1. Internetworking &devices: Repeaters, Hubs, Bridges, Switches, Router, Gateway
2. Addressing: Internet address, classful address
3. Subnetting
4. Routing: techniques, static vs. dynamic routing, routing table for classful address
5. Routing Protocols: RIP, OSPF, BGP, Unicast and multicast routing protocols
6. Routing algorithms: shortest path algorithm, flooding, distance vector routing, link state routing; Protocols: ARP, RARP, IP, ICMP

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

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

Network Layer Functions

Devices of Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Network Layer Features

With its standard functionalities, Layer 3 can provide various features as:

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.
- helps to communicate end to end devices over the internet. It comes in two flavors.

Layer 3 network addressing is one of the major tasks of Network Layer always points to host / node / server or it can represent a whole network. Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

There are different kinds of network addresses in existence: IP, IPX, AppleTalk

IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent as shown in below figure…

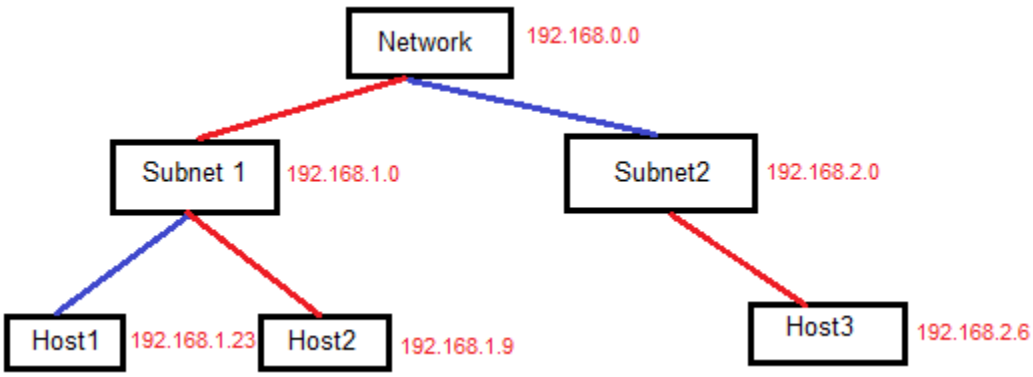


Fig. IP Address assigning in Hierarchical Manner

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

Routers take help of routing tables, which has the following information: -

- Method to reach the network
- Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination.
- The next router on the path follows the same thing and eventually the data packet reaches its destination.

4.1 Networking & Devices : Repeaters, Hubs, Bridges, Switches, Router, Gateway

Repeaters: Physical Layer devices

Repeaters are used in transmission systems to replicate or regenerate analog or digital signals distorted by transmission loss. **Analog Repeaters** frequently can only amplify the signal while **Digital Repeaters** can reconstruct a signal to near its original quality.

In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. **Hubs** can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.

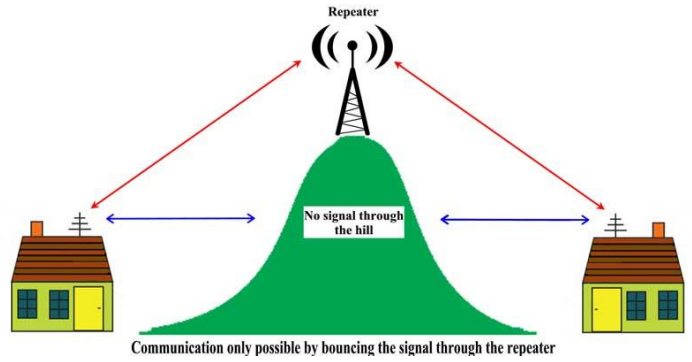
A repeater does exactly that- it repeats any electrical signals that come into one port, out its other port. (there are only 2 ports on a repeater). It is a very "dumb" device (no offense to any of you repeaters out there).

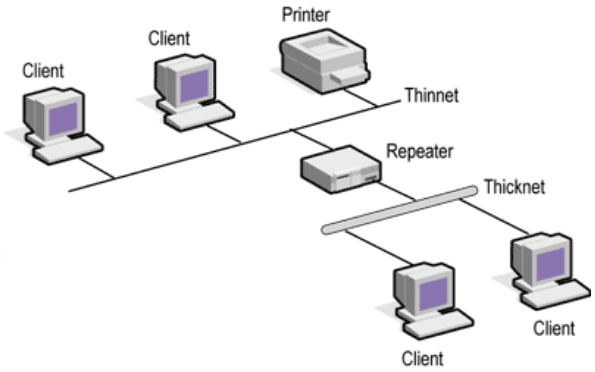
Example :-

- In a **wireless communications system**, a repeater consists of a radio receiver, an amplifier, a transmitter, an isolator, and two antennas. The transmitter produces a signal on a frequency that differs from the received signal. This so-called frequency offset is necessary to prevent the strong transmitted signal from disabling the receiver. The isolator provides additional protection in this respect. A repeater, when strategically located on top of a high building or a mountain, can greatly enhance the performance of a wireless network by allowing communications over distances much greater than would be possible without it.
- In **satellite wireless**, a repeater (more frequently called a transponder) receives uplink signals and retransmits them, often on different frequencies, to destination locations.
- In a **cellular telephone system,** a repeater is one of a group of transceivers in a geographic area that collectively serve a system user.
- In a **fiber optic network,** a repeater consists of a photocell, an amplifier, and a light-emitting diode (LED) or infrared-emitting diode (IRED) for each light or IR signal that requires amplification. Fiber optic repeaters operate at power levels much lower than wireless repeaters, and are also much simpler and cheaper. However, their design requires careful attention to ensure that internal circuit noise is minimized.

Repeaters are commonly used by commercial and unprofessional radio operators to extend signals in the radio frequency range from one receiver to another. These consist of ***drop repeaters***, similar to the cells in cellular radio, and ***hub repeaters***, which receive and retransmit signals from and to a number of directions.

A *bus repeater* links one computer bus to a bus in another computer chassis, essentially chaining one computer to another.





HUB: Physical Layer devices

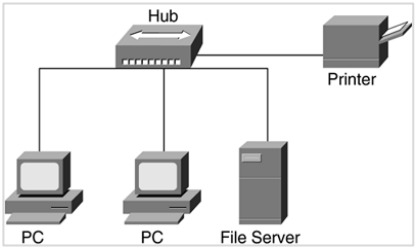
Hubs are very similar to repeaters. A Hub is essentially a multiport repeater. Any electrical signal that comes into one port, goes out all other ports. Again, a very dumb device.

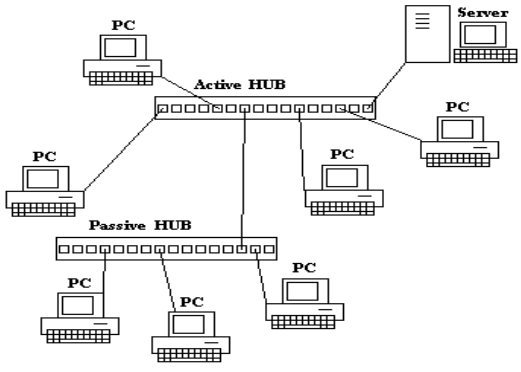
- fundamentally used in networks that use twisted pair cabling to connect devices.
- Act as pathways to direct electrical signals to travel along.

Hub Categories

***Passive Hub:** A passive hub is just a connector, it just split the signal. No-need of power supply.

***Active Hub:** an active hub is actually a multiport repeater. which can amplify or regenerate the information signal. This type of bus has an advantage as it also amplifies the incoming signal as well as forward it to multiple devices. Need power supply





Switches

- A switch when compared to bridge has multiple ports.
- Switches can perform error checking before forwarding data.
- Switches are very efficient by forwarding good packets selectively to correct devices only by checking MAC address in table, otherwise transmits to all.
- Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch.
- Usually large networks use switches instead of hubs to connect computers within the same subnet.

Bridges: Data Link Layer devices

- A bridge is more complex than hub.
- A bridge maintains a MAC address table for both LAN segments it is connected to.
- Bridge has a single incoming and outgoing port.
- Bridge filters traffic on the LAN by looking at the MAC address.
- **Data filtering**- bridge looks at the destination address before forwarding unlike a hub. It restricts transmission on other LAN segment if destination is not found.
- Bridges are used to separate parts of a network that do not need to communicate regularly, but need to be connected.

Routers

- A router, like a switch forwards packets based on address.
- A router uses the IP address to forward packets. This allows the network to go across different protocols.
- Routers forward packets based on software while a switch (Layer 3 for example) forwards using hardware called ASIC (Application Specific Integrated Circuits)
- Routers support different WAN technologies but switches do not.
- Wireless Routers have Access Point built in.
- The most common home use for routers is to share a broadband internet connection. The router has a public IP address and that address is shared with the network. When data comes through the router it is forwarded to the correct computer.

Fig. Switch

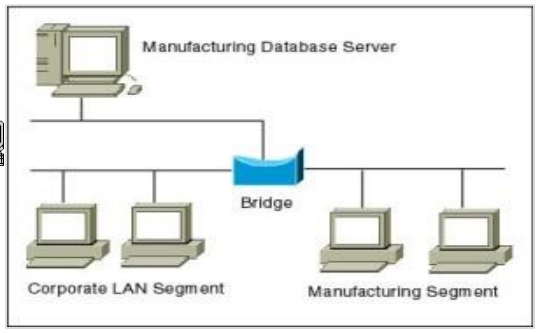


Fig. Bridge

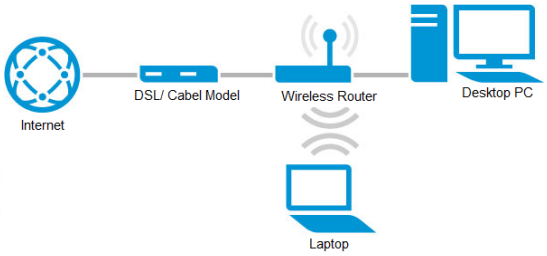
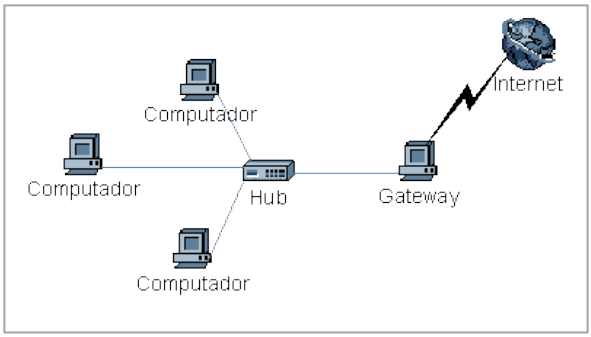


Fig. Router

Gateways

- Gateway is also a router, which forwards the traffic of a subnetwork to other or to the internet.
- Gateway acts as an intermediary device between computers in the subnet with other computers outside the subnet. All the traffic to the outside of subnet must go through the gateway.
- Gateways are also useful in forwarding traffic from one ISP (AS) to the other, those are called **border gateways.**
- When you are connected to the access point, all the systems which are connected to the same access point are in same subnet and can directly communicate. When you make a request to some server out there in the internet, then your packet will go through the configured gateway which is provided by your DHCP server.



4.2 Addressing : Internet Address, Classful Address

An Internet address uniquely identifies a node on the Internet. Internet address may also refer to the name or IP of a Web site (URL),someone's e-mail address.

In classless addressing variable-length blocks are assigned that belong to no class. In this architecture, the entire address space (232 addresses) is divided into blocks of different sizes.

Classful is based on the default Class A,B or C networks.

All devices in the same routing domain must use the same subnet mask. Since routers running a classful routing protocol do not include subnet mask information with routing updates, the router assumes either its own subnet mask, or defaults to the classful subnet mask.

Classless on the other hand, allows the use of variable length subnet masks, or Variable-Length Subnet Masking (VLSM), because subnet mask information is included with routing updates. You can have a mixture of different subnet masks in the same routing domain: - 10.1.0.0/19, 10.2.0.0/20, 172.16.8.0/21, 172.16.16.0/24

Classful addressing:

- In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.
- Each of the IP address belongs to a particular class that's why they are classful addresses.
- Earlier this addressing system did not have any name, but when classless addressing system came into existence then it is named as Classful addressing system.
- The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device.
- One of the major disadvantage of classful addressing is that it does not send subnet information but it will send the complete network address. The router will supply its own subnet mask based on its locally configured subnets. As long as you have the same subnet mask and the network is contiguous, you can use subnets of a classful network address.

Host *IP* address - The Host ID portion of an IP address, is the portion of the address used to identify hosts (any device requiring a Network Interface Card, such as a PC or networked printer) on the network. *e.g. ip add 192.168.100.2 and subnet mask 255.255.255.0 now 192.168.100.X is network id which is used to identify from which network u belongs to and x is host id which is unique for every node on network*

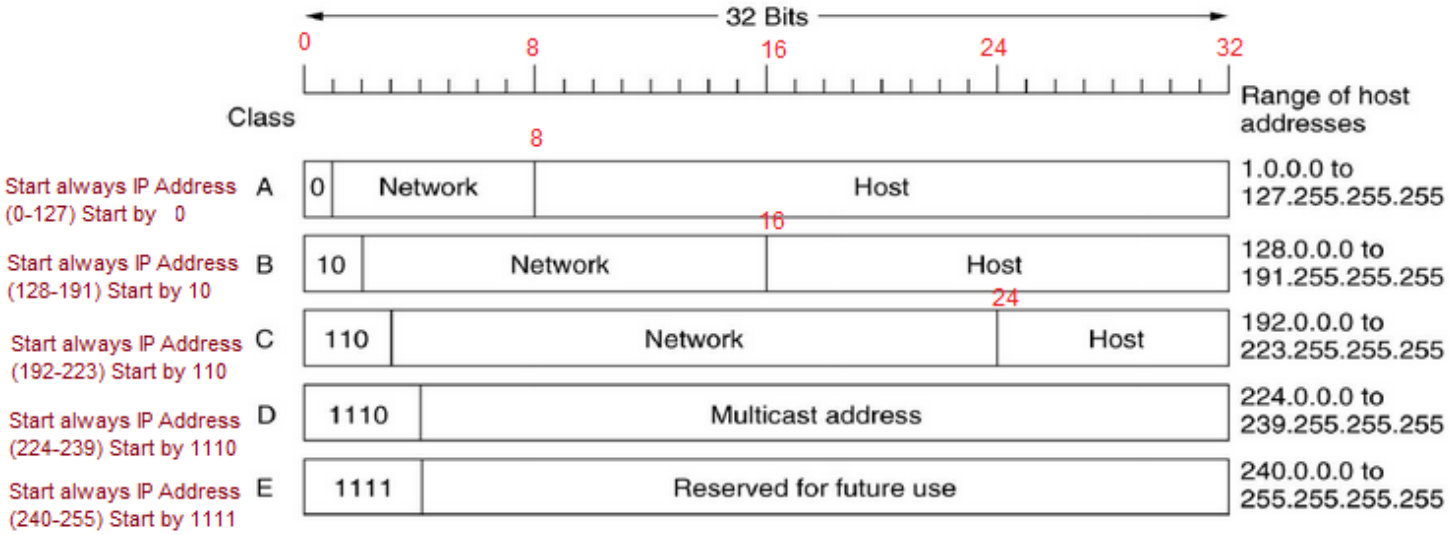


Table 43: IP Address Classes and Class Characteristics and Uses

IP Address Class	Fraction of Total IP Address Space	n = Number Of Network ID Bits	p = Number Of Host ID Bits	IP Range	Intended Use
Class A	1/2	8	24	0-127	Unicast addressing for very large organizations with hundreds of thousands or millions of hosts to connect to the Internet.
Class B	1/4	16	16	128-191	Unicast addressing for medium-to-large organizations with many hundreds to thousands of hosts to connect to the Internet.
Class C	1/8	24	8	192-223	Unicast addressing for smaller organizations with no more than about 250 hosts to connect to the Internet.
Class D	1/16	n/a	n/a	224-239	IP multicasting.
Class E	1/16	n/a	n/a	240-255	Reserved for “experimental use”.

Class	Starting Bits (fixed to m bits)	Example	Max Networks 2^{n-m}	Max Hosts 2^p-2	Default subnet mask
A	0 (m=1)	125.168.3.5 = 01111101.10101000.0000011.00000101	2^{8-1} = 126	2^{24}-2= 16,777,214	255.0.0.0
B	10 (m=2)	155.168.3.5 = 10011011.10101000.0000011.00000101	2^{16-2} = 16,384	2^{16}-2=65,534	255.255.0.0
C	110 (m=3)	192.168.3.5 = 1100000.10101000.0000011.00000101	2^{24-3} = 2,097,152	2^8-2=254	255.255.255.0
D	1110				
E	1111				

Private IP Address

- A private IP address is an IP address that's reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public.
- Private IP addresses are in contrast to public IP addresses, which are public and cannot be used within a home or business network.
- Sometimes a private IP address is also referred to as a *local IP address*.
- The Internet Assigned Numbers Authority (IANA) reserves the following IP address blocks for use as private IP addresses:
  i. **10.0.0.0 to 10.255.255.255**, allows over 16 million addresses
  ii. **172.16.0.0 to 172.31.255.255**, allows over 1 million addresses
  iii. **192.168.0.0 to 192.168.255.255**, allows over 65,000 addresses

Reserved IP Address

- Another set of IP addresses that are restricted even further are called *reserved* IP addresses.
- These are similar to private IP addresses in the sense that they can't be used for communicating on the greater internet, but they're even more restrictive than that.
- The most famous reserved IP is 127.0.0.1. This address is called the loopback address and is used to test the network adapter or integrated chip. No traffic addressed to 127.0.0.1 is sent over the local network or public internet.
- Technically, the entire range from **127.0.0.0 to 127.255.255.255** is reserved for loopback purposes but you'll almost never see anything but 127.0.0.1 used in the real world.
- The range from **0.0.0.0 to 0.255.255.255** are also reserved but don't do anything at all.

Google Public DNS operates recursive name servers for public use at the two following IP addresses: **8.8.8.8** and 8.8.4.4 for IPv4 service, as well as 2001:4860:4860::8888 and 2001:4860:4860::8844, for IPv6 access.

4.3 Subnetting

- Is a process of dividing large network into the smaller networks known as subnets based on layer 3 IP address. Every computer on network has an IP address that represent its location on network. Two version of IP addresses are available IPv4 and IPv6.

Example :- Being a network administrator you are asked to create two networks, each will host 30 systems.

Single class C IP range can fulfill this requirement, still you have to purchase 2 class C IP range, one for each network. Single class C range provides 256 total addresses and we need only 30 addresses, this will waste 226 addresses. These unused addresses would make additional route advertisements slowing down the network.

In a **/24 network** you can't use **0** because it is the identification of the network (devices use it to recognize the different networks they are connected to). The last address, **255** in the case of a **/24** network, is the broadcast address. Devices connected to the network use it to send a broadcast, a message intended for all devices on the network.

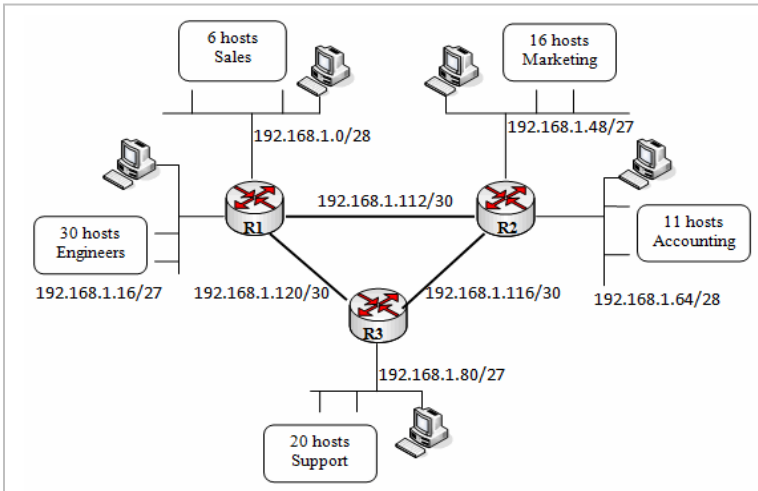


Figure 3.3. Subnetting example

Advantage of Subnetting

- Subnetting breaks large network in smaller networks and smaller networks are easier to manage.
- Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
- Subnetting allows you to apply network security polices at the interconnection between subnets.
- Subnetting allows you to save money by reducing requirement for IP range.

Subnet mask : Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

For example, how will figure out network partition and host partition from IP address 192.168.1.10? Here we need subnet mask to get details about network address and host address.

- In decimal notation subnet mask value 1 to 255 represent network address and value 0 [Zero] represent host address.
- In binary notation subnet mask on bit [1] represent network address while off bit [0] represent host address.

- Network ID: First address of subnet is called network ID. This address is used to identify one segment or broadcast domain from all the other segments in the network.
- Block Size: Block size is size of subnet including network address, hosts address and broadcast address.
- Broadcast ID: There are two types of broadcast, direct broadcast and full broadcast.
  (i)Direct broadcast: or local broadcast is the last address of subnet and can be hear by all hosts in subnet.
  (ii)Full broadcast: is the last address of IP classes and can be hear by all IP hosts in network. Full broadcast address is 255.255.255.255
- The main difference between direct broadcast and full broadcast is that routers will not propagate local broadcasts between segments, but they will propagate directed broadcasts.
- Host Addresses: All address between the network address and the directed broadcast address is called host address for the subnet. You can assign host addresses to any IP devices such as PCs, servers, routers, and switches.

CIDR [Classless Inter Domain Routing]

CIDR is a slash notation of subnet mask. CIDR tells us number of on bits in a network address.

Example: **192.30.250.0/18** - The "192.30.250.0" is the network address itself and the "18" says that the first 18 bits are the network part of the address, leaving the last 14 bits for specific host addresses.

192.30.250.0 = 11000000 00011110 11111010 00000000

- **Class A** has default subnet mask **255.0.0.0**. that means first octet of the subnet mask has all on bits. In slash notation it would be written as **/8**, means address has 8 bits on.
- **Class B** has default subnet mask **255.255.0.0.** that means first two octets of the subnet mask have all on bits. In slash notation it would be written as **/16,** means address has 16 bits on.
- **Class C** has default subnet mask **255.255.255.0.** that means first three octets of the subnet mask have all on bits. In slash notation it would be written as **/24**, means address has 24 bits on.

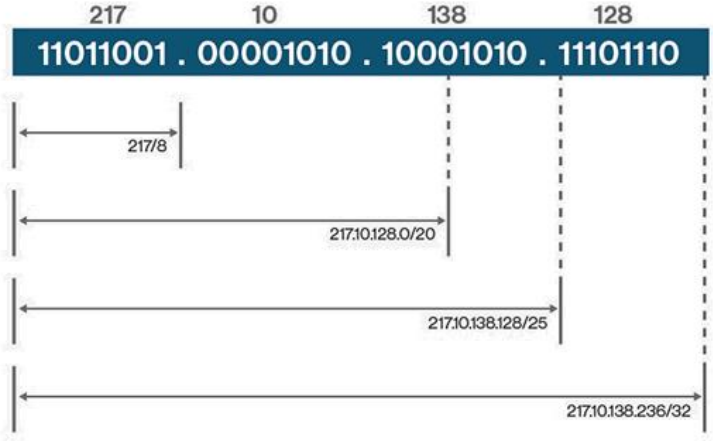


Fig CIDR Example

4.4 Routing: techniques, static vs dynamic routing, routing table for classful address

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. Routing is performed for many types of networks, (i)including circuit-switched networks, such as the public switched telephone network (PSTN), (ii) computer networks, such as the Internet, as well as (iii) in networks used in public and private transportation, such as the system of streets, roads, and highways in national infrastructure.

Routing is the process that a router uses to forward packets toward the destination network. The router makes the decision based upon the destination IP address of a packet. To make the correct decisions router must learn how to reach remote networks. The routing algorithm is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

Techniques of routing

1) **Static Routing :** In this technique router is configured manually. Static routing manually sets up the optimal paths between the source and the destination computers.
   - A Static route is a route that is manually entered by a network administrator. This is known as non-adaptive routing because the router will always use this static route when sending data, i.e. the data path is predetermined by the administrator. Static routes are useful for network security.
   - If there is a fault with any of the routes then the system administrator will have to go to the affected routers and make the required changes to get the system working again. The overuse of static routing is not recommended because the main function of a router is to learn and plan new paths for data in the event of system failures.

2) **Dynamic Routing :** Dynamic routing makes it possible to avoid the configuration of the static routes. On the other hand, the Dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.

- Most routers are dynamic with the capability of being statically configured
- Dynamic routing involves the regular communication of routers with other routers. This allows the routers to learn and adapt to a changing environment. This is the embodiment of packet switching with routers automatically adapting to network changes and even system failures.

Routing schemes differ in how they deliver messages:

- Unicast delivers a message to a single specific node
- Anycast delivers a message to anyone out of a group of nodes, typically the one nearest to the source
- Multicast delivers a message to a group of nodes that have expressed interest in receiving the message
- Geocast delivers a message to a geographic area
- Broadcast delivers a message to all nodes in the network

Static vs Dynamic routing

• The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths. The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network. Also, the dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination. If any router is down or faulty due to certain reasons, this fault is circulated in the entire network. Due to this quality of the dynamic routers, they are also called adaptive routers.

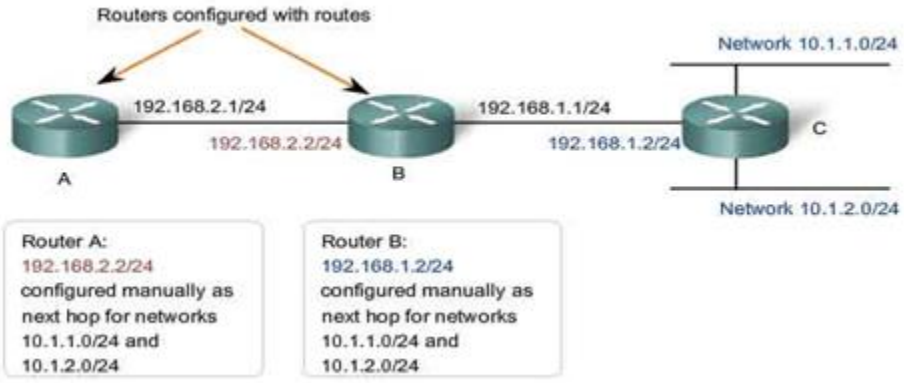
• The static routing is suitable for very small networks and they cannot be used in large networks. As against this, dynamic routing is used for larger networks. The manual routing has no specific routing algorithm. The dynamic routers are based on various routing algorithms like OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) and RIP (Routing Information Protocol).

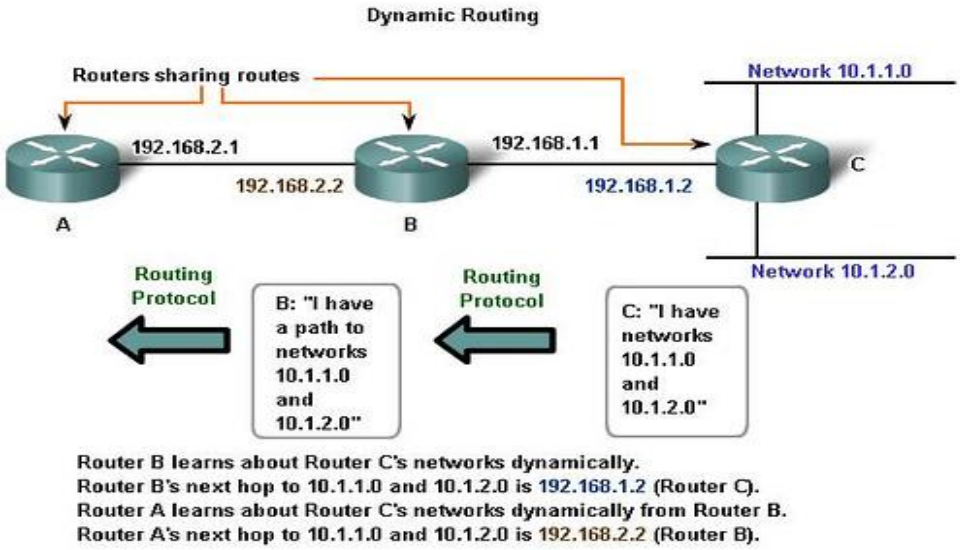
• The static routing is the simplest way of routing the data packets from a source to a destination in a network. The dynamic routing uses complex algorithms for routing the data packets.

• The static routing has the advantage that it requires minimal memory. Dynamic router, however, have quite a few memory overheads, depending on the routing algorithms used.

• The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing. In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

Static	Dynamic
1. The paths are pre-computed by a host and are loaded into routing table. 2. The paths are fixed for long duration of time. 3. static routing is good when • network size is small, • traffic load does not change variably • network topology is fixed 4. Does not scale to large network 5. Disadvantage is its inability to react rapidly to network failures.	1. Each node computes the best path by communicating with its neighbors. 2. each node continuously learn the state of network by communicating with its neighbors 3. Adapt to changes in network conditions 4. Scales well 5. Disadvantage is added complexity in the node.





Routing table for classful address

IPV4 contain the 32-bit number to represent the internet address. This 32-bit number has the different format for different classes. There are 5 classes i.e. A, B, C, D, E. There were three address *classes* to choose from: A,B, C corresponding to 8-bit, 16-bit, or 24-bit prefixes. No other prefix lengths were allowed, and there was no concept of nesting a group of 24-bit prefixes, for example, within a 16-bit prefix.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of logically addressed network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing.

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.

A basic routing table includes the following information:

- **Destination**: The IP address of the packet's final destination
- **Next hop**: The IP address to which the packet is forwarded
- **Interface**: The outgoing network interface the device should use when forwarding the packet to the next hop or final destination
- **Metric**: Assigns a cost to each available route so that the most cost-effective path can be chosen
- **Routes**: Includes directly-attached subnets, indirect subnets that are not attached to the device but can be accessed through one or more hops, and default routes to use for certain types of traffic or when information is lacking.

Routing tables are also a key aspect of certain security operations, such as *unicast reverse path forwarding* (URPF). In this technique, which has several variants, the router also looks up, in the routing table, the *source address* of the packet. If there exists no route back to the source address, the packet is assumed to be malformed or involved in a network attack, and is dropped.

Network id	Cost	Next hop
.....	.....	.....
.....	.....	.....

Shown below is an example of what the table above could look like on an average computer connected to the internet via a home router:

Network Destination	Netmask	Gateway/ Next hop	Interface	Metric
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.100	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	192.168.0.100	192.168.0.100	10
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.0.1	255.255.255.255	192.168.0.100	192.168.0.100	10

- The column **Network Destination** and **Netmask** together describe the **Network id** as mentioned earlier. For example, destination **192.168.0.0** and netmask **255.255.255.0** can be written as network id **192.168.0.0/24**.

- The **Gateway** column contains the same information as the **Next hop**, i.e. it points to the gateway through which the network can be reached.
- The **Interface** indicates what locally available interface is responsible for reaching the gateway. In this example, gateway **192.168.0.1** (the internet router) can be reached through the local network card with address **192.168.0.100**.
- Finally, the **Metric** indicates the associated cost of using the indicated route. This is useful for determining the efficiency of a certain route from two points in a network. In this example, it is more efficient to communicate with the computer itself through the use of address **127.0.0.1** (called "localhost") than it would be through **192.168.0.100** (the IP address of the local network card).

4.5 Routing Protocols : RIP, OSPF, BGP, Unicast and Multicast routing protocols

* RIP (Routing Information Protocol)

RIP is the distance vector routing protocol which means that each router may not know where the final destination network is, but it does know in which direction it exists and how far away it is. It employs the hop count as the routing metrics. Hop count is the number of a router the packet must travel till it reaches its destination. RIP uses the hop count to determine the best path between the router/location. Each router contains the RIP table and the table is updated in every 30 seconds. Each router broadcasts its entire RIP table to its neighbor.

How RIP works:

What makes RIP work is a routing database that stores information on the fastest route from computer to computer, an update process that enables each *router* to tell other routers which route is the fastest from its point of view, and an update algorithm that enables each router to update its database with the fastest route communicated from neighbouring routers.

RIP places a limit on the maximum distance to the targeted computer as 16 hops or 16 routers, with each router representing a hop from one network to another. Because the route starts with router 0, you are dealing with routes that touch 15 or fewer other routers. For routers farther away, the routing information is dropped or ignored.

You may think that 16 hops is a limitation, but even on a network as large as the Internet, you can usually get to where you want to go within 16 hops. *When you traceroute (tracert on Windows) an address, traceroute traces for only 30 hops, and in most cases, it gets you to your destination in fewer than 15 hops.*

To accomplish this efficiency requires a high level of network planning to ensure that your hop counts are as low as possible.

* OSPF (Open Shortest Path First)

OSPF is the routing algorithm that uses the link state routing algorithm. It is the shortest path algorithm to calculate the best path from the source to the destination. OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. It falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF doesn't need high memory and high-speed processor.

Today, although scale is not much of a reason for implementing multiple areas, OSPF areas are still useful as administrative boundaries in a network. For example:

- Route summarization & aggregation (*replacing several small routes with one larger route that covers them*) can only happen at OSPF area boundaries.
- Not all routers need to know about every other route available in a network. Using OSPF areas, it's possible to inject a default route representing all routes outside of the local area.

If there are several routers on a network, OSPF builds a table (or topography) of the router connections. When data is sent from one location to another, the OSPF algorithm compares the available options and chooses the most efficient way for the data to be sent. This limits unnecessary delays in data transmission and prevents infinite loops.

* BGP (Border Gateway Protocol)

BGP is the Exterior Gateway Protocol which is used for communicating information among **autonomous systems** (AS *is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division).)* on the Internet. BGP is the routing method that enables the Internet to function. Without it, we wouldn't be able to do a Google search or send an email. Neighboring BGP routers i.e. BGP peers exchange detailed path information. It is also called the path vector routing algorithm. The protocols are more concerned with reachability than optimality.

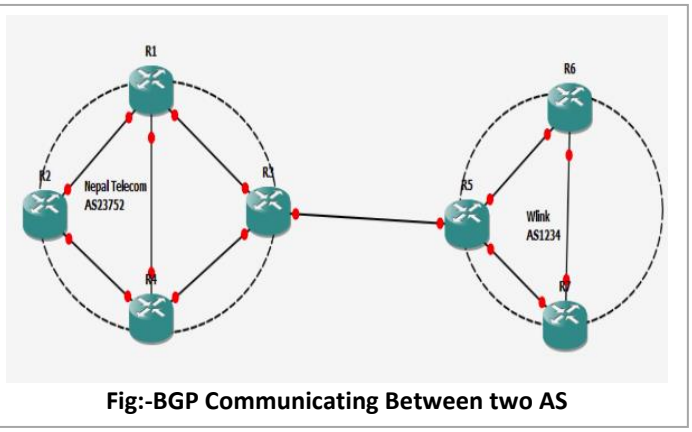


Fig:-BGP Communicating Between two AS

How BGP works?

When a BGP router first comes up on the Internet, it establishes connections with the other BGP routers with which it directly communicates. The first thing it does is download the entire routing table of each neighboring router. After that it only exchanges much shorter update messages with other routers.

BGP routers send and receive update messages to indicate a change in the preferred path to reach a computer with a given IP address. If the router decides to update its own routing tables because this new path is better, then it will subsequently propagate this information to all of the other neighboring BGP routers to which it is connected, and they will in turn decide whether to update their own tables and propagate the information further.
BGP uses the TCP/IP protocol on port 179 to establish connections. It has strong security features, including the incorporation of a digital signature in all communications between BGP routers.

Network address can be of one of the following:

- Unicast (destined to one host)
- Multicast (destined to group)
- Broadcast (destined to all)
- Anycast (destined to nearest one)

***Unicast routing**

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

***Broadcast routing**

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

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

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

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

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

This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.
Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

***Multicast Routing**

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.
Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

*** Anycast Routing**

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.
Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

*** Unicast Routing Protocols**

The analogy stated that distance vector routing protocols are like using road signs to guide you on your way to a destination, only giving you information about distance and direction. However, link-state routing protocols are like using a map. With a map, you can see all of the potential routes and determine your own preferred path.

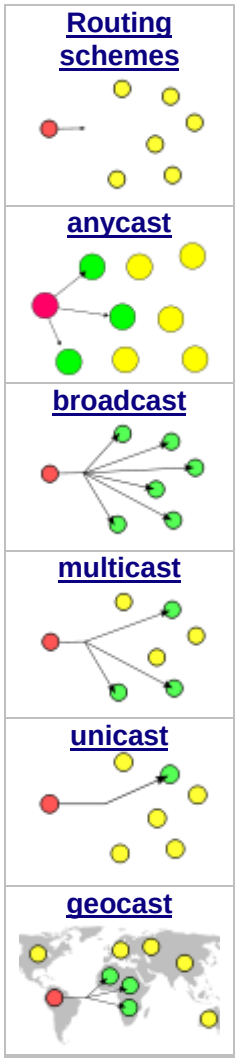
***Multicast Routing Protocols**

Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

- **DVMRP** - Distance Vector Multicast Routing Protocol
- **MOSPF** - Multicast Open Shortest Path First
- **CBT** - Core Based Tree
- **PIM** - Protocol independent Multicast

Protocol Independent Multicast is commonly used now. It has two flavors:

- **PIM Dense Mode**
  This mode uses source-based trees. It is used in dense environment such as LAN.
- **PIM Sparse Mode**
  This mode uses shared trees. It is used in sparse environment such as WAN.



4.6 Routing Algorithms: Shortest path, Flooding, Distance Vector Routing, Link State Routing, Protocols: ARP, RARP, IP, ICMP

*Flooding

Flooding is simplest method packet forwarding. When a packet is received, the routers send it to all the interfaces except the one on which it was received. This creates too much burden on the network and lots of duplicate packets wandering in the network.

Time to Live (TTL) can be used to avoid infinite looping of packets. There exists another approach for flooding, which is ***called Selective Flooding*** to reduce the overhead on the network. In this method, the router does not flood out on all the interfaces, but selective ones.

Flooding is a static routing algorithm, in which every incoming packet is sent out on every outgoing line except the one it arrived on.

Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to dump the process.

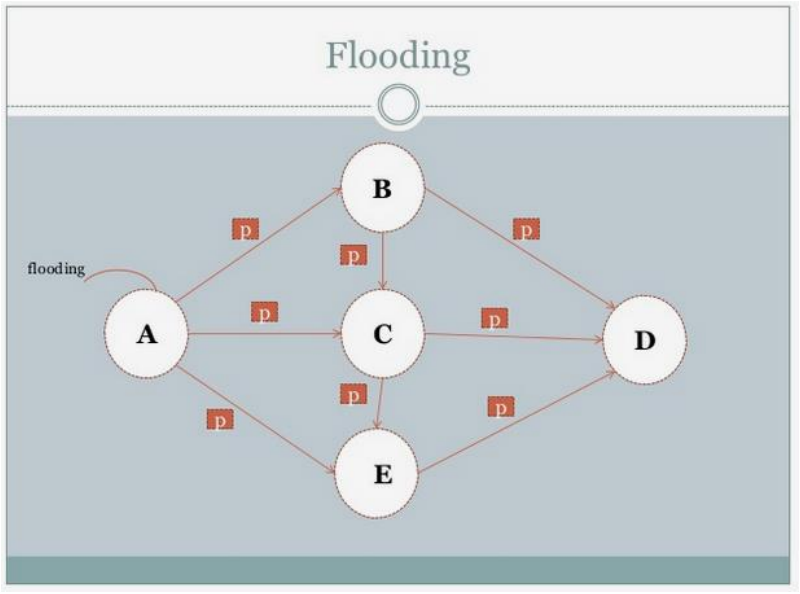


fig:- Flooding

*Shortest Path

Routing decision in networks, are mostly taken on the basis of cost between source and destination. Hop count plays major role here. Shortest path is a technique which uses various algorithms to decide a path with minimum number of hops.

Common shortest path algorithms are:

- Dijkstra's algorithm
- Bellman Ford algorithm

Shortest path algorithm finds the shortest paths between routers/node in a graph. The widely used shortest path algorithm is ***Dijkstra's shortest path algorithm***.

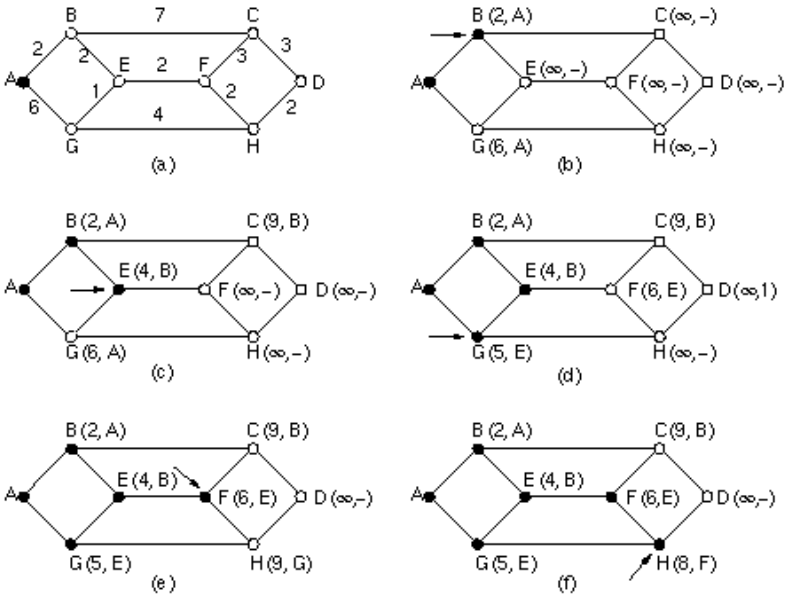


Fig. Shortest path algorithm

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

- **Distance Vector Routing Protocol:** router knows cost to each destination
  Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers,
  For example Routing Information Protocol (RIP).
  Distance vector routing protocols are like road signs because routers must make preferred path decisions based on a distance or metric to a network. Just as travelers trust a road sign to accurately state the distance to the next town, a distance vector router trusts that another router is advertising the true distance to the destination network.
- **Link State Routing Protocol:** router knows entire network topology and computes shortest path
  Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then calculate their best path for routing purposes. For example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).
  Link-state routing protocols take a different approach. Link-state routing protocols are more like a road map because they create a topological map of the network and each router uses this map to determine the shortest path to each network. Just as you refer to a map to find the route to another town, link-state routers use a map to determine the preferred path to reach another destination.

  Link State Routing Process :-
  1. Each router learns about its own links, its own directly connected networks, by detecting that an interface is in the up state.
  2. Each router is responsible for meeting its neighbors on directly connected networks. link state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.
  3. Each router builds a Link-State Packet (LSP) containing the state of each directly connected link. This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.
  4. Each router floods the LSP to all neighbors, who then store all LSPs received in a database. Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.
  5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network. Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to determine the best path to each network.

  There are several **advantages of link-state routing protocols** compared to distance vector routing protocols.
  ***Builds a Topological Map :** Link-state routing protocols create a topological map, or SPF tree of the network topology. Distance vector routing protocols do not have a topological map of the network. Routers implementing a distance vector routing protocol only have a list of networks, which includes the cost (distance) and next-hop routers (direction) to those networks. Because link-state routing protocols exchange link-states, the SPF algorithm can build an SPF tree of the network. Using the SPF tree, each router can independently determine the shortest path to every network.
  ***Fast Convergence :** When receiving a Link-state Packet (LSP), link-state routing protocols immediately flood the LSP out all interfaces except for the interface from which the LSP was received. A router using a distance vector routing protocol needs to process each routing update and update its routing table before flooding them out other interfaces, even with triggered updates. Faster convergence is achieved for link-state routing protocols. A notable exception is EIGRP.
  ***Event-driven Updates :** After the initial flooding of LSPs, link-state routing protocols only send out an LSP when there is a change in the topology. The LSP contains only the information regarding the affected link. Unlike some distance vector routing protocols, link-state routing protocols do not send periodic updates.
  Note: OSPF routers do flood the own link-states every 30 minutes. This is known as a paranoid update and is discussed in the following chapter. Also, not all distance vector routing protocols send periodic updates. RIP and IGRP send periodic updates; however, EIGRP does not.
  ***Hierarchical Design :** Link-state routing protocols such as OSPF and IS-IS use the concept of areas. Multiple areas create a hierarchical design to networks, allowing for better route aggregation (summarization) and the isolation of routing issues within an area. Multi-area OSPF and IS-IS are discussed further in CCNP.

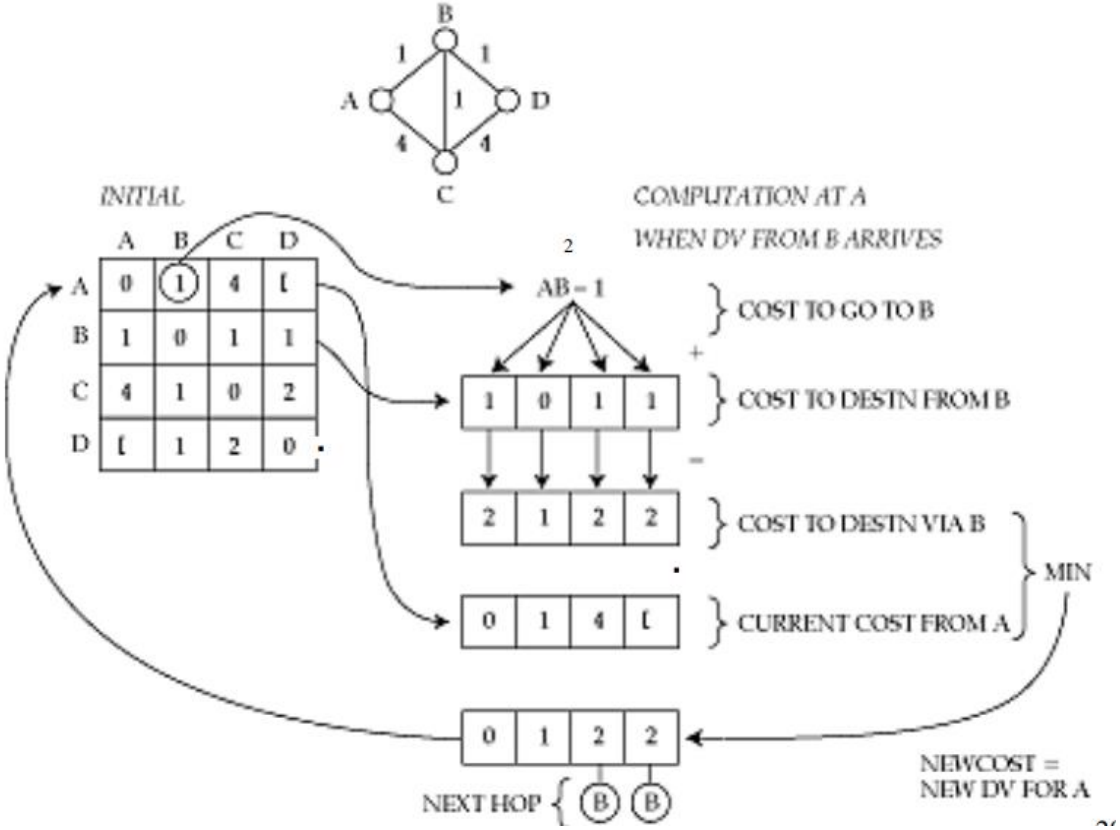
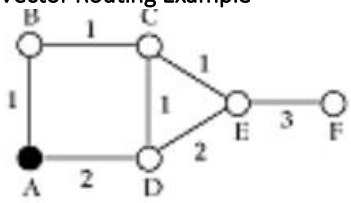


Fig. Distance Vector Routing Example



B(A,1) means B was reached by A, cost 1

PERMANENT	TEMPORARY	COMMENTS
A	B(A,1), D(A,2)	ROOT AND ITS NEIGHBORS
A, B(A,1)	D(A,2), C(B,2)	ADD C(B,2)
A, B(A,1) D(A,2)	E(D,4), C(B,2)	C(D,3) DIDN'T MAKE IT
A, B(A,1) D(A,2), C(B,2)	E(C,3)	E(D,4) TOO LONG
A, B(A,1) D(A,2), C(B,2) E(C,3)	F(E,6)	
A, B(A,1) C(B,2), D(A,2) E(C,3), F(E,6)	NULL	STOP

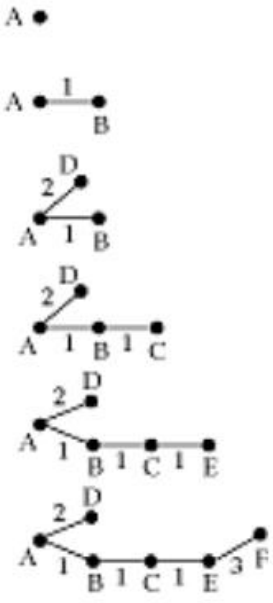


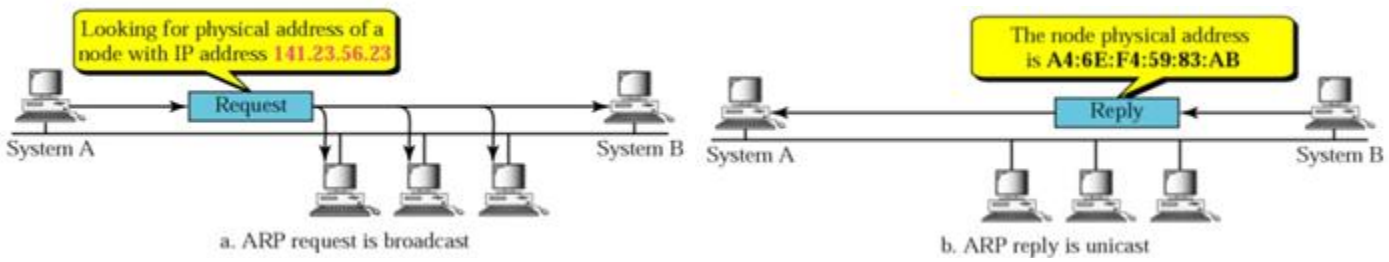
Fig. Link State Routing Example

Distance Vector	Link State
• Entire routing table is sent as an update • Distance vector protocol send periodic update at every 30 or 90 second • Updates are sent to directly connected neighbor only • Routers don't have end to end visibility of entire network. • Suffer from count to infinity problem • Examples: RIP, BGP	• Updates are incremental & entire routing table is not sent as update. • Updates are triggered not periodic. • Update are sent to entire network & to just directly connected neighbor. • Routers have visibility of entire network of that area only. • No routing loops • Convergence is fast because of triggered updates. • Examples: OSPF, IS-IS

fig:- Distance Vector Vs Link State

*ARP,

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.



How ARP Works

ARP works on modern Ethernet and Wi-Fi networks as follows:

- Network adapters are produced with a physical address embedded in the hardware called the Media Access Control (MAC) address. Manufacturers take care to ensure these 6-byte (48-bit) addresses are unique, as IP relies on these unique identifiers for message delivery.
- When any device wishes to send data to another target device, it must first determine the MAC address of that target given its IP address These IP-to-MAC address mappings are derived from an ARP cache maintained on each device.
- If the given IP address does not appear in a device's cache, that device cannot direct messages to that target until it obtains a new mapping. To do this, the initiating device first sends an ARP request broadcast message on the local subnet. The host with the given IP address sends an ARP reply in response to the broadcast, allowing the initiating device to update its cache and proceed to deliver messages directly to the target.

*RARP Inverse ARP and Reverse ARP

A network protocol called RARP (Reverse ARP) was also developed in the 1980s to complement ARP. As its name implies, RARP performed the opposite function of ARP, converting from physical network addresses to the IP addresses assigned to those devices. RARP was made obsolete by DHCP and is no longer used.

A separate protocol called Inverse ARP also supports the reverse address mapping function. Inverse ARP is not used on Ethernet or Wi-Fi networks either although it can sometimes be found on other types.

RARP, RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding

Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

In Ethernet it would be implemented like: given a MAC address, get the corresponding IP Address.

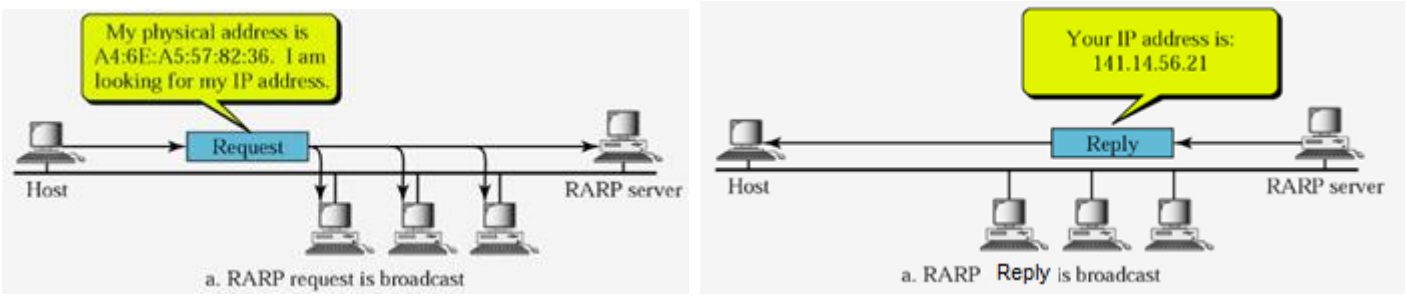


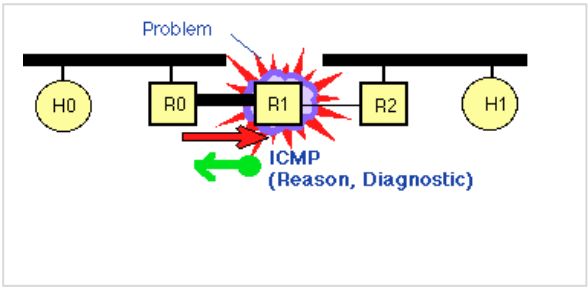
Fig:- RARP Protocol

*IP, The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

*ICMP(Internet Control Message Protocol)



ICMP is an error-reporting protocol network device i.e. send the error message for example, that a requested service is not available or that a host or router could not be reached. like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. It can also be used to relay query messages. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute)., it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including ping and traceroute.

When you send data from one device to another remote device, the IPv4 Datagram often travels through one or more routers. There can be errors at routers while they try to forward the IPv4 Datagram to its final destination. The Internet Control Message Protocol (ICMP) protocol is used to report problems with delivery of IPv4 Datagrams within an IPv4 network. ICMP is also used for other diagnosis and troubleshooting functions.

The most common ICMP messages

- **Echo Request and Echo Reply**: Internet Control Message Protocol (ICMP) is often used during test the connectivity between devices. We can use the ping (Packet InterNet Grouper, a command-line utility used to check the connectivity between two devices) command to check connectivity from one device with another device and the ping command is using Internet Control Message Protocol (ICMP). Ping command sends an IP datagram packet to the IPv4 address of the device we are trying to check the connectivity and requests the destination device to return the data sent in a response datagram. Ping command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply.
- **Source Quench**: If a device is sending large amounts of data to another remote device, the volume can flood the router with data. The router can use Internet Control Message Protocol (ICMP) to send a Source Quench message to the source IPv4 address to ask it to slow down the rate at which it is sending data.
- **Destination Unreachable**: If a router receives a datagram that cannot be delivered, Internet Control Message Protocol (ICMP) returns a Destination Unreachable message to the source IPv4 address.

- **Time Exceeded**: Internet Control Message Protocol (ICMP) sends this message to the source IP if a datagram is discarded because Time-to-Live (TTL) value reaches zero. One reason is the destination device is too many router hops away to reach with the current Time-to-Live (TTL) value or a routing loop (An undesirable condition when the IP Datagrams loop infinitely between the routers, without reaching the destination).

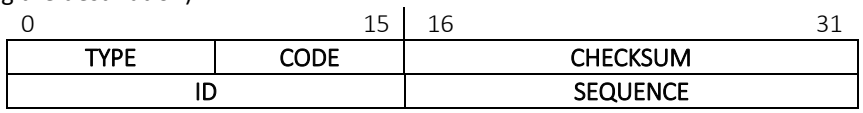


Fig. Internet Control Message Protocol (ICMP) Header

- **Type and Code:** The following table shows the values which are possible for the Type and Code fields in the Internet Control Message Protocol (ICMP) header. Some examples are :-

Type	Code	Description
0	0	Echo reply (used to ping)
4	0	Traffic Congestion Control
8	0	Echo request

- **Checksum**: The checksum field in the Internet Control Message Protocol (ICMP) message contains error checking data calculated from the Internet Control Message Protocol (ICMP) header+data, with value 0 for this field.
- **ID**: The ID field in the Internet Control Message Protocol (ICMP) message contains an ID value, should be returned in case of ECHO REPLY.
- **Sequence number:** The sequence number field in the Internet Control Message Protocol (ICMP) message is the sequence number for each host, generally this starts at 1 and is incremented by 1 for each packet.

Problem :
Q. Suppose there are 4 Departments A(23 Hosts), B(16 Hosts), C(28 Hosts), D(13 Hosts). Given a network 202.70.64.0/24, perform subnetting in such way that IP wastage in each sub-network is minimum. Find subnet mask, Network ID, Broadcast ID and usable host range for each network.

Solution:-

Available network is 202.70.64.0/24
i.e. Total range of available IP address 202.70.64.0-202.70.64.255
We proceed sub-netting with the department with highest no. of host i.e. C and then A, B and D respectively.

For Dept. C (Start with network with maximum hosts)

• No. of hosts = 28
• For No. of bits required for host(Suffix) part (H),
• 2^H -2 ≥ 28 => H = 5 (Select minimum value of H)
• ie. Total no. of IP addresses this n/w can provide = 25 = 32
• No. of bits for Network(Prefix) part = 32 – 5 = 27
• No. of Subnets that can be created = 2^(27-24) = 8, which are given below:
• Available Subnets: 202.70.64.0/27 , 202.70.64.32/27, 202.70.64.64/27, 202.70.64.96/27 , 202.70.64.128/27, 202.70.64.160/27, 202.70.64.192/27 , 202.70.64.224/27
• Let us Select Subnet for C as 202.70.64.0/27, then,
• Subnet Mask = 255.255.255.[11100000] = 255.255.255.224
• Network ID = 202.70.64.0 (The first ip address of network)
• Broadcast ID = 202.70.64.31 (The last ip address of network)
• Usable Host IP range = 202.70.64.1/27 – 202.70.64.30/27

For Dept. A

• No. of hosts = 23
• For No. of bits required for host(Suffix) part (H),
• 2^H -2 ≥ 23 => H = 5 (Select minimum value of H)
• ie. Total no. of IP addresses this n/w can provide = 25 = 32
• No. of bits for Network(Prefix) part = 32 – 5 = 27
• No. of Subnets that can be created = 2^(27-24) = 8, which are given below: 202.70.64.0 / 27 is already used for Department C so cannot be used.
• Available Subnets: 202.70.64.32/27, 202.70.64.64/27, 202.70.64.96/27, 202.70.64.128/27, 202.70.64.160/27, 202.70.64.192/27, 202.70.64.224/27
• Let us Select Subnet for A as 202.70.64.32/27, then,
• Subnet Mask = 255.255.255.[11100000] = 255.255.255.224
• Network ID = 202.70.64.32 (The first ip address of network)
• Broadcast ID = 202.70.64.63 (The last ip address of network)
• Usable Host IP range = 202.70.64.33/27 – 202.70.64.62/27

For Dept. B

• No. of hosts = 16
• For No. of bits required for host(Suffix) part (H),
• 2^H -2 ≥ 16 => H = 5 (Select minimum value of H)
• ie. Total no. of IP addresses this n/w can provide = 25 = 32
• No. of bits for Network(Prefix) part = 32 – 5 = 27
• No. of Subnets that can be created = 2^(27-24) = 8, which are given below: 202.70.64.0 / 27 and 202.70.64.32/27 are already used for Departments C and A, so cannot be used.
• Available Subnets: 202.70.64.64 / 27, 202.70.64.96/27, 202.70.64.128/27, 202.70.64.160 / 27, 202.70.64.192/27 , 202.70.64.224/27
• Let us Select Subnet for B as 202.70.64.64 / 27, then,
• Subnet Mask = 255.255.255.[11100000] = 255.255.255.224
• Network ID = 202.70.64.64 (The first ip address of network)
• Broadcast ID = 202.70.64.95 (The last ip address of network)
• Usable Host IP range = 202.70.64.65/27 – 202.70.64.94/27

For Dept. D

•No. of hosts = 13
•For No. of bits required for host(Suffix) part (H),
•2^H-2 ≥ 13 => H = 4 (Select minimum value of H)
•ie. Total no. of IP addresses this n/w can provide = 2^4= 16
•No. of bits for Network(Prefix) part = 32 –4 = 28
•No. of Subnets that can be created = 2^(28-24)= 16
•(IP addresses upto 202.70.64.95 are already occupied)
•Let us Select Subnet for D as 202.70.64.96 / 28, then,
•Subnet Mask = 255.255.255.[11110000] = 255.255.255.240
•Network ID = 202.70.64.96
(The first ip address of network)
•Broadcast ID = 202.70.64.111 (The last ipaddress of network)
•Usable Host IP range = 202.70.64.97/28 –202.70.64.110/28