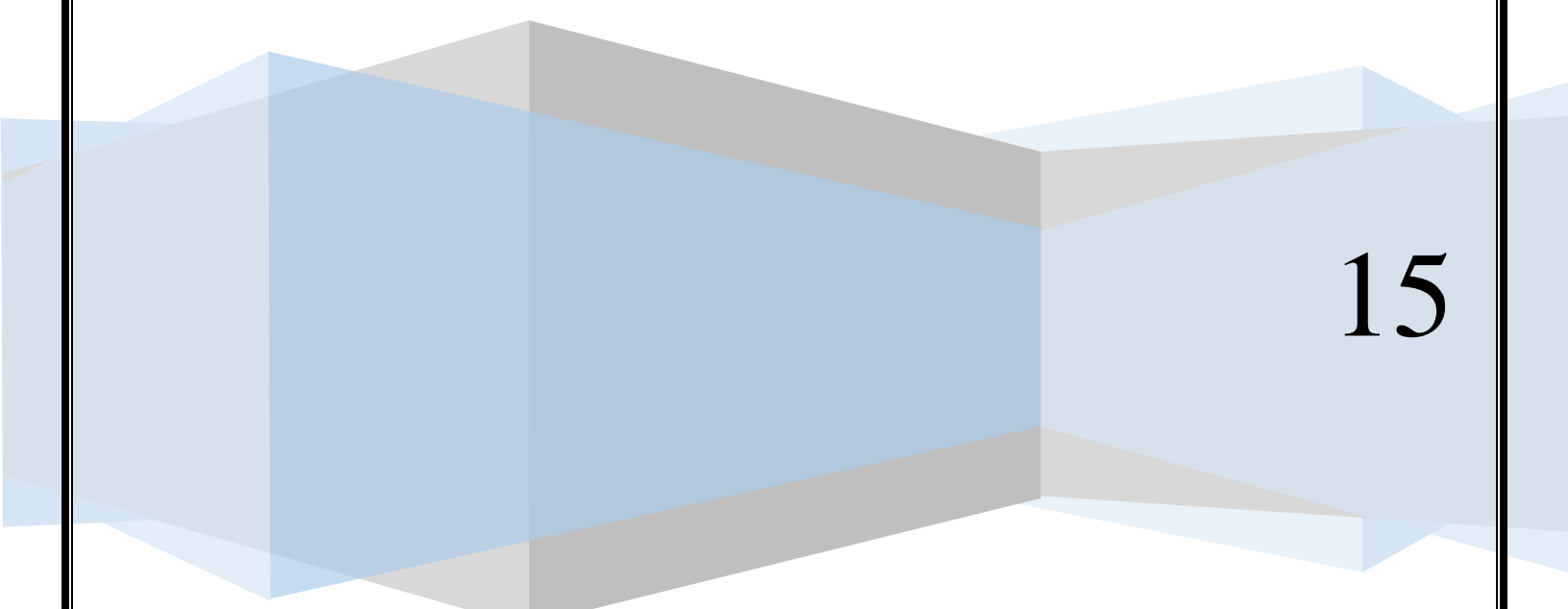


MEPL

IBPS SO PREPRATION

Network Layer

SHOBHIT BANDHU



15

Network Layer

Introduction

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining 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 subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to how to route packets from source to destination, mapping different addressing schemes and protocols.

Layer-3 Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include variety of 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:

- QoS management.
- Load balancing and link management.
- Provides Security.
- Interrelates different protocols and subnets with different schema.
- L3 can produce different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Internet protocol is widely respected and deployed Network Layer protocol which helps to communicate end to end devices over the internet. It comes in two flavors. IPv4 which has ruled the world for decades but now is running out of address space. IPv6 which has been created to replace IPv4 and hopefully mitigates IPv4's limitations too.

Network Addressing

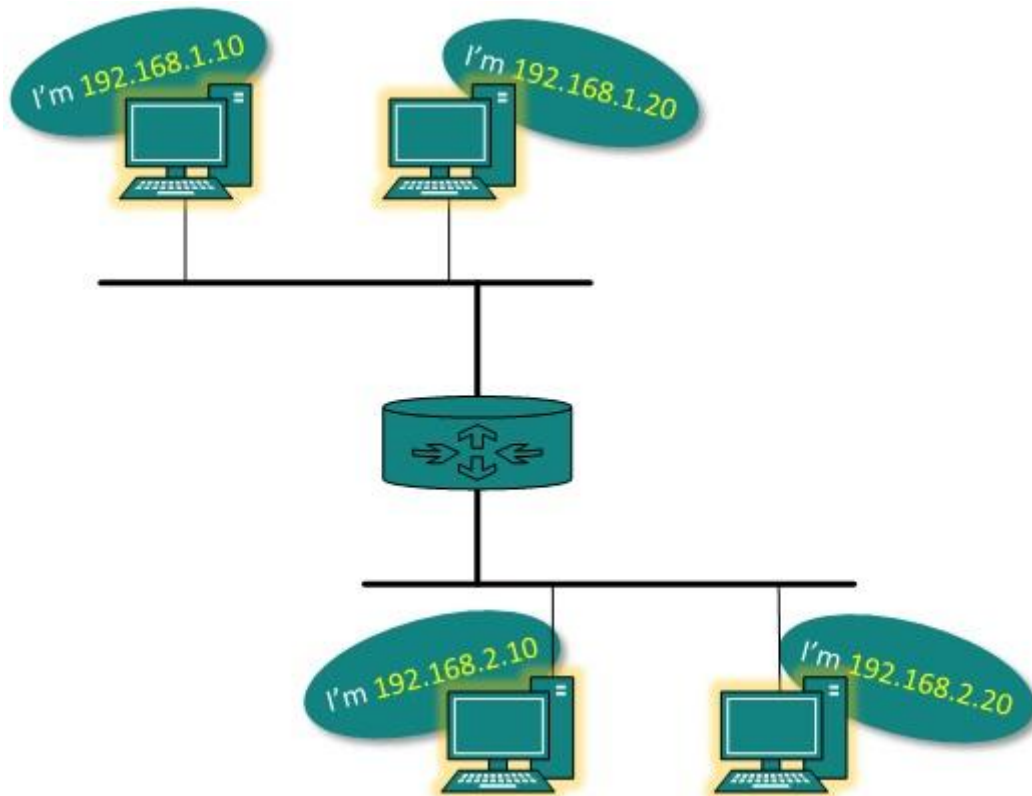
Layer 3 network addressing is one of the major tasks of Network Layer. Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

A network address always points to host / node / server or it can be represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of network address were in existence:

- IP
- IPX
- AppleTalk

We are discussing IP here as it is the only one we use in practice these days.



[Image: Network Addressing]

IP addressing provides mechanism to differentiate between host and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network only. Hosts which needs to communicate outside their subnet, needs to know destination network address, where the packet/data is to be sent.

Hosts in different subnet needs a mechanism 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:

- Where is the Destination Network address?
- How to reach that?

Routers upon receiving 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.

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)

A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just like unicast, but the packets are delivered to the nearest destination when more than one are available.

Network Layer Routing

Introduction

When a device has multiple paths to reach a destination it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes, but software based routers have limited functionality and limited scope.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple

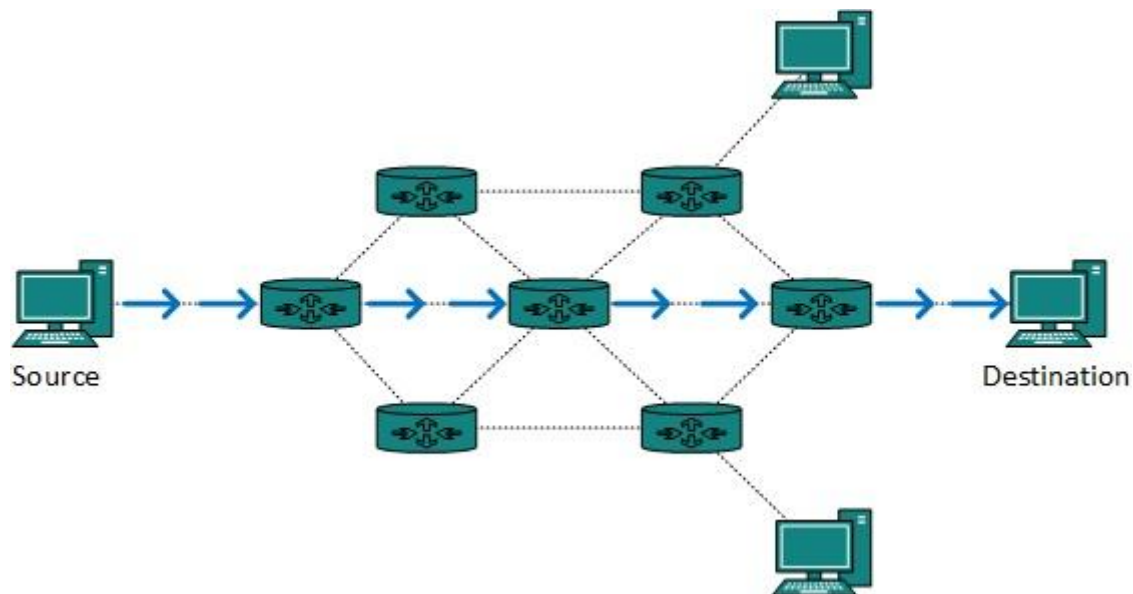
paths exist to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

Unicast routing

Most of the traffic on the Internet and Intranets are sent with destination specified, known as unicast data or unicast traffic. Routing unicast data over the internet is called Unicast Routing. It is the simplest form of routing because the destination is already known. So router just have to look up the routing table and forward the packet to next hop.



[Image: Unicast routing]

Broadcast routing

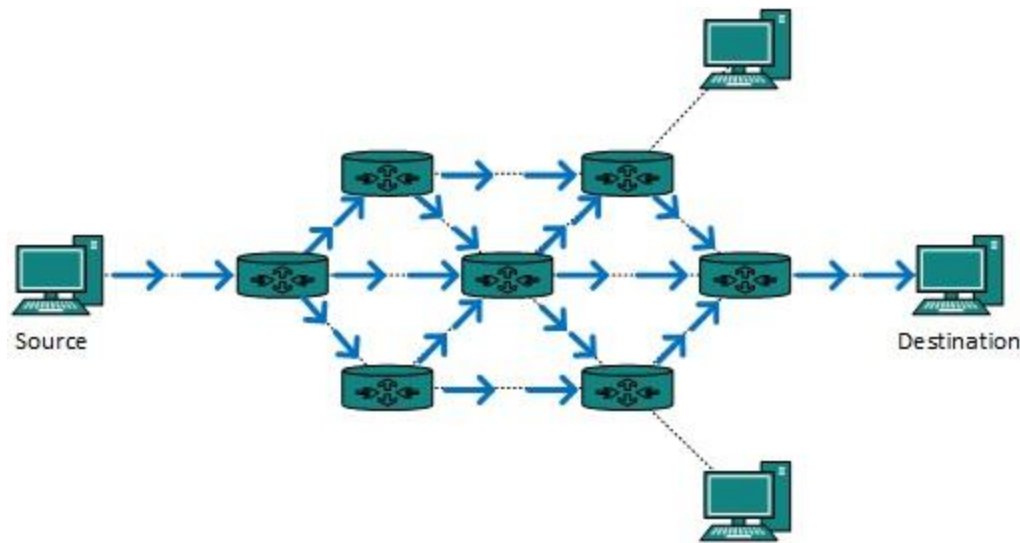
By default a Broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

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 scenario 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 that way.



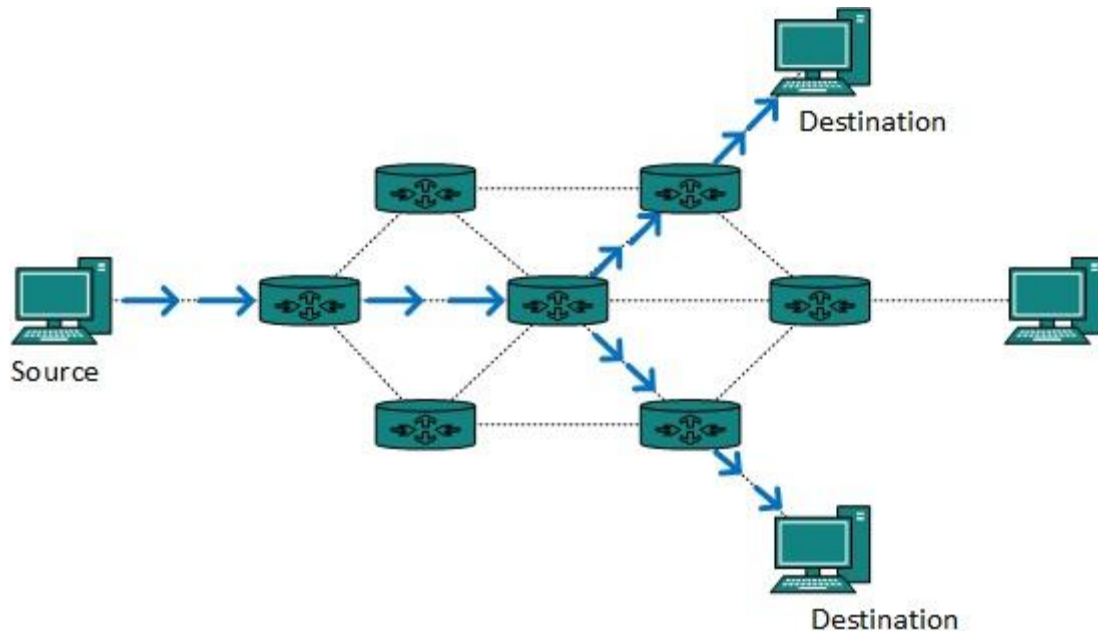
[Image: Broadcast routing]

This method is easy on routers 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 but has 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.



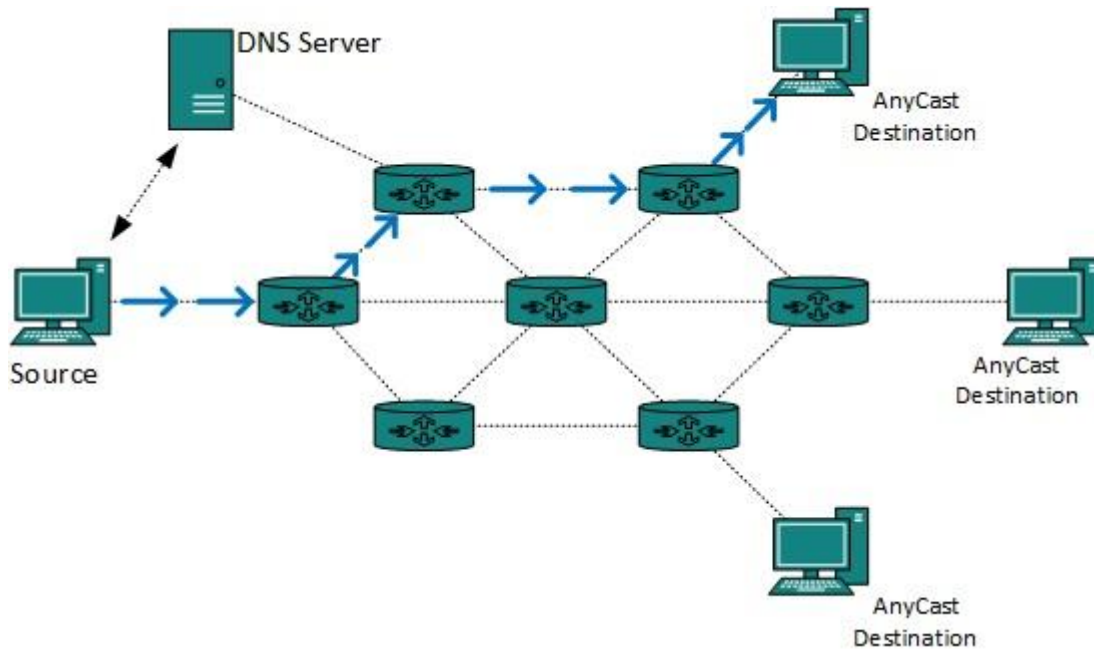
[Image: Multicast routing]

Router must know that there are nodes who 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 host 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.



[Image: Anycast routing]

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

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

- **Distance Vector Routing Protocol**

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 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.

Example: Routing Information Protocol *RIP*.

- **Link State Routing Protocol**

Link State protocol is slightly complicated protocol than Distance Vector. It takes in 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.

Example: Open Shortest Path First *OSPF* and Intermediate System to Intermediate System *ISIS*.

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.

Routing Algorithms

Flooding

Flooding is simplest method packet forwarding. When a packet is received 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 packet wandering in the network.

TTL *Time to Live* 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 router does not flood out on all interfaces, but selective ones.

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 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
- Floyd Warshall algorithm

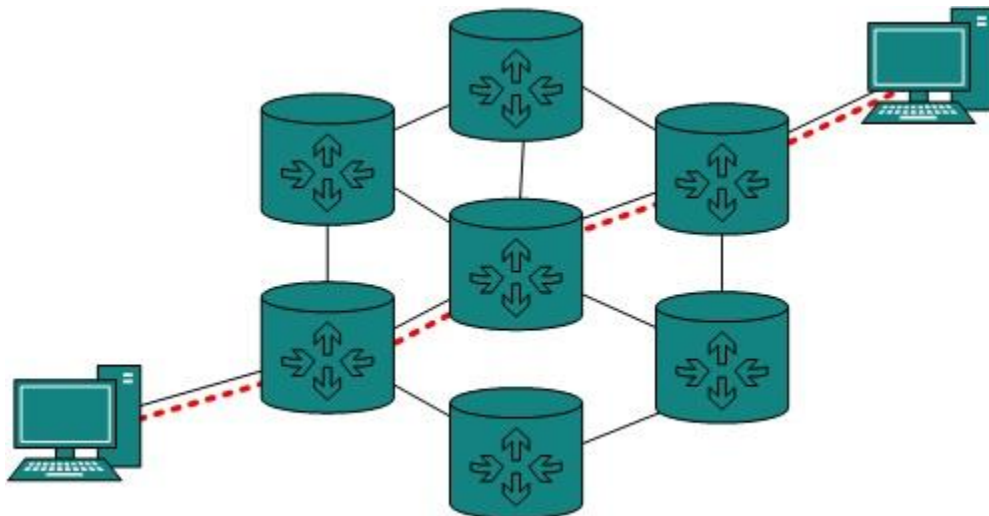
Internetworking

Internetwork Routing

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.



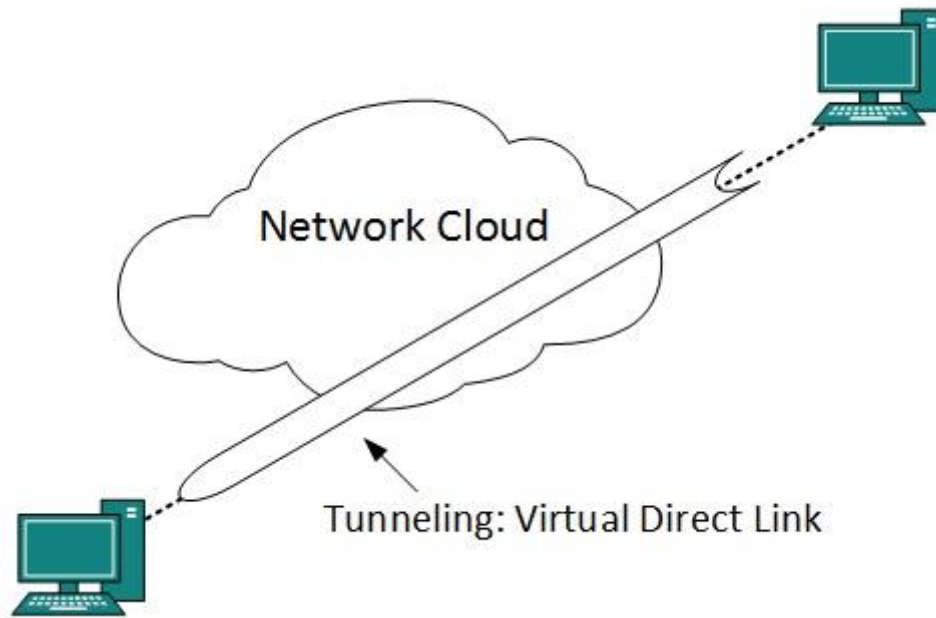
[Image: Routing]

Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are example of IGP. Routing between different organization or administration may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Tunneling

If they are two geographically separate networks, which wants to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



[Image: Tunneling]

Data when enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

Both ends feel as if they are directly connected and tagging makes data travel through transit network without any modifications.

Packet fragmentation

Most Ethernet segments have their maximum transmission unit MTU fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

If a packet with DF don't fragment bit set to 1 comes to a router which cannot handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF more fragments bit set to 1, router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not able to process it and it might drop.

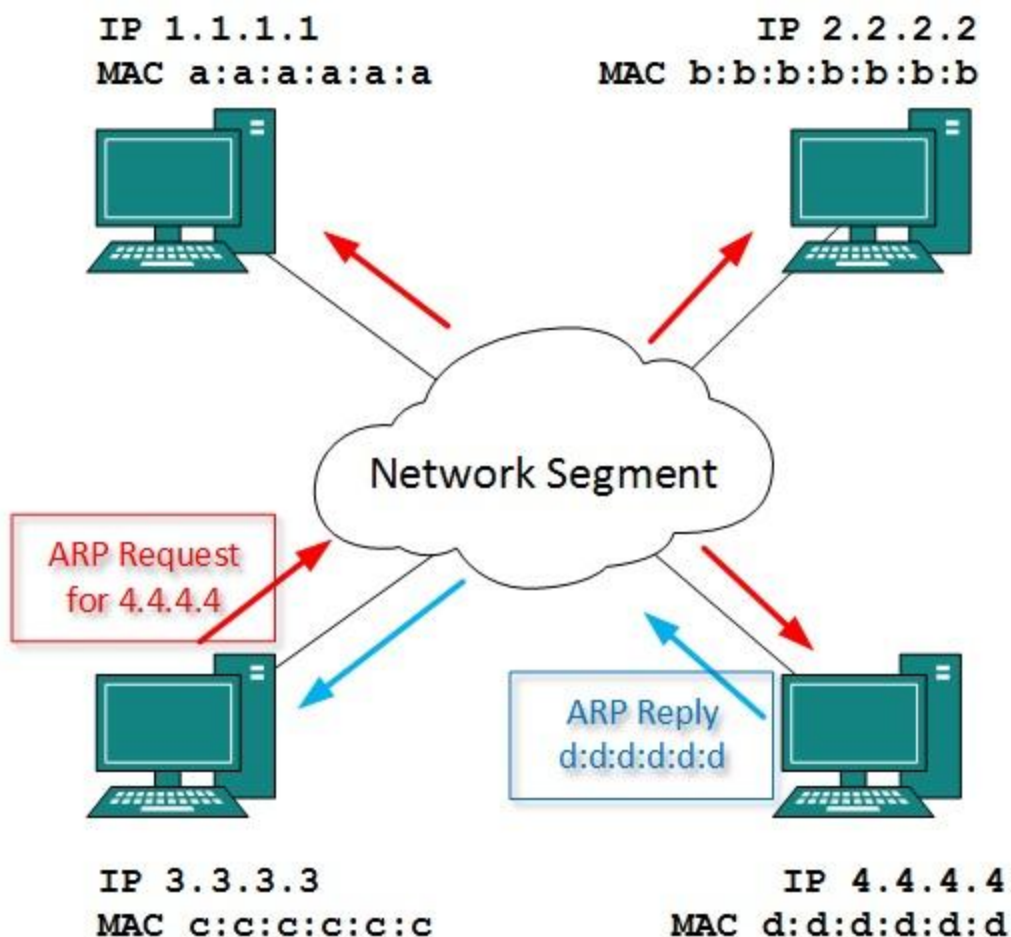
Network Layer Protocols

Address Resolution Protocol

In a network, every computer has an IP address by which a computer can be uniquely identified and addressed in whole broadcast domain. An IP address is Layer-3 *Network Layer* logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

While communicating, a host needs Layer-2 *MAC* address of the destination machine which belong to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card of a machine and it never changes.

On the other hand, IPs on the public domain are rarely changed but if their NIC is changed *in case of mechanical fault etc.* their MAC address also changes. This way, for Layer-2 communication to take place, a mapping between to is required.



[Image: ARP Mechanism]

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking “who has this IP address?”. Because it is a broadcast, all hosts on the network segment *broadcast domain* receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, now it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require communicating, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet it is encapsulated in IP packet. Because IP is itself a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network the ICMP will report that problem.

Internet Protocol version 4

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A:** uses first octet for network addresses and last three octets for host addressing
- **Class B:** uses first two octets for network addresses and last two for host addressing
- **Class C:** uses first three octets for network addresses and last one for host addressing
- **Class D:** provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E:** experimental

IPv4 also has well-defined address spaces to be used as private addresses *not routable on internet* and public addresses *provided by ISPs and routable on internet*.

Though IP is not reliable one but it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol version 6

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but have removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of DHCP servers. This way even the DHCP server on that subnet is down, hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There is some transition mechanism available for IPv6 enabled networks to easily speak and roam around different networks on IPv4. These are:

- Dual Stack implementation
- Tunneling
- NAT-PT