on the same network or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data. Designing, implementing and managing an effective IP addressing plan ensures that networks can operate effectively and efficiently.

To understand the operation of devices on a network, we need to look at addresses and other data the way devices do - in binary notation. Binary notation is a representation of information using only ones and zeros. Computers communicate using binary data. Binary data can be used to represent many different forms of data. For example, when typing letters on a keyboard, those letters appear on screen in a form that you can read and understand; however, the computer translates each letter to a series of binary digits for storage and transport. To translate those letters, the computer uses American Standard Code for Information Interchange (ASCII).

Using ASCII, the letter “A” is represented in bit form as: 01000001, while the lowercase letter “a” is represented in bit form as 01100001.

While it is not generally necessary for people to concern themselves with binary conversion of letters, it is necessary to understand the use of binary for IP addressing. Each device on a network must be uniquely identified using a binary address. In IPv4 networks, this address is represented using a string of 32 bits (1s and 0s). At the network layer, the packets then include this unique identification information for both the source and destination systems. Therefore, in an IPv4 network, each packet includes a 32-bit source address and a 32-bit destination address in the Layer 3 header.

For most individuals, a string of 32 bits is difficult to interpret and even more difficult to remember. Therefore, we represent IPv4 addresses using dotted decimal format instead of binary. This means that we look at each byte (octet) as a decimal number in the range of 0 to 255.

- **Content/Topic 2: Classification of IP Address**

Classification

Released in 1981, RFC 790 and RFC 791 describe how IPv4 network addresses were initially allocated based on a classification system. In the original specification of IPv4, the authors established the classes to provide three different sizes of networks for large, medium, and small organizations. As a result, class A, B, and C addresses were defined with a specific format for the high order bits. High order bits are the far left bits in a 32-bit address.

As shown in the figure:

Class A addresses begin with 0 - Intended for large organizations; includes all addresses from 0.0.0.0 (00000000) to 127.255.255.255 (01111111). The 0.0.0.0 address is reserved for default routing and the 127.0.0.0 address is reserved for loopback testing.

Class B addresses begin with 10 - Intended for medium-to-large organizations; includes all addresses from 128.0.0.0 (10000000) to 191.255.255.255 (10111111).

Class C addresses begin with 110 - Intended for small-to-medium organizations; includes all addresses from 192.0.0.0 (11000000) to 223.255.255.255 (11011111).

The remaining addresses were reserved for multicasting and future uses.

Class D Multicast addresses begin with 1110 - Multicast addresses are used to identify a group of hosts that are part of a multicast group. This helps reduce the amount of packet processing that is done by hosts, particularly on broadcast media (i.e., Ethernet LANs). Routing protocols, such as RIPv2, EIGRP, and OSPF use designated multicast addresses (RIP = 224.0.0.9, EIGRP = 224.0.0.10, OSPF 224.0.0.5, and 224.0.0.6).

Class E Reserved IP addresses begin with 1111 - These addresses were reserved for experimental and future use.

High Order Bits

Class	High Order Bits	Start	End
Class A	0xxxxxxx	0.0.0.0	127.255.255.255
Class B	10xxxxxx	128.0.0.0	191.255.255.255
Class C	110xxxxx	192.0.0.0	223.255.255.255
Class D (Multicast)	1110xxxx	224.0.0.0	239.255.255.255
Class E (Reserved)	1111xxxx	240.0.0.0	255.255.255.255

As specified in RFC 790, each network class has a default subnet mask associated with it.

As shown in Figure 1, class A networks used the first octet to identify the network portion of the address. This is translated to a 255.0.0.0 classful subnet mask. Because only 7 bits were left in the first octet (remember, the first bit is always 0), this made 2 to the 7th power, or 128 networks. The actual number is 126 networks, because there are two reserved class A addresses (i.e., 0.0.0.0/8 and 127.0.0.0/8). With 24 bits in the host portion, each class A address had the potential for over 16 million individual host addresses.

As shown in Figure 2, class B networks used the first two octets to identify the network portion of the network address. With the first two bits already established as 1 and 0, 14 bits remained in the first two octets for assigning networks, which resulted in 16,384 class B network addresses. Because each class B network address contained 16 bits in the host portion, it controlled 65,534 addresses. (Recall that two addresses were reserved for the network and broadcast addresses.)

As shown in Figure 3, class C networks used the first three octets to identify the network portion of the network address. With the first three bits established as 1 and 1 and 0, 21 bits remained for assigning networks for over 2 million class C networks. But, each class C network only had 8 bits in the host portion, or 254 possible host addresses.

An advantage of assigning specific default subnet masks to each class is that it made routing update messages smaller. Classful routing protocols do not include the subnet mask information in their updates. The receiving router applies the default mask based on the value of the first octet which identifies the class.

Class A Networks					Class B Networks				
	1st Octet	2nd Octet	3rd Octet	4th Octet		1st Octet	2nd Octet	3rd Octet	4th Octet
Always starts with binary 0:	0xxxxxxx				Always starts with binary 10:	10xxxxxx	xxxxxxx		
Decimal equivalent:	0 – 127				Decimal equivalent:	128 – 191	0 – 255		
	Network	Host	Host	Host		Network	Network	Host	Host
Subnet mask	255	.0	.0	.0	Subnet mask	255	.255	.0	.0

Class C Networks				
	1st Octet	2nd Octet	3rd Octet	4th Octet
Always starts with binary 110:	110xxxx	xxxxxxxx	xxxxxxxx	
Decimal equivalent:	192 – 223	0 – 255	0 – 255	
	Network	Network	Network	Host
Subnet mask	255	.255	.255	.0

IP Address Grouping

All IPv4 IP addresses can be divided into two major groups: **public/global**, or external - this group can also be called 'WAN addresses' — those that are used in the Internet, and **private**, or local, or internal addresses — those that are used in the local network (LAN). There are also special-use addresses, intended for technical purposes such as protocol functions etc. Normally these are not exposed to a user at all.

Public IP-address

It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

The presence of a public IP address on your router or computer will allow you to organize your own server (VPN, FTP, WEB, etc.), remote access to your computer, video surveillance cameras, and access them from anywhere in the global network.

With a public IP address, you can set up any home server to publish it on the Internet: Web (HTTP), VPN (PPTP/IPSec/OpenVPN), media (audio/video), FTP, NAS network drive, game server, etc.

Private IP-address

Private internal addresses are not routed on the Internet and no traffic cannot be sent to them from the Internet, they only supposed to work within the local network.

Private addresses include IP addresses from the following subnets:

Range from 10.0.0.0 – 10.255.255.255, in IPv4 Class A

Range from 172.16.0.0 – 172.31.255.255, in IPv4 Class B

Range from 192.168.0.0 – 192.168.255.255, in Class C

Those are reserved IP addresses. These addresses are intended for use in closed local area networks and the allocation of such addresses is not globally controlled by anyone.

Direct access to the Internet using a private IP address is not possible. In this case, the connection to the Internet is via NAT (Network Address Translation) replaces the private IP address with a public one. Private IP addresses within the same local network must be unique and cannot be repeated.

- **Content/Topic 3: Description of IP Address Scheme and Subnet Mask**

IP Address Scheme

Network Address

The network address is a standard way to refer to a network. The subnet mask or the prefix length might also be used when referring to network address. For example, the network shown in Figure 1 could be referred to as the 10.1.1.0 network, the 10.1.1.0 255.255.255.0 network or the 10.1.1.0/24 network. All hosts in the 10.1.1.0/24 network will have the same network portion bits.

As shown in Figure 2, within the IPv4 address range of a network, the first address is reserved for the network address. This address has a 0 for each host bit in the host portion of the address. All hosts within the network share the same network address.

Host Address

Every end device requires a unique address to communicate on the network. In IPv4 addresses, the values between the network address and the broadcast address can be assigned to end devices in a

network. As shown in Figure 3, this address has any combination of 0 and 1 bits in the host portion of the address but cannot contain all 0 bits or all 1 bits.

Broadcast Address

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network at once, a host can send a single packet that is addressed to the broadcast address of the network, and each host in the network that receives this packet will process its contents.

The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s. All 1s in an octet in binary form, is equal to the number 255 in decimal form. Therefore, as shown in Figure below, for the network 10.1.1.0/24, in which the last octet is used for the host portion, the broadcast address would be 10.1.1.255. Note that the host portion will not always be an entire octet. This address is also referred to as the directed broadcast.

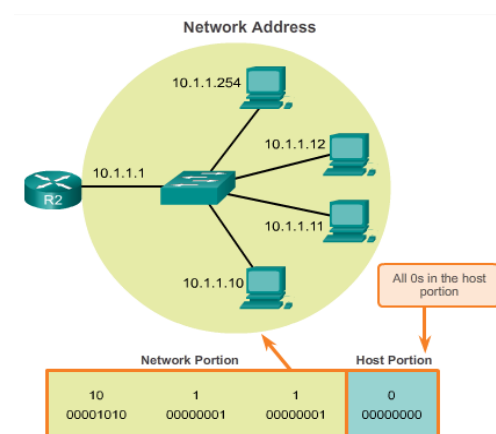


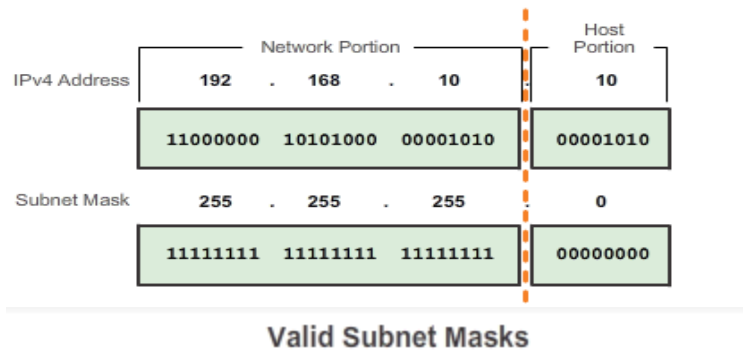
Fig.24: An example of Network Address

IP Address Subnet Mask

Understanding binary notation is important when determining if two hosts are in the same network. Recall that an IP address is a hierarchical address that is made up of two parts: a network portion and a host portion. But when determining the network portion versus the host portion, it is necessary to look, not at the decimal value, but at the 32-bit stream. Within the 32-bit stream, a portion of the bits makes up the network and a portion of the bits makes up the host. The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the

host portion of the address must be unique to identify a specific host within a network. Regardless of whether the decimal numbers between two IPv4 addresses match up, if two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

But how do hosts know which portion of the 32-bits is network and which is host? That is the job of the subnet mask. When an IP host is configured, a subnet mask is assigned along with an IP address. Like the IP address, the subnet mask is 32 bits long. The subnet mask signifies which part of the IP address is network and which part is host. The subnet mask is compared to the IP address from left to right, bit for bit. The 1s in the subnet mask represent the network portion; the 0s represent the host portion. As shown in Figure 1, the subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion. Note that the subnet mask does not actually contain the network or host portion of an IPv4 address, it just tells the computer where to look for these portions in a given IPv4 address. Similar to IPv4 addresses, the subnet mask is represented in dotted decimal format for ease of use. The subnet mask is configured on a host device, in conjunction with the IPv4 address, and is required so the host can determine which network it belongs to. Figure 2 displays the valid subnet masks for an IPv4 octet.



Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

- Content/Topic4: Examining the prefix length and types of IP Address**

✓ Prefix length

The prefix length is another way of expressing the subnet mask. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, a “/” followed by the number of bits set to 1. For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Networks are not always assigned a /24 prefix. Depending on the number of hosts on the network, the prefix assigned may be different. Having a different prefix number changes the host range and broadcast address for each network.

The figures illustrate different prefixes using the same 10.1.1.0 address. Figure 1 illustrates /24 to /26 prefixes. Figure 2 illustrates /27 to /28 prefixes.

Notice that the network address could remain the same, but the host range and the broadcast address are different for the different prefix lengths. In the figures, you can see that the number of hosts that can be addressed on the network also changes.

Dotted Decimal		Significant bits shown in binary
Network Address	10.1.1.0/24	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: $2^8 - 2 = 254$ hosts		

Network Address	10.1.1.0/25	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: $2^7 - 2 = 126$ hosts		

Network Address	10.1.1.0/26	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.62	10.1.1.00111110
Broadcast Address	10.1.1.63	10.1.1.00111111
Number of hosts: $2^6 - 2 = 62$ hosts		

Dotted Decimal		Significant bits shown in binary
Network Address	10.1.1.0/27	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.30	10.1.1.00011110
Broadcast Address	10.1.1.31	10.1.1.00011111
Number of hosts: $2^5 - 2 = 30$ hosts		

Network Address	10.1.1.0/28	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.14	10.1.1.00001110
Broadcast Address	10.1.1.15	10.1.1.00001111
Number of hosts: $2^4 - 2 = 14$ hosts		

There are three types of addresses within the address range of each IPv4 network:

- Network address
- Host addresses
- Broadcast address

Types of IP Addresses

There are 2 Types of IP Addresses Consumers Have, every person or business with an internet service plan will have two types of IP addresses: their private IP addresses, and the public IP address.

✓ Private IP Addresses

A private IP address is an address which is reserved for use only within private/local network and cannot be seen outside the private networks. These private addresses are translated at the company's firewall into an external (public) IP address, which will be some address that does 'not' fall within the range of Private ones.

Ranger of private IP address

Class A: 10.0.0.0/8=10.0.0.0 – 10.255.255.255

Class B: 172.16.0.0/12=172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0/16=192.168.0.0 – 192.168.255.255

✓ Public IP-address

It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

Note: All servers and sites on the Internet use public IP addresses (for example, google.com — 172.217.22.14, Google's DNS server — 8.8.8.8).

All of the public IP-addresses in the Internet are unique to their host or server and cannot duplicate assignment.

LO3.2. Applying IP v4

- **Content/Topic 1: Introduction to IPv4**

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6.

IPv4 uses a 32-bit address space which provides 4,294,967,296 (2^{32}) unique addresses, but large blocks are reserved for special networking methods.

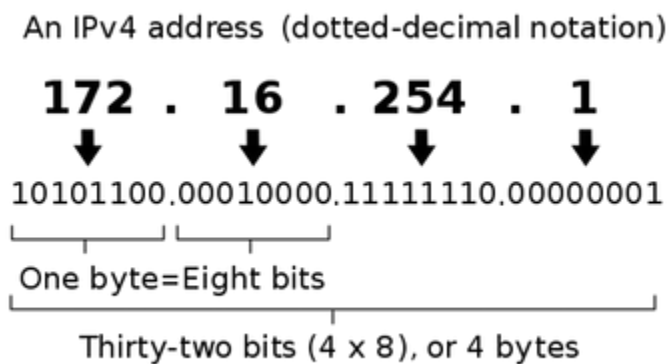


Fig. 25: IPv4 Address Structure

- **Content/Topic 2: Description of IPv4 address**

Parts of the IPv4 Address

Each network running TCP/IP must have a unique network number, and every machine on it must have a unique IP address. It is important to understand how IP addresses are constructed before you register your network and obtain its network number.

As we have seen in the introduction, IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine. An IPv4 address is typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IPv4 address.

The bytes of the IPv4 address are further classified into two parts: the network part and the host part. The following figure shows the component parts of a typical IPv4 address, 129.144.50.56.

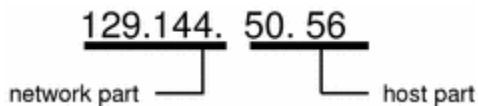


Fig. 26: Parts of an IPv4 Address

Network Part

This part specifies the unique number assigned to your network. It also identifies the class of network assigned. In Figure above, the network part takes up two bytes of the IPv4 address.

Host Part

This is the part of the IPv4 address that you assign to each host. It uniquely identifies this machine on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

IPv4 packet

An IPv4 packet consists of header information as well as encapsulated data. An IP header consists of 14 fields and contains necessary information required to deliver the packet at another end.

0	4	8	15	16	31
Version	IHL	Type Of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options (if IHL > 5)					

Fig. 27: IP Packet Structure

1. Version: Provides the version number of Internet Protocol used (such as IPv4).
2. IHL: Refers to Internet Header Length which is the length of an entire IP header.
3. DSCP: Differentiated Services Code Point, also called Type of Service, and caters to data from emerging technologies.

4. ECN: Explicit Congestion Notification provides information about the network congestion seen in the route.
5. Total Length: Length of entire IP packet, which includes IP header and encapsulated data.
6. Identification: This field is used to uniquely identify a group of fragments in the single IP packet.
7. Flags: This is a three-bit field that's used to identify and control fragments. In this 3-bit flag, the bit 0 is always set to '0'.
8. Fragment Offset: This offset provides the location of the fragment in the original IP Packet.
9. Time to Live (TTL): Every packet is sent with some TTL value set to avoid looping in the network. TTL tells the network about the hops it has crossed on the router. With each hop, the TTL value is decremented by one, and when the value reaches zero, the packet is discarded.
10. Protocol: This field provides the protocol that's used in the data part of the packet.
11. Header Checksum: This field is used for error-checking of the entire header. The value of the header checksum is matched at the router and the packet is discarded if values don't match.
12. Source Address: This field is the 32-bit address of the sender of the packet.
13. Destination Address: This field is the 32-bit address of the receiver of the packet.
14. Options: This is an optional field, which is used if the value of header length (IHL) is greater than 5. This may contain values for options such as Security, Record-Route, or Time Stamp.

- **Content/Topic 3: Assigning IP address**

IP addresses are assigned to a host either dynamically as they join the network, or persistently by configuration of the host hardware or software. Persistent configuration is also known as using a static IP address. In contrast, when a computer's IP address is assigned each time it restarts, this is known as using a dynamic IP address.

✓ **Methods of Assigning IP address**

➤ **Address autoconfiguration method**

Address block 169.254.0.0/16 is defined for the special use in link-local addressing for IPv4 networks. These addresses are only valid on the link, such as a local network segment or point-to-point

connection, to which a host is connected. These addresses are not routable and, like private addresses, cannot be the source or destination of packets traversing the Internet. When the link-local IPv4 address block was reserved, no standards existed for mechanisms of address autoconfiguration.

➤ **Static IP Assignment method**

In Static IP address assignment, the IP address, network mask and default gateway are **configured manually** in the system configuration file. However, it is possible to **change the IP address at runtime**. The static configuration specifies also a primary and optional secondary DNS server. To make use of the static IP configuration, you need to disable DHCP.

When static IPs are needed

Most users don't need static IP addresses. Static IP addresses normally matter more when external devices or websites need to remember your IP address. One example is VPN or other remote access solutions that trust (whitelists) certain IPs for security purposes. A static IP address is not required if you are hosting a server, although it can simplify the setup process.

Disadvantages of Static IP Addressing

Static IPs are more hackable: With a static IP address, hackers know exactly where your server is on the Internet. That makes it easier for them to attack it.

It limits the amount of IP addresses: A static IP address assigned to a device or website is occupied until otherwise noted, even when the device is off and not in use.

Static IP Addressing may create IP address conflict, which occurs when two or more devices on the same network are assigned the same IP address.

➤ **Dynamic IP Assignment method**

This mode is mostly used. It requires a centralized DHCP server in the local area network (LAN). DHCP server maintains a database of leased IP addresses, and assigns to the client an unused **IP address**. It specifies also a **network mask** and a **default gateway** to use, when the system wants to access the Internet. The DHCP server specifies also a primary and optional secondary DNS server. The **DNS server** is used to resolve the IP address for a known host name. Dynamic IP addressing may be also carried out by your router using a **protocol** known as Dynamic Host Configuration Protocol (DHCP). It's a handy way for devices to connect to your network more easily, because you don't have to configure IP addressing for each new device yourself. The downside to automatic addressing is that it's possible for a device's IP address to change from time to time.

- **Content/Topic 4: Calculation of IP addresses**

- ✓ **Binary to decimal and decimal to binary conversion**

Learning to convert binary to decimal requires an understanding of the mathematical basis of a numbering system called positional notation.

Positional Notation

Positional notation means that a digit represents different values depending on the position the digit occupies. In a positional notation system, the number base is called the radix. In the base ten system, the radix is 10. In the binary system we use a radix of 2. The term radix and base can be used interchangeably. More specifically, the value that a digit represents is that value multiplied by the power of the base, or radix, represented by the position the digit occupies. Some examples will help to clarify how this system works.

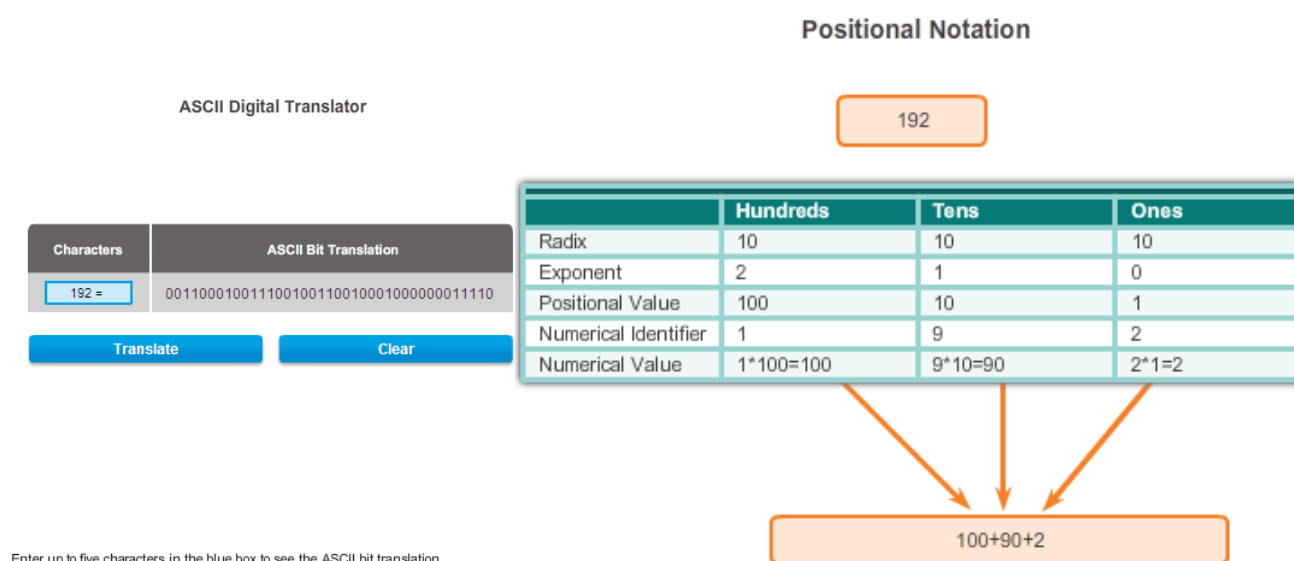
For the decimal number 192, the value that the 1 represents is $1 \cdot 10^2$ (1 times 10 to the power of 2). The 1 is in what we commonly refer to as the "100s" position. Positional notation refers to this position as the base^2 position because the base, or radix, is 10 and the power is 2. The 9 represents $9 \cdot 10^1$ (9 times 10 to the power of 1). Positional notation for the decimal number 192 is shown in Figure 2.

Using positional notation in the base 10 number system, 192 represents:

$$192 = (1 \cdot 10^2) + (9 \cdot 10^1) + (2 \cdot 10^0)$$

or

$$192 = (1 \cdot 100) + (9 \cdot 10) + (2 \cdot 1)$$



In IPv4, addresses are 32-bit binary numbers. However, for ease of use by people, binary patterns representing IPv4 addresses are expressed as dotted decimals. This is first accomplished by separating each byte (8 bits) of the 32-bit binary pattern, called an octet, with a dot. It is called an octet because each decimal number represents one byte or 8 bits.

The binary address:

11000000 10101000 00001010 00001010

is expressed in dotted decimal as:

192.168.10.10

In Figure 1, select each button to see how the 32-bit binary address is represented in dotted decimal octets.

But how are the actual decimal equivalents determined?

Binary Numbering System

In the binary numbering system, the radix is 2. Therefore, each position represents increasing powers of 2. In 8-bit binary numbers, the positions represent these quantities:

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

The base 2 numbering system only has two digits: 0 and 1.

When we interpret a byte as a decimal number, we have the quantity that position represents if the digit is a 1 and we do not have that quantity if the digit is a 0, as shown in Figure 1.

Figure 2 illustrates the representation of the decimal number 192 in binary. A 1 in a certain position means we add that value to the total. A 0 means we do not add that value. The binary number 11000000 has a 1 in the 2^7 position (decimal value 128) and a 1 in the 2^6 position (decimal value 64). The remaining bits are all 0 so we do not add the corresponding decimal values. The result of adding 128+64 is 192, the decimal equivalent of 11000000.

Here are two more examples:

Example 1: An octet containing all 1s: 11111111

A 1 in each position means that we add the value for that position to the total. All 1s means that the values of every position are included in the total, therefore, the value of all 1s in an octet is 255.

$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$

Example 2: An octet containing all 0s: 00000000

A 0 in each position indicates that the value for that position is not included in the total. A 0 in every position yields a total of 0.

$$0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$$

A different combination of ones and zeros will yield a different decimal value.

192	.	168	.	10	.	10
11000000		10101000		00001010		00001010

192.168.10.10 is an IP address that is assigned to a computer.

Dotted Decimal Address

Octets

32-Bit Address

Radix	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Octet Bit Values	128	64	32	16	8	4	2	1
Binary Address	1	1	0	0	0	0	0	0
Binary Bit Values	128	64	0	0	0	0	0	0

Add the binary bit values.
128 + 64 = 192

Legend

- 1 in this position means add the octet bit value to the total
- 0 in this position means 0 is added to the total

Each octet is made up of 8 bits and each bit has a value, either 0 or 1. The four groups of 8 bits have the same set of valid values in the range of 0 to 255 inclusive. The value of each bit placement, from right to left is 1, 2, 4, 8, 16, 32, 64, and 128.

Determine the value of the octet by adding the values of positions wherever there is a binary 1 present.

- If there is a 0 in a position, do not add the value.
- If all 8 bits are 0s, 00000000, the value of the octet is 0.
- If all 8 bits are 1s, 11111111, the value of the octet is 255 (128+64+32+16+8+4+2+1)
- If the 8 bits are mixed, the values are added together. For example, the octet 00100111 has a value of 39 (32+4+2+1).

So the value of each of the four octets can range from 0 to a maximum of 255.

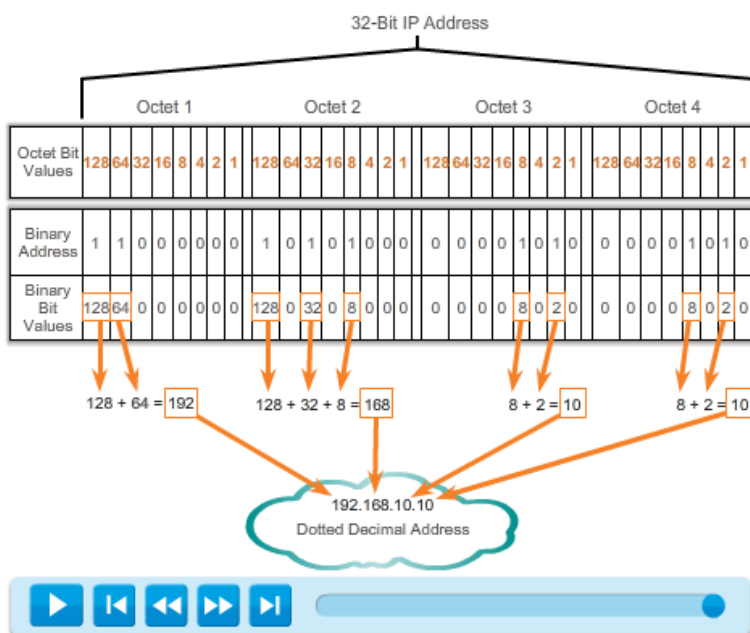
Using the 32-bit IPv4 address, 11000000101010000000101000001010, convert the binary representation to dotted decimal using the following steps:

Step 1. Divide the 32 bits into 4 octets.

Step 2. Convert each octet to decimal.

Step 3. Add a "dot" between each decimal.

Click Play in the figure to see how a binary address is converted to dotted decimal.



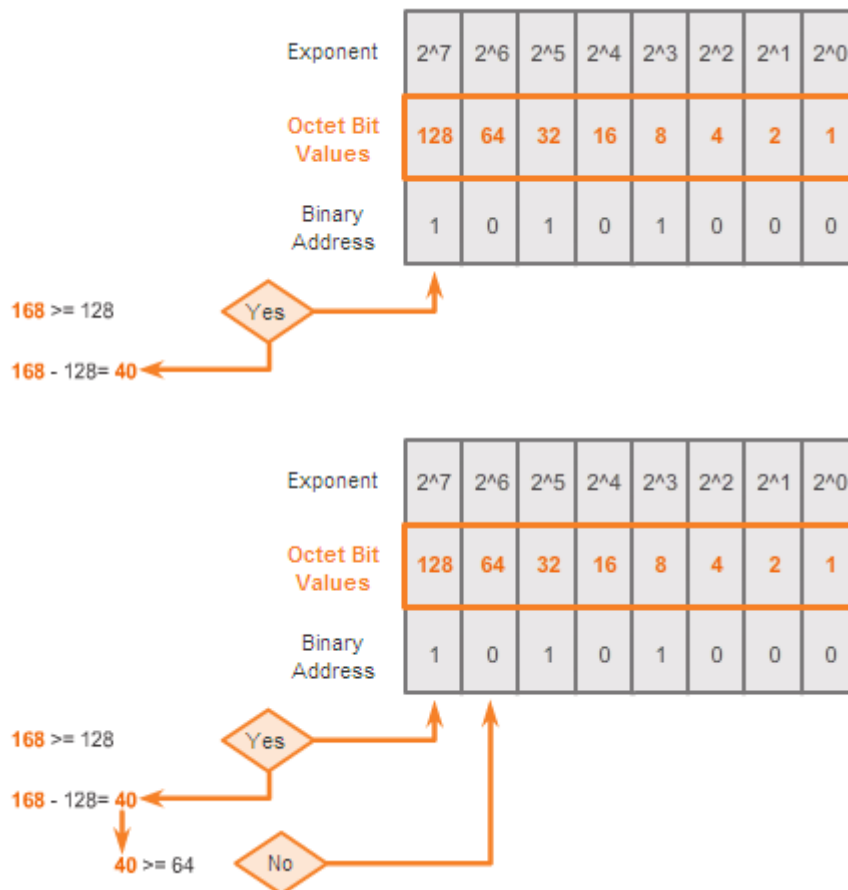
In addition to being able to convert binary to decimal, it is also necessary to understand how to convert decimal to binary.

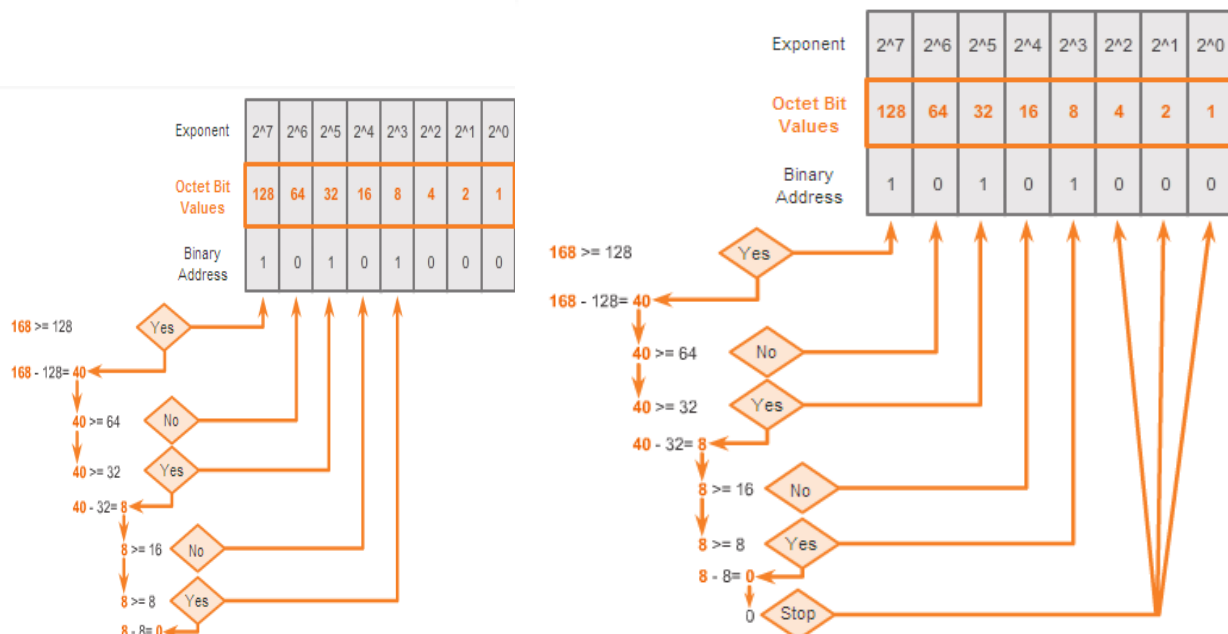
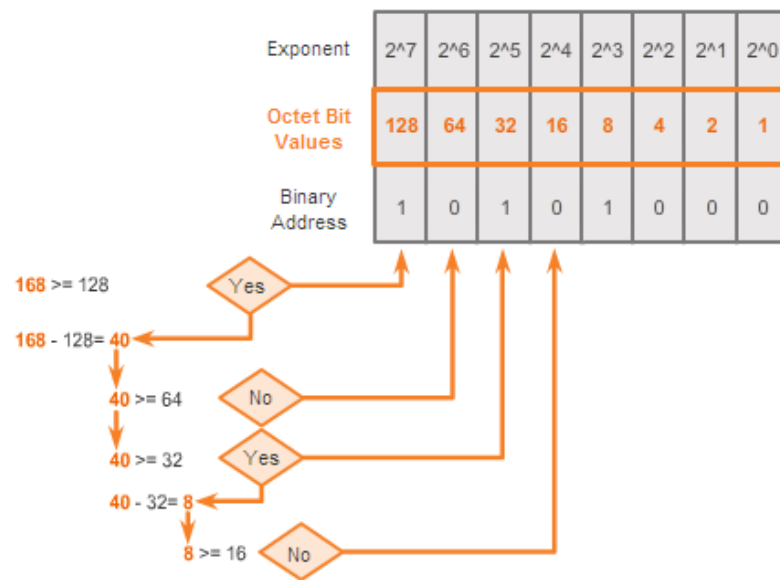
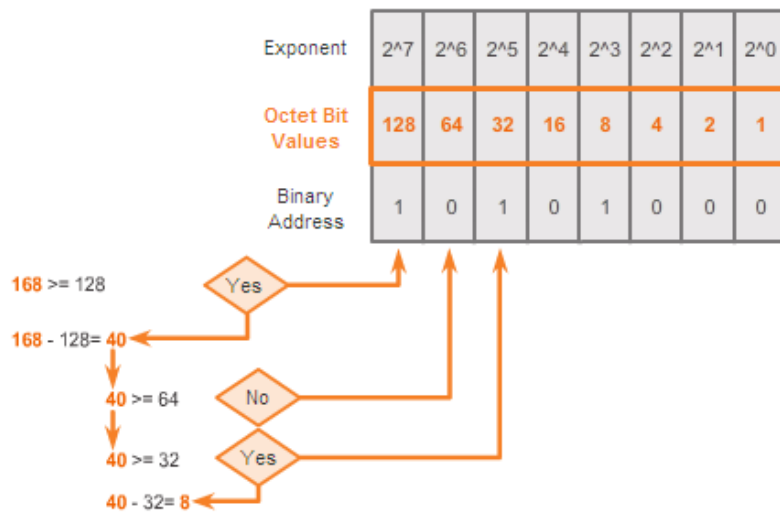
Because we represent IPv4 addresses using dotted decimal format, it is only necessary that we examine the process of converting 8-bit binary to the decimal values of 0 to 255 for each octet in an IPv4 address.

To begin the conversion process, we start by determining if the decimal number is equal to or greater than our largest decimal value represented by the most-significant bit. In the highest position, we

determine if the octet number is equal to or greater than 128. If the octet number is smaller than 128, we place a 0 in the bit position for decimal value 128 and move to the bit position for decimal value 64. If the octet number in the bit position for decimal value 128 is larger than or equal to 128, we place a 1 in the bit position for decimal value 128 and subtract 128 from the octet number being converted. We then compare the remainder of this operation to the next smaller value, 64. We continue this process for all the remaining bit positions.

Click through Figures 1-6 to see the process of converting 168 to the binary equivalent of 10101000.





Follow the conversion steps in the figures to see how an IP address is converted to binary.

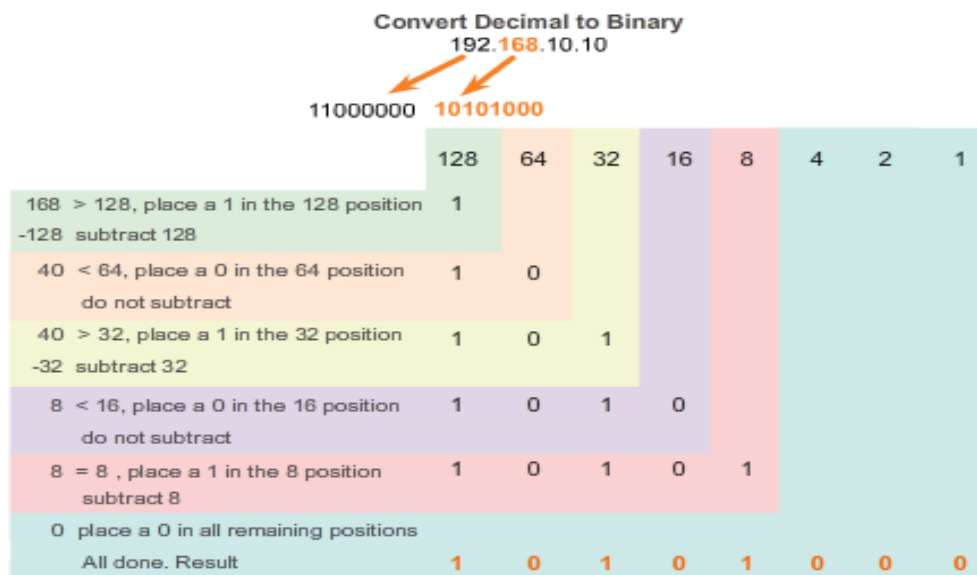
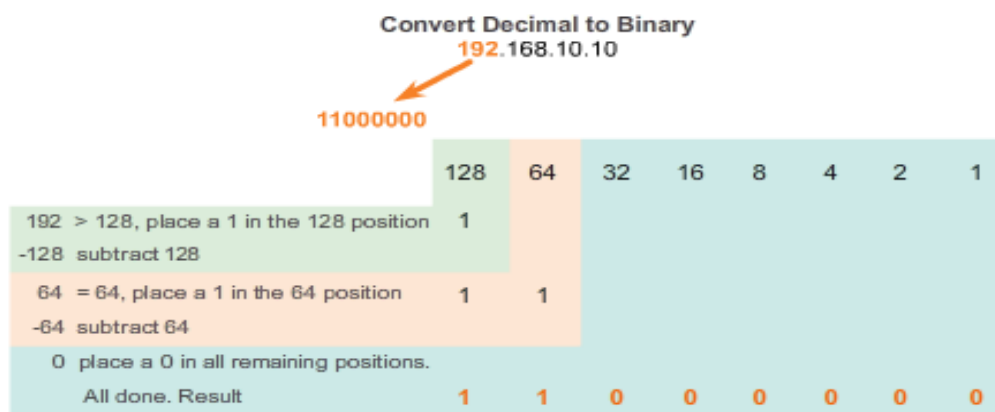
Figure 1: Convert 192 to binary.

Figure 2: Convert 168 to binary.

Figure 3: Convert 10 to binary.

Figure 4: Convert 10 to binary.

Figure 5: Combine the converted octets beginning with the first octet.



Convert Decimal to Binary
192.168.10.10

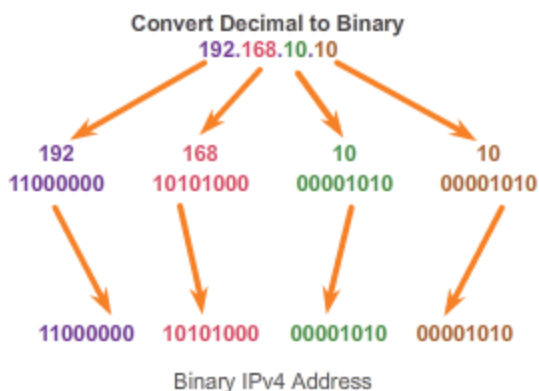
11000000 10101000 00001010

	128	64	32	16	8	4	2	1
10 < 128, place a 0 in the 128 position do not subtract	0	0	0	0	1	0	1	0
10 < 64, place a 0 in the 64 position do not subtract	0	0	0	0	1	0	1	0
10 < 32, place a 0 in the 32 position do not subtract	0	0	0	0	1	0	1	0
10 < 16, place a 0 in the 16 position do not subtract	0	0	0	0	1	0	1	0
10 > 8, place a 1 in the 8 position subtract 8	0	0	0	0	1	0	1	0
2 < 4, place a 0 in the 4 position do not subtract	0	0	0	0	1	0	1	0
2 = 2, place a 1 in the 2 position -2 subtract 2	0	0	0	0	1	0	1	0
0 place a 0 in all remaining positions All done. Result	0	0	0	0	1	0	1	0

Convert Decimal to Binary
192.168.10.10

11000000 10101000 00001010 00001010

	128	64	32	16	8	4	2	1
10 < 128, place a 0 in the 128 position do not subtract	0	0	0	0	1	0	1	0
10 < 64, place a 0 in the 64 position do not subtract	0	0	0	0	1	0	1	0
10 < 32, place a 0 in the 32 position do not subtract	0	0	0	0	1	0	1	0
10 < 16, place a 0 in the 16 position do not subtract	0	0	0	0	1	0	1	0
10 > 8, place a 1 in the 8 position subtract 8	0	0	0	0	1	0	1	0
2 < 4, place a 0 in the 4 position do not subtract	0	0	0	0	1	0	1	0
2 = 2, place a 1 in the 2 position -2 subtract 2	0	0	0	0	1	0	1	0
0 place a 0 in all remaining positions All done. Result	0	0	0	0	1	0	1	0



✓ IP address Sub-netting calculation

Sub-netting is the process of borrowing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called subnets. After sub-netting, we end up with NETWORK SUBNET HOST fields. We always reserve an IP address to identify the subnet and another one to identify the broadcast subnet address.

Reasons of use sub-netting

Here are three reasons why you may want to use sub-netting:

1. Conservation of IP addresses: Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses ($254-20=234$). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.
2. Reduced network traffic: The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
3. Simplification: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

Concept of Sub-netting

To better understand the concept of sub-netting, imagine a network with a total of 256 addresses (a Class C network). One of these addresses is used to identify the network address and another one is used to identify the broadcast address on the network. Therefore, we are left with 254 addresses available for addressing hosts.

If we take all these addresses and divide them equally into 8 different subnets we still keep the total number of original addresses, but we have now split them into 8 subnets with 32 addresses in each. Each new subnet needs to dedicate 2 addresses for the subnet and broadcast address within the subnet.

The result is that we eventually come up with 8 subnets, each one possessing 30 subnet addresses available for hosts. You can see that the total amount of addressable hosts is reduced (240 instead of 254) but better management of addressing space is gained.

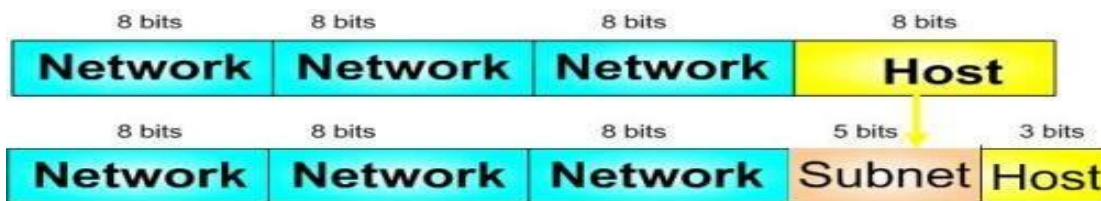
Calculation of Sub-netting

It can be helpful to know how to be your own subnet mask calculator. Subset a Class C address with the binary method by following these four steps (which will be explained in more detail below):

- ✓ Convert to binary.
- ✓ Calculate the subset address.
- ✓ Find host range.
- ✓ Calculate the total number of subsets and the hosts per subnet.

We will use a Class C address, which takes 5 bits from the Host field for sub-netting and leaves 3 bits for defining hosts as shown in figure 1 below. Having 5 bits available for defining subnets means that we can have up to 32 (2^5) different subnets.

It should be noted that in the past using subnet zero (00000---) and all-ones subnet (11111---) was not allowed. This is not true nowadays. Since Cisco IOS Software Release 12.0 the entire address space including all possible subnets is explicitly allowed.



Let's use IP address 192.168.10.44 with subnet mask 255.255.255.248 or /29.

STEP 1: Convert to Binary

IP Address (Decimal)	192.	168.	10.	44
IP Address (Binary)	11000000	10101000	00001010	00101100
Subnet Mask (Binary)	11111111	11111111	11111111	11111000
Subnet Mask (Decimal)	255.	255.	255.	248

STEP 2: Calculate the Subnet Address

To calculate the IP Address Subnet you need to perform a bit-wise AND operation ($1+1=1$, $1+0$ or $0+1=0$, $0+0=0$) on the host IP address and subnet mask. The result is the subnet address in which the host is situated.

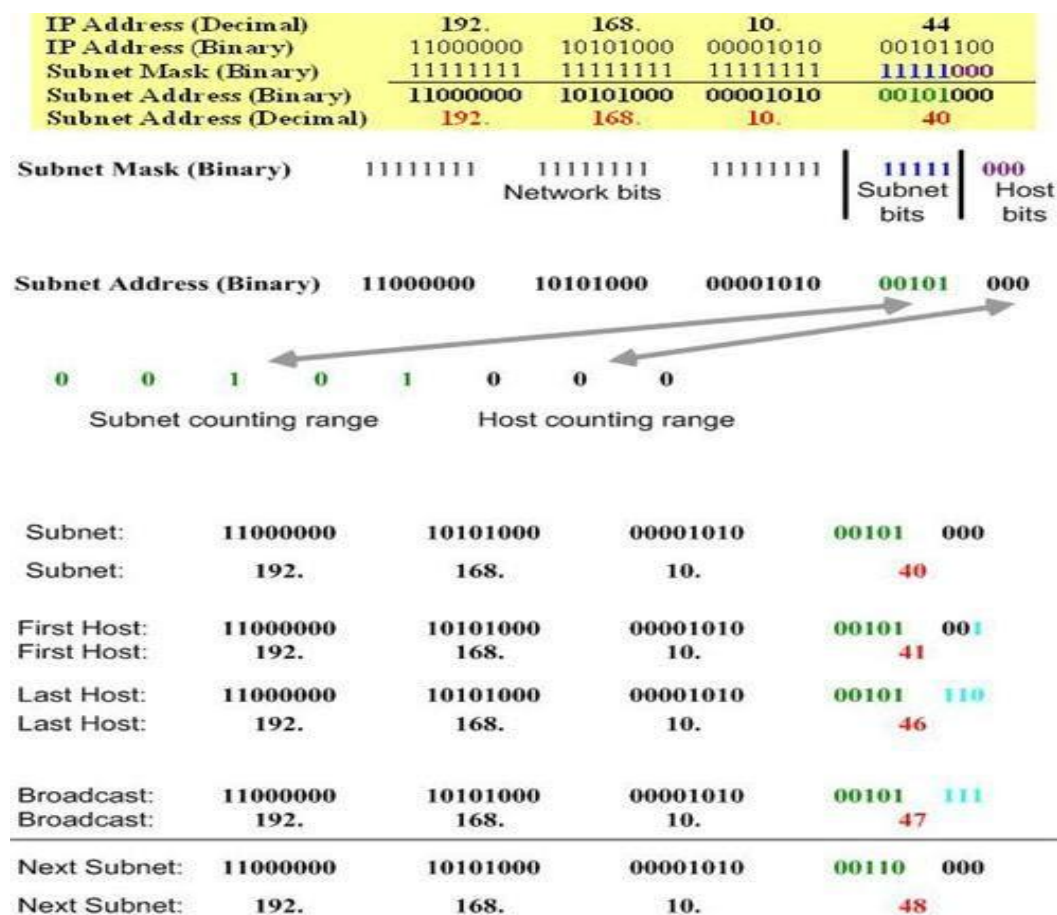
IP Address (Decimal)	192.	168.	10.	44
IP Address (Binary)	11000000	10101000	00001010	00101100
Subnet Mask (Binary)	11111111	11111111	11111111	11111000
Subnet Address (Binary)	11000000	10101000	00001010	00101000
Subnet Address (Decimal)	192.	168.	10.	40

STEP 3: Find Host Range

We know already that for sub-netting this Class C address we have borrowed 5 bits from the Host field. These 5 bits are used to identify the subnets. The remaining 3 bits are used for defining hosts within a particular subnet.

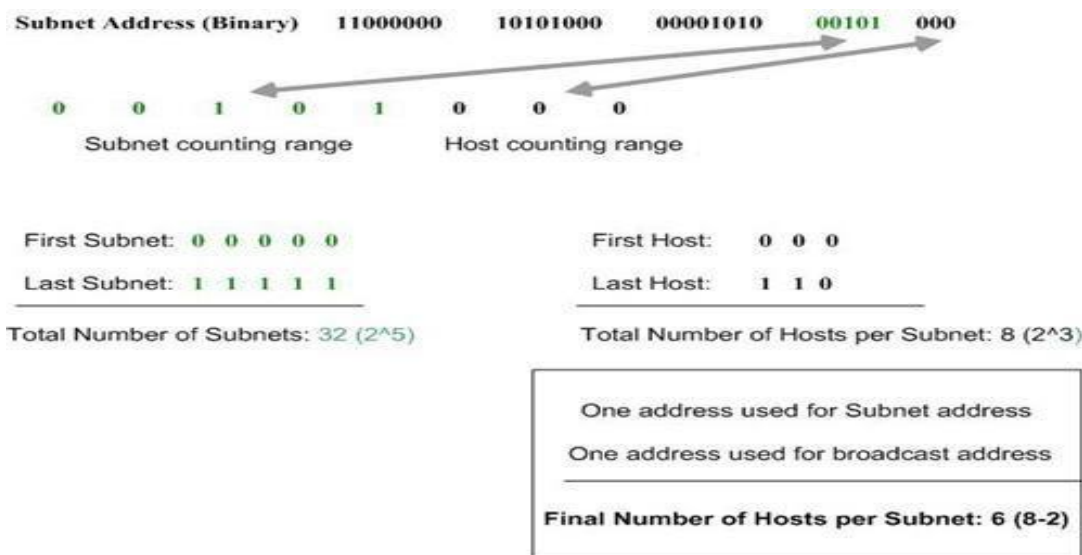
The Subnet address is identified by all 0 bits in the Host part of the address. The first host within the subnet is identified by all 0s and a 1. The last host is identified by all 1s and a 0. The broadcast address is the all 1s. Now, we move to the next subnet and the process is repeated the same way.

The following diagram clearly illustrates this process:



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

Knowing the number of Subnet and Host bits we can now calculate the total number of possible subnets and the total number of hosts per subnet. We assume in our calculations that all-zeros and all-ones subnets can be used. The following diagram illustrates the calculation steps.



Fast Way to Subset a Class C IP Address

Now let's see how to subnet the same Class C address using a faster method. Let's again use the IP address 192.168.10.44 with subnet mask 255.255.255.248 (/29).

The steps to perform this task are the following:

- ✓ Total number of subnets: Using the subnet mask 255.255.255.248, number value 248 (11111000) indicates that 5 bits are used to identify the subnet. To find the total number of subnets available simply raise 2 to the power of 5 (2^5) and you will find that the result is 32 subnets. Note that if subnet all-zeros is not used then we are left with 31 subnets and if also all-ones subnet is not used then we finally have 30 subnets.
- ✓ Hosts per subnet: 3 bits are left to identify the host therefore the total number of hosts per subnet is 2 to the power of 3 minus 2 (1 address for subnet address and another one for the broadcast address)(2^3-2) which equals to 6 hosts per subnet.
- ✓ Subnets, hosts and broadcast addresses per subnet: To find the valid subnets for this specific subnet mask you have to subtract 248 from the value 256 ($256-248=8$), which is the first available subnet address. Actually the first available one is the subnet-zero which we explicitly note. Next subnet address is $8+8=16$, next one is $16+8=24$ and this goes on until we reach value 248.

Table: Information of subnet calculation

Subnet	0	8	16	...	40	...	248
First Host	1	9	17	...	41	...	249
Last Host	6	14	22	...	46	...	254
Broadcast	7	15	23	...	47	...	255

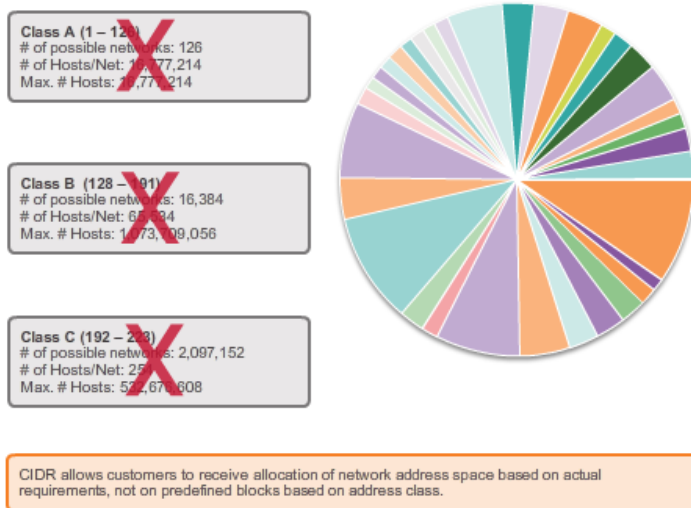
✓ **Summarization**

Route summarization - Also known as prefix aggregation, routes are summarized into a single route to help reduce the size of routing tables. For instance, one summary static route can replace several specific static route statements.

Super-netting - Occurs when the route summarization mask is a smaller value than the default traditional classful mask.

Note: A supernet is always a route summary, but a route summary is not always a supernet.

CIDR = Efficient



In the figure, notice that ISP1 has four customers, and that each customer has a variable amount of IP address space. The address space of the four customers can be summarized into one advertisement to ISP2. The 192.168.0.0/20 summarized or aggregated route includes all the networks belonging to Customers A, B, C, and D. This type of route is known as a supernet route. A supernet summarizes multiple network addresses with a mask that is smaller than the classful mask.

Determining the summary route and subnet mask for a group of networks can be done in the following three steps:

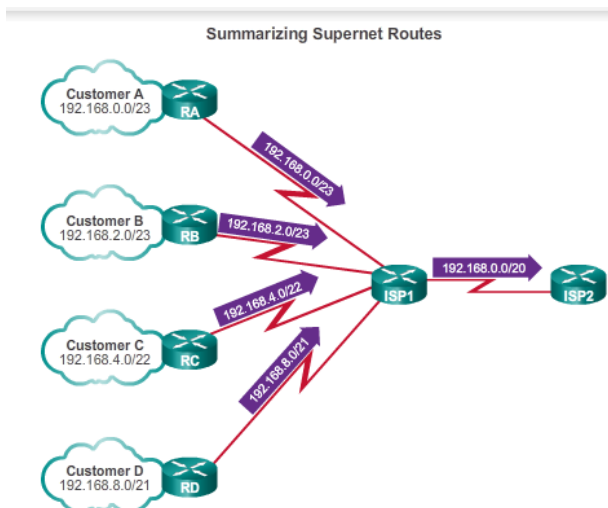
Step 1. List the networks in binary format.

Step 2. Count the number of far left matching bits. This identifies the prefix length or subnet mask for the summarized route.

Step 3. Copy the matching bits and then add zero bits to the rest of the address to determine the summarized network address.

The summarized network address and subnet mask can now be used as the summary route for this group of networks.

Summary routes can be configured by both static routes and classless routing protocols.

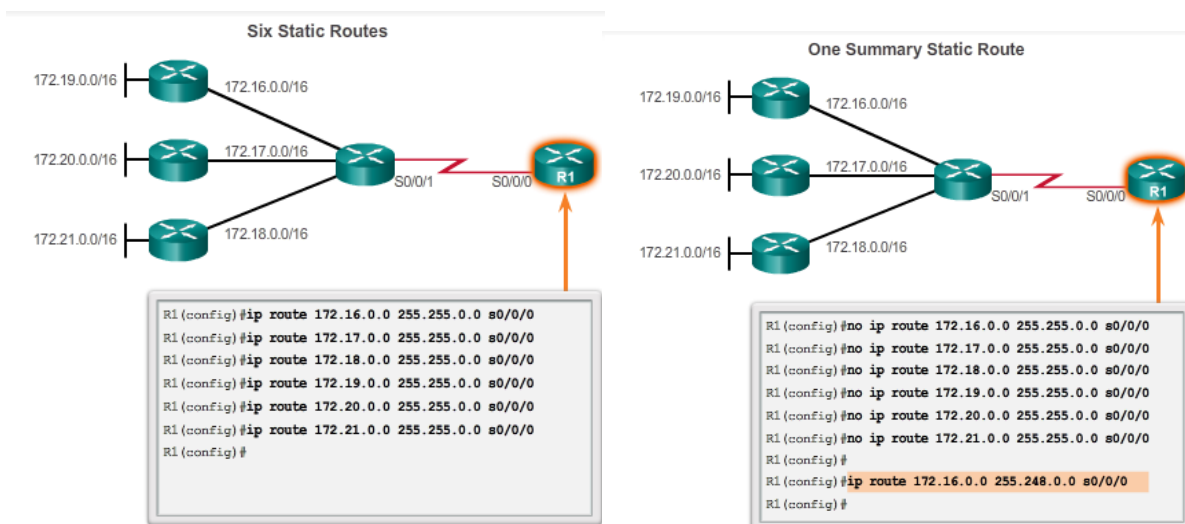


Creating smaller routing tables makes the routing table lookup process more efficient, because there are fewer routes to search. If one static route can be used instead of multiple static routes, the size of the routing table is reduced. In many cases, a single static route can be used to represent dozens, hundreds, or even thousands of routes.

Summary CIDR routes can be configured using static routes. This helps to reduce the size of routing tables.

In Figure 1, R1 has been configured to reach the identified networks in the topology. Although acceptable, it would be more efficient to configure a summary static route.

Figure 2 provides a solution using CIDR summarization. The six static route entries could be reduced to 172.16.0.0/13 entry. The example removes the six static route entries and replaces them with a summary static route.



Classful routing protocols cannot send supernet routes. This is because the receiving router automatically applies the default classful subnet mask to the network address in the routing update. If the topology in the figure contained a classful routing protocol, then R3 would only install 172.16.0.0/16 in the routing table.

- **Content/Topic5: Testing IP address**

✓ **Diagnostic tools**

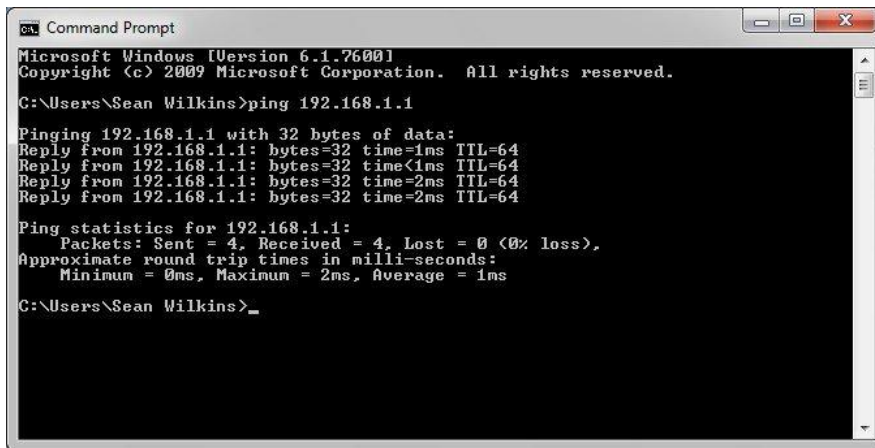
The Network Diagnostic Tool (NDT) is a client/server program that provides network configuration and performance testing to a user's desktop or laptop computer. The system is composed of a client program (command line or java applet) and a pair of server programs (a webserver and a testing/analysis engine).

Several studies have shown that the majority of network performance problems occur in or near the users' desktop/laptop computer. These problems include, but are not limited to, duplex mismatch conditions on Ethernet/Fast Ethernet links, incorrectly set TCP buffers in the user's computer, or problems with the local network infrastructure. The NDT is designed to quickly and easily identify a specific set of conditions that are known to impact network performance.

Network troubleshooting tools are a necessity for every network administrator. When you are in the networking field, you may find a mass number of tools that can be used to troubleshoot a variety of different network conditions. So let's see general and common used network troubleshooting tools.

✓ **Ping**

The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an Internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the Internet provider. The Figure below figure shows an example of the ping utility being used to obtain the reachability status of the locally connected router.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sean Wilkins>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

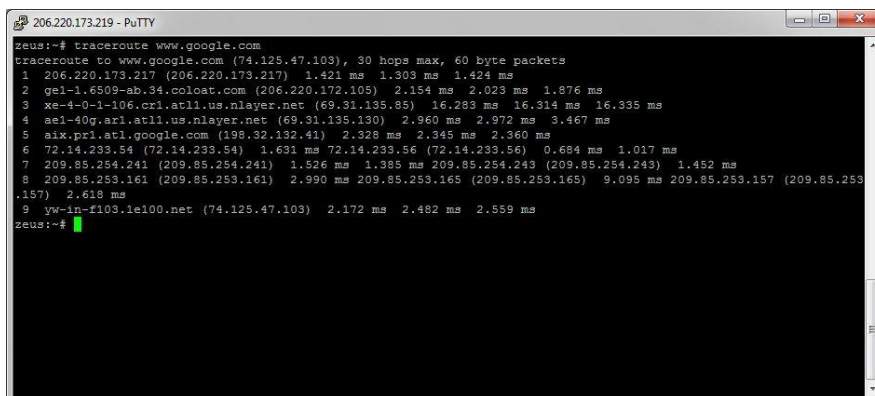
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\Sean Wilkins>
```

Fig.28: Ping utility

✓ Tracert/traceroute

Typically, once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can be used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts. The Figure below shows an example of the tracert utility being used to find the path from a host inside an office to www.google.com. The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux/*nix based machines.

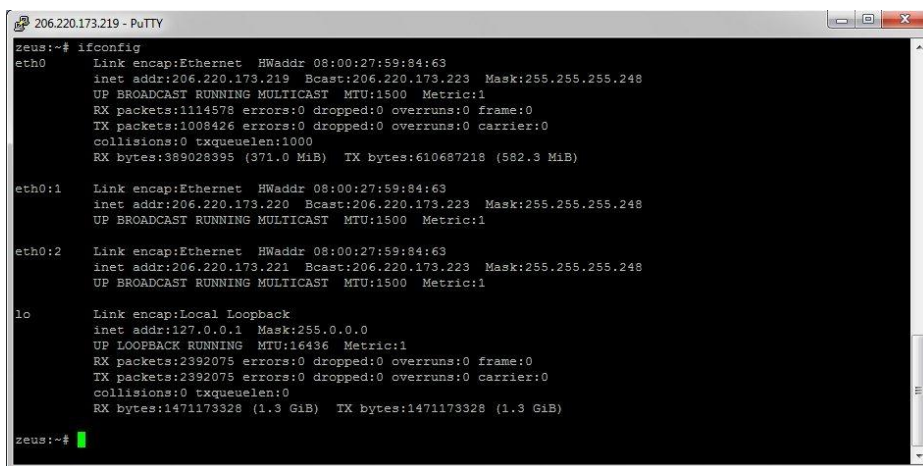


```
zeus:~# traceroute www.google.com
traceroute to www.google.com (74.125.47.103), 30 hops max, 60 byte packets
 1 206.220.173.217 (206.220.173.217) 1.421 ms 1.303 ms 1.424 ms
 2 ge1-1.6509-ab.34.colost.com (206.220.172.105) 2.154 ms 2.023 ms 1.876 ms
 3 xe-4-0-1-106.crl.atl1.us.nlayer.net (69.31.135.85) 16.203 ms 16.314 ms 16.395 ms
 4 ae1-40g.ar1.atl1.us.nlayer.net (69.31.135.130) 2.360 ms 2.972 ms 3.467 ms
 5 aix.px1.atl.google.com (198.32.132.41) 2.328 ms 2.345 ms 2.360 ms
 6 72.14.233.54 (72.14.233.54) 1.631 ms 72.14.233.56 (72.14.233.56) 0.684 ms 1.017 ms
 7 209.85.254.241 (209.85.254.241) 1.526 ms 1.385 ms 209.85.254.243 (209.85.254.243) 1.452 ms
 8 209.85.253.161 (209.85.253.161) 2.990 ms 209.85.253.165 (209.85.253.165) 9.095 ms 209.85.253.157 (209.85.253.157) 2.618 ms
 9 yw-in-f103.1e100.net (74.125.47.103) 2.172 ms 2.482 ms 2.559 ms
zeus:~#
```

Fig.29:Tracert/traceroute utility

✓ Ipconfig/ifconfig

One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities that can be used to find out this IP configuration information include the ipconfig utility on Windows machines and the ifconfig utility on Linux/*nix based machines. The Figure below shows an example of the ifconfig utility showing the IP configuration information of a queries host.



```
206.220.173.219 - PuTTY
zeus:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.219  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1114578 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1008426 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:389028395 (371.0 MiB)  TX bytes:610687218 (582.3 MiB)

eth0:1    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.220  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:2    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.221  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2392075 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2392075 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1471173328 (1.3 GiB)  TX bytes:1471173328 (1.3 GiB)

zeus:~#
```

Fig.30: ipconfig/ifconfig utility

✓ Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. DNS is used by everyone using the Internet to resolve commonly known domain names (i.e. google.com) to commonly unknown IP addresses (i.e. 74.125.115.147). When this system does not work, most of the functionality that people are used to goes away, as there is no way to resolve this information. The nslookup utility can be used to lookup the specific IP address (es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host. The Figure below shows an example of how the nslookup utility can be used to query the associated IP address information.

```
206.220.173.219 - PuTTY
zeus:~# nslookup www.google.com
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
www.google.com canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 74.125.47.99
Name:   www.l.google.com
Address: 74.125.47.103
Name:   www.l.google.com
Address: 74.125.47.104
Name:   www.l.google.com
Address: 74.125.47.105
Name:   www.l.google.com
Address: 74.125.47.106
Name:   www.l.google.com
Address: 74.125.47.147

zeus:~#
```

Fig.31: Nslookup utility

✓ Netstat

Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a specific port on local host. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. The Figure below shows an example of the netstat utility being used to display the currently active ports on a Linux machine.

```
206.220.173.219 - PuTTY
zeus:~# netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:imap2                  *:*                     LISTEN
tcp        0      0 localhost:spamd          *:*                     LISTEN
tcp        0      0 *:www                    *:*                     LISTEN
tcp        0      0 *:webmin                  *:*                     LISTEN
tcp        0      0 zeus.wilkinshouse.c:ftp  *:*                     LISTEN
tcp        0      0 zeus.sr-wconsulting:ftp  *:*                     LISTEN
tcp        0      0 206.220.173.221:domain  *:*                     LISTEN
tcp        0      0 zeus.sr-wconsult:domain *:*                     LISTEN
tcp        0      0 zeus.wilkinshous:domain *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                     *:*                     LISTEN
tcp        0      0 localhost:11000          *:*                     LISTEN
tcp        0      0 *:smtp                    *:*                     LISTEN
tcp        0      0 localhost:953            *:*                     LISTEN
tcp        0      0 *:https                   *:*                     LISTEN
tcp        0      0 *:20000                   *:*                     LISTEN
tcp        0      0 localhost:10023          *:*                     LISTEN
tcp        0      0 localhost:mysql          *:*                     LISTEN
tcp        0      0 *:pop3                    *:*                     LISTEN
zeus:~#
```

Fig.32: Netstat utility

- **Content/Topic 6 : Description of IP addressing forms**

Computer communications describes a process in which two or more computers or devices transfer data, instructions, and information.

In an IPv4 network, the hosts can communicate one of the following ways:

Unicast - The process of sending a packet from one host to an individual host

Multicast - The process of sending a packet from one host to a selected group of hosts, possibly in different networks

Broadcast - The process of sending a packet from one host to all hosts in the network

Anycast– The process of sending a packet from one host to single member of a group of potential receivers that are all identified by the same destination address.

These three types of communication are used for different purposes in data networks. In all three cases, the IPv4 address of the originating host is placed in the packet header as the source address.

✓ **Unicast Traffic**

Unicast communication is used for normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the addresses of the destination device as the destination address and can be routed through an internetwork.

In an IPv4 network, the unicast addresses applied to an end device is referred to as the host address. For unicast communication, the addresses assigned to the two end devices are used as the source and destination IPv4 addresses. During the encapsulation process, the source host places its IPv4 address in the unicast packet header as the source address and the IPv4 address of the destination host in the packet header as the destination address. Regardless of whether the destination specified a packet is a unicast, broadcast or multicast; the source address of any packet is always the unicast address of the originating host.

✓ **Multicast Transmission**

Multicast transmission is designed to conserve the bandwidth of an IPv4 network. It reduces traffic by allowing a host to send a single packet to a selected set of hosts that are part of a subscribing multicast group. To reach multiple destination hosts using unicast communication, a source host would need to send an individual packet addressed to each host. With multicast, the source host can send a single packet that can reach thousands of destination hosts. The internetwork's responsibility is to replicate the multicast flows in an efficient manner so that they reach only their intended recipients.

Some examples of multicast transmission are:

- Video and audio broadcasts
- Routing information exchange by routing protocols
- Distribution of software
- Remote gaming

✓ **Broadcast Transmission**

Broadcast traffic is used to send packets to all hosts in the network using the broadcast address for the network. With a broadcast, the packet contains a destination IP address with all ones (1s) in the host portion. This means that all hosts on that local network (broadcast domain) will receive and look at the packet. Many network protocols, such as DHCP, use broadcasts. When a host receives a packet sent to the network broadcast address, the host processes the packet as it would a packet addressed to its unicast address.

Some examples for using broadcast transmission are:

- Mapping upper layer addresses to lower layer addresses
- Requesting an address
- Unlike unicast, where the packets can be routed throughout the internetwork, broadcast packets are usually restricted to the local network. This restriction is dependent on the configuration of the gateway router and the type of broadcast. There are two types of broadcasts: directed broadcast and limited broadcast.

✓ **Anycast Transmission**

Anycast is a network addressing and routing methodology in which a single destination address has multiple routing paths to two or more endpoint destinations. Routers will select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route. Anycast networks are widely used for content delivery network (CDN) products to bring their content closer to the end user.

- **Content/Topic7: IP addressing modification**

✓ **IP broking and Firewalls**

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier

between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

How does a firewall work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest.

Types of firewalls

Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network.

✓ IP address translation

Network Address Translation

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.

LO3.3: Apply IPv6:

- **Content/Topic 1: Introduction to IPv6**

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

The exhaustion of IPv4 address had already been predicted in 1990s to be depleted within next 20 years when the World Wide Web became popular around the globe. However, the IPv4 network infrastructure is well stable in its service, it has several issues which are briefly highlighted with the improvement in IPv6 in this section.

IPv4 provides approximately 4.3 billion addresses, which is already depleted as announced by IANA. This is the main cause of birth of IPv6 having 128 bits address length. It has $2^{128} = 3.4 \times 10^{38}$ addresses where 80 bits is already an astronomical. It is expected that there will be living beings on other planets as well in the future and they shall be able to communicate as an inter-planet communication due to the sufficiency of IPv6 addresses.

NAT (Network Address Translation) is the technology which maps one public IPv4 address to many private addresses in the hidden zone. But unfortunately, NAT is not suitable to several applications which require end to end communication like FTP, NFS and group conferencing. NAT is not required in IPv6 due to the sufficiency of addresses in which every device shall have more than one IPv6 addresses. Address assignment is an issue in IPv4 network. Either Static (i.e. the network administrator manually set IPv4 address on every machine, which is a headache to set address for hundreds of machines in the LAN) or provide address dynamically via DHCP server, which raises machine renumbering problem making difficulties for network administrator to take control over the devices remotely. IPv6 has additionally unique approach called SLAAC (Stateless Address Auto-Configuration) in which every machine in the LAN calculates its interface identification number by using the technique like EUI-64 (SUFFIX) and receives always unique PREFIX via router advertisement.

An IPv6 address consists of eight groups of four hexadecimal digits. Here's an example IPv6 address:
3001:0da8:75a3:0000:0000:8a2e:0370:7334

This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4.

Advantages of IPv6

- Reliability
- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4. This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stronger Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

Disadvantages of IPv6

- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

Content/Topic 2 Migration from IPv4 to IPv6

There is not a single date to move to IPv6. For the foreseeable future, both IPv4 and IPv6 will coexist. The transition is expected to take years. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories:

- **Dual Stack** – As shown in Figure 1, dual stack allows IPv4 and IPv6 to coexist on the same network. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunnelling**– As shown in Figure 2, tunnelling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.

- **Translation** – As shown in Figure 3, Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.

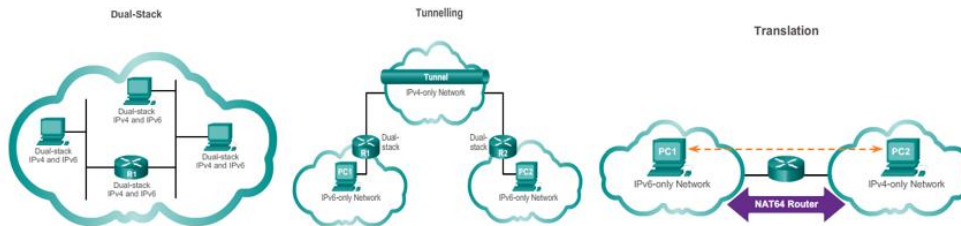


Fig.33: Categories of Migration from IPv4 to IPv6

- **Content/Topic 3: Introduction to Anatomy of IPv6 address**

Unlike IPv4 addresses that are expressed in dotted decimal notation, IPv6 addresses are represented using hexadecimal values. There are 128 bits (**binary digits**) in IPv6, which gets converted into a **hexadecimal** format so that it can be used in networking. That large set of 0's and 1's once converted will look like this IPv6 example format: **6e3d:e161:de2a:eb9e:28af:86bc:55a3:e5ce**.

This will be the new format of IP addresses going forward once IPv4 addresses run out, and they are quite a bit longer than most people are used to seeing.

An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ Zeroes can be omitted

2001:0DB8:AC10:FE01::

0010000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

Fig. 34: Translation of IPv6 from 128 bits to usable hexadecimal number

Parts of the IPv6 Address

As an IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the next figure, the x's represent hexadecimal numbers.

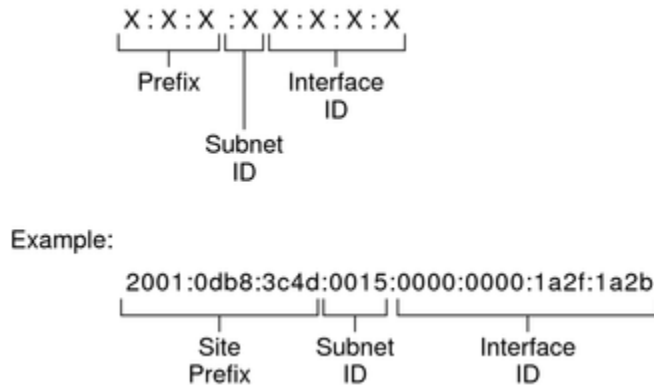


Fig. 35: Basic IPv6 Address Format

Assigning IPv6 addresses

Unlike IPv4, feature of IPv6 is a host's ability to auto-configure an interface. Through Neighbor Discovery, the host locates an IPv6 router on the local link and requests a site prefix. The host does the following, as part of the auto-configuration process:

- Creates a link-local address for each interface, which does not require a router on the link.
- Verifies the address's uniqueness on a link, which does not require a router on the link.
- Determines if the global addresses should be obtained through the stateless mechanism, the stateful mechanism, or both mechanisms. (Requires a router on the link.)

✓ Methods of assigning IP address

➤ Automatic method

Link-local Address is automatically configured from the interface MAC address. The scope of a link-local address is the intercommunication between hosts on the local area network. The link-local address allows IPv6 hosts to communicate when there is no router and no DHCPv6 server available on the local area network (LAN).

➤ **Static addressing method**

The IPv6 address, subnet prefix length and default gateway are configured manually in the system configuration file. However, it is possible to change the IPv6 address at runtime. The static configuration specifies also a primary and optional secondary DNS server. To make use of the static IPv6 configuration, you need to disable DHCP for IPv6.

➤ **Dynamic method**

Stateless auto-configuration

Automatic method or Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism enables a host to generate its own addresses. The stateless mechanism uses local information as well as nonlocal information that is advertised by routers to generate the addresses.

You can implement temporary addresses for an interface, which are also auto-configured. You enable a temporary address token for one or more interfaces on a host. However, unlike standard, auto-configured IPv6 addresses, a temporary address consists of the site prefix and a randomly generated 64 bit number. This random number becomes the interface ID portion of the IPv6 address. A link-local address is not generated with the temporary address as the interface ID.

Routers advertise all prefixes that have been assigned on the link. IPv6 hosts use Neighbor Discovery to obtain a subnet prefix from a local router. Hosts automatically create IPv6 addresses by combining the subnet prefix with an interface ID that is generated from an interface's MAC address. In the absence of routers, a host can generate only link-local addresses. Link-local addresses can only be used for communication with nodes on the same link.

Stateful Auto configuration Model

In the stateful auto configuration model, hosts obtain interface addresses or configuration information and parameters from a server. Servers maintain a database that checks which addresses have been assigned to which hosts. The stateful auto configuration protocol allows hosts to obtain addresses and other configuration information from a server. Stateless and stateful auto configuration complement each other. For example, a host can use stateless auto configuration to configure its own addresses, but use stateful auto configuration to obtain other information.

When to Use Stateless and Stateful Approaches

The stateless approach is used when a site is not concerned with the exact addresses that hosts use. However, the addresses must be unique. The addresses must also be properly routable. The stateful approach is used when a site requires more precise control over exact address assignments. Stateful and stateless address auto configuration can be used simultaneously. The site administrator specifies which type of auto configuration to use through the setting of appropriate fields in router advertisement messages.

- **Content/Topic 5: Calculation of IP Addressing**

- ✓ **Sub-netting an IPv6 Network**

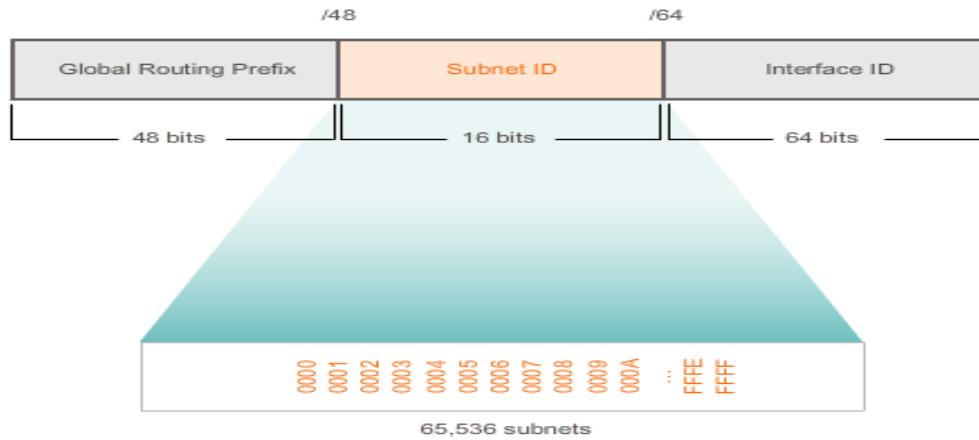
IPv6 sub-netting requires a different approach than IPv4 sub-netting. The primary reason is that with IPv6 there are so many addresses, that the reason for sub-netting is completely different. An IPv6 address space is not sub-netted to conserve addresses; rather, it is sub-netted to support hierarchical, logical design of the network. While IPv4 sub-netting is about managing address scarcity, IPv6 sub-netting is about building an addressing hierarchy based on the number of routers and the networks they support.

Recall that an IPv6 address block with a /48 prefix has 16 bits for subnet ID, as shown in Figure 1. Sub-netting using the 16 bit subnet ID yields a possible 65,536 /64 subnets and does not require borrowing any bits from the interface ID, or host portion of the address. Each IPv6 /64 subnet contains roughly eighteen quintillion addresses, obviously more than will ever be needed in one IP network segment.

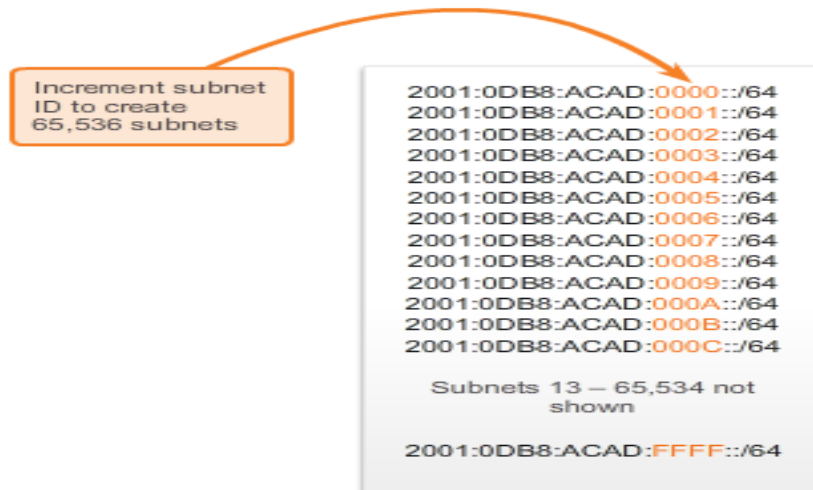
Subnets created from the subnet ID are easy to represent because there is no conversion to binary required. To determine the next available subnet, just count up in hexadecimal. As shown in Figure 2, this means counting by hexadecimal in the subnet ID portion.

The global routing prefix is the same for all subnets. Only the subnet ID quartet is incremented for each subnet.

IPv6 /48 Address Block



Address Block: 2001:0DB8:ACAD::/48



With over 65,000 subnets to choose from, the task of the network administrator becomes one of designing a logical scheme to address the network.

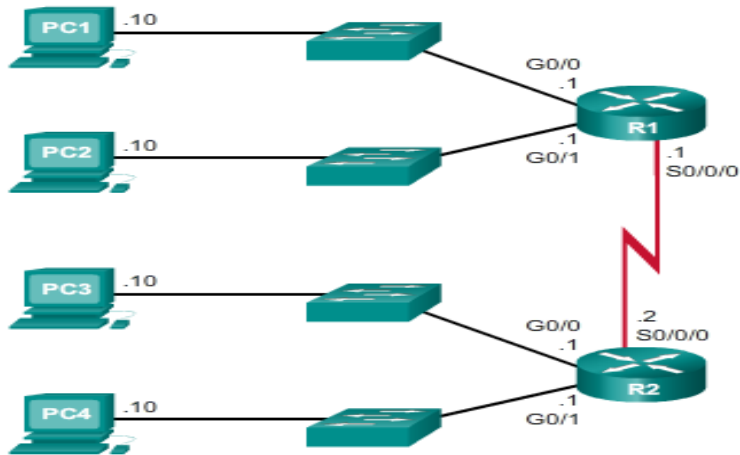
As shown in Figure 1, the example topology will require subnets for each LAN as well as for the WAN link between R1 and R2. Unlike the example for IPv4, with IPv6 the WAN link subnet will not be subnetted further. Although this may “waste” addresses, that is not a concern when using IPv6.

As shown in Figure 2, the allocation of 5 IPv6 subnets, with the subnet ID field 0001 through 0005 will be used for this example. Each /64 subnet will provide more addresses than will ever be needed.

As shown in Figure 3, each LAN segment and the WAN link is assigned a /64 subnet.

Similar to configuring IPv4, Figure 4 shows that each of the router interfaces has been configured to be on a different IPv6 subnet.

Example Topology



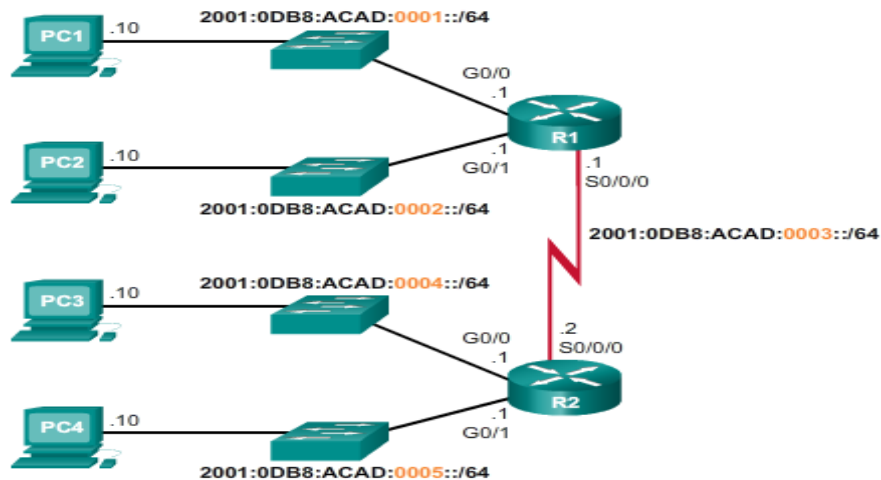
IPv6 Subnetting

Address Block: 2001:0DB8:ACAD::/48

5 subnets allocated
from 65,536 available
subnets

```
2001:0DB8:ACAD:0000::/64
2001:0DB8:ACAD:0001::/64
2001:0DB8:ACAD:0002::/64
2001:0DB8:ACAD:0003::/64
2001:0DB8:ACAD:0004::/64
2001:0DB8:ACAD:0005::/64
2001:0DB8:ACAD:0006::/64
2001:0DB8:ACAD:0007::/64
2001:0DB8:ACAD:0008::/64
...
2001:0DB8:ACAD:FFFF::/64
```

IPv6 Subnet Allocation



IPv6 Address Configuration



```
R1 (config)#interface gigabitethernet 0/0
R1 (config-if)#ipv6 address 2001:db8:acad:1::1/64
R1 (config-if)#exit
R1 (config)#interface gigabitethernet 0/1
R1 (config-if)#ipv6 address 2001:db8:acad:2::1/64
R1 (config-if)#exit
R1 (config)#interface serial 0/0/0
R1 (config-if)#ipv6 address 2001:db8:acad:3::1/64
R1 (config-if)#end
R1#
```

Similar to borrowing bits from the host portion of an IPv4 address, with IPv6 bits can be borrowed from the interface ID to create additional IPv6 subnets. This is typically done for security reasons to create fewer hosts per subnet and not necessarily to create additional subnets.

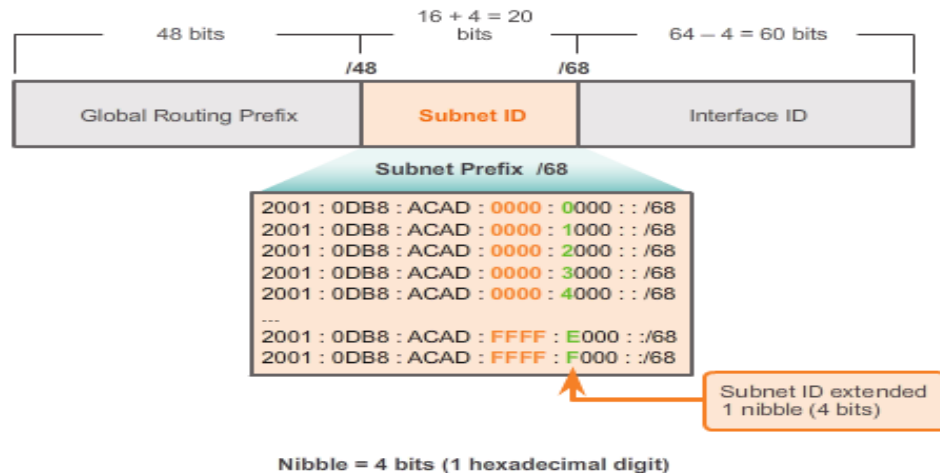
When extending the subnet ID by borrowing bits from the interface ID, the best practice is to subnet on a nibble boundary. A nibble is 4 bits or one hexadecimal digit. As shown in the figure, the /64 subnet prefix is extended 4 bits or 1 nibble to /68. Doing this reduces the size of the interface ID by 4 bits, from 64 to 60 bits.

Subnetting on nibble boundaries means only using nibble aligned subnet masks. Starting at /64, the nibble aligned subnet masks are /68, /72, /76, /80, etc.

Subnetting on a nibble boundary creates subnets by using the additional hexadecimal value. In the example, the new subnet ID consists of the 5 hexadecimal values, ranging from 00000 through FFFFF.

It is possible to subnet within a nibble boundary, within a hexadecimal digit, but it is not recommended or even necessary. Subnetting within a nibble takes away the advantage easily determining the prefix from the interface ID. For example, if a /66 prefix length is used, the first two bits would be part of the subnet ID and the second two bits would be part of the interface ID.

Subnetting on a Nibble Boundary



Your network administrator wants you to assign five /64 IPv6 subnets to the network shown in the topology. Your job is to determine the IPv6 subnets, assign IPv6 addresses to the routers, and set the PCs to automatically receive IPv6 addressing. Your final step is to verify connectivity between IPv6 hosts.

✓ Summarization

As shown in the figure, the process of segmenting a network, by dividing it into to multiple smaller network spaces, is called sub-netting.

Every network address has a valid range of host addresses. All devices attached to the same network will have an IPv4 host address for that network and a common subnet mask or network prefix. Traffic can be forwarded between hosts directly if they are on the same subnet. Traffic cannot be forwarded between subnets without the use of a router. To determine if traffic is local or remote, the router uses the subnet mask. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

IPv4 subnets are created by using one or more of the host bits as network bits. Two very important factors that will lead to the determination of the IP address block with the subnet mask, are the number of subnets required and the maximum number of hosts needed per subnet. There is an inverse relationship between the number of subnets and the number of hosts. The more bits borrowed to create subnets the fewer host bits are available; therefore fewer hosts per subnet.

The formula 2^n (where n is the number of host bits remaining) is used to calculate how many addresses will be available on each subnet. However, the network address and broadcast address within a range are not useable; therefore, to calculate the useable number of addresses the calculation $2^n - 2$ is required.

Sub-netting a subnet, or using Variable Length Subnet Mask (VLSM) was designed to avoid wasting addresses.

IPv6 sub-netting requires a different approach than IPv4 sub-netting. An IPv6 address space is not sub-netted to conserve addresses; rather it is sub-netted to support hierarchical, logical design of the network. So, while IPv4 sub-netting is about managing address scarcity, IPv6 sub-netting is about building an addressing hierarchy based on the number of routers and the networks they support.

Careful planning is required to make best use of the available address space. Size, location, use, and access requirements are all considerations in the address planning process.

After it is implemented, an IP network needs to be tested to verify its connectivity and operational performance.

Original	192.	168.	1.	0	000	0000	Network: 192.168.1.0/24
Mask	255.	255.	255.	0	000	0000	Mask: 255.255.255.0

Borrowing 1 bit creates 2 subnets with the same mask.

Net 0	192.	168.	1.	0	000	0000	Network: 192.168.1.0/25
Mask	255.	255.	255.	1	000	0000	Mask: 255.255.255.128

Net 1	192.	168.	1.	1	000	0000	Network: 192.168.1.128/25
Mask	255.	255.	255.	1	000	0000	Mask: 255.255.255.128

✓ Binary to Hexadecimal and Hexadecimal to Binary conversion

Converting from binary to hex is easy since hexadecimal numbers are simplified versions of binary strings. You just need to remember that each hex digit represents four binary digits. It follows that four binary digits will be equal to one hex digit. The method is easier than it sounds but it's always useful to use a binary to hex conversion chart to save time.

Step 1: Write down the binary number and group the digits (0's and 1's) in sets of four. Start doing this from the right. If the leftmost group doesn't have enough digits to make up a set of four, add extra 0's to make a group.

Step 2: Write 8, 4, 2 and 1 below each group. These are the weights of the positions or place holders in the number (2^3 , 2^2 , 2^1 and 2^0).

Step 3: Every group of four in binary will give you one digit in hexadecimal. Multiply the 8, 4, 2 and 1's by the digit above.

Step 4: Add the products within each set of four. Write the sums below the groups they belong to.

Step 5: The digits you get from the sums in each group will give you the hexadecimal number, from left to right.

Now, let's apply these steps to, for example, the binary number $(10101010)_2$

Step 1: 10101010 has eight digits and therefore can be grouped in sets of four without adding 0's.

Think of the number as (1010)(1010)

Step 2: Write 8, 4, 2 and 1 below each group.

1010 1010

8421 8421

Step 3: Multiply the 8, 4, 2 and 1's with the digit above.

1010 1010

8421 8421

8020 8020

Step 4: Add the products within each set of four.

In the first group, $8 + 2 = 10$

In the second group, $8 + 2 = 10$

Write these digits below the groups they belong to.

1010 1010

8421 8421

8020 8020

10 10

Step 5: Notice that, in order to represent values above 9, letters will be used. 10 is represented as the letter A in the hexadecimal system. Therefore, $(10101010)_2 = (AA)_{16}$

Binary to Hex Conversion Examples

Example 1: $(10001110)_2 = (8E)_{16}$

1000 1110

8421 8421

8000 8420

8 15

8 E

- **Content/Topic 6 : Testing IP Addressing and IP Address form**

✓ Diagnostic and testing tools

The Network Diagnostic Tool (NDT) is a client/server program that provides network configuration and performance testing to a user's desktop or laptop computer. The system is composed of a client program (command line or java applet) and a pair of server programs (a webserver and a testing/analysis engine).

Several studies have shown that the majority of network performance problems occur in or near the users' desktop/laptop computer. These problems include, but are not limited to, duplex mismatch conditions on Ethernet/Fast Ethernet links, incorrectly set TCP buffers in the user's computer, or problems with the local network infrastructure. The NDT is designed to quickly and easily identify a specific set of conditions that are known to impact network performance.

Network troubleshooting tools are a necessity for every network administrator. When you are in the networking field, you may find a mass number of tools that can be used to troubleshoot a variety of different network conditions. The general and common used network troubleshooting tools include but not limited to:

- Ping
- Tracert/ Trace Route
- Ipconfig/ ifconfig
- Netstat
- Nslookup
- Pathping/MTR
- Route
- PuTTY

✓ IP Addressing forms

Unicast

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. As shown in the figure, a source IPv6 address must be a unicast address.

Multicast

An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.

Anycast

An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

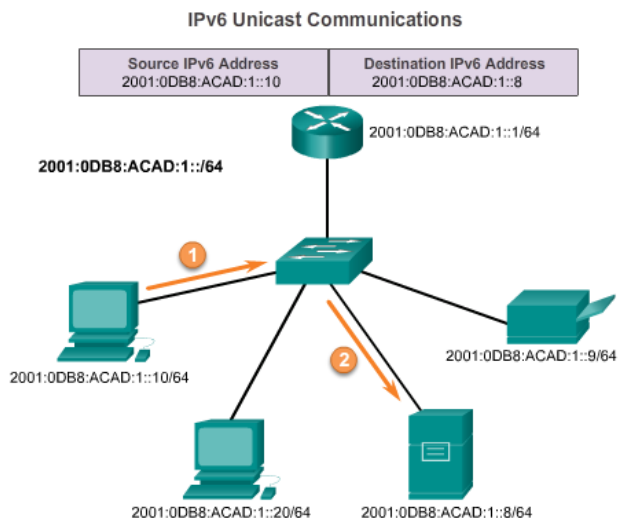


Fig. 36: IPv6 Unicast Communication

References

Dordal, P. L. (2020). An Introduction to Computer Network. Chicago.

Malay Kumar Kundu, D. P. (2014). Advance Computing Networking and Informatics. Canberra.

Olivier, B. (2011). Computer Networking: Principles, Protocols and Practice.

Rackly, S. (2007). Wireless Network Technology. Oxford.

Reid, A. (2007). WAN Technologies, CCNA4 Companion Guid. India.

Sosinsky, B. (2009). Networking Bible. Indianapolis: Wiley publication Inc.

