UNIT-3

**MODULE III:** Network Layer: Basics of Network Layer - Logical Addressing, Internetworking, Tunneling, Address mapping,

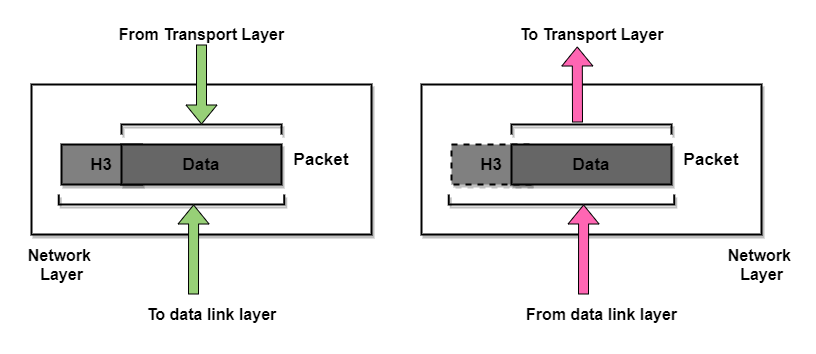
B: Communication Protocols - ICMP, IGMP, Forwarding, Unicast Routing Protocols, and Multicast Routing Protocols.

Network Layer

* The Network Layer is the third layer of the OSI model.
* It handles the service requests from the transport layer and further forwards the service request to the data link layer.
* The network layer translates the logical addresses into physical addresses
* It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
* The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

* **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
* **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
* **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
* **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.



## Services provided by the Network Layer

**1. Guaranteed delivery of Packets** The network layer guarantees that the packet will reach its destination.

**2. Guaranteed delivery with the bounded delay** It is another service provided by the network layer and it guarantees that the packet will surely be delivered within a specified host-to-host delay bound.

**3. Transfer of packets in Order** According to this service, it is ensured that packets arrive at the destination in the same order in which they are sent by the sender.

**4. Security** Security is provided by the network layer by using a session key between the source host and the destination host.

### Advantages of Network Layer Services

Given below are some benefits of services provided by the network layer:

* By forwarding service of the network layer, the data packets are transferred from one place to another in the network.
* In order to reduce the traffic, the routers in the network layer create collisions and broadcast the domains.
* Failure in the data communication system gets eliminated by packetization.

### Disadvantages of Network layer Services

* In the design of the network layer, there is a lack of flow control
* In the network layer, there is a lack of proper error control mechanisms; due to the presence of fragmented data packets the implementation of error control mechanism becomes difficult.

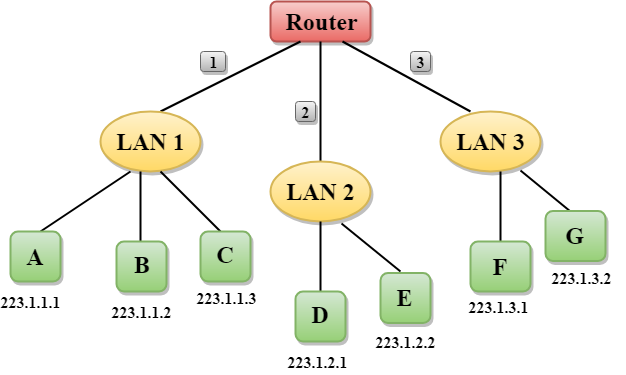
### Design Issues with Network Layer

* A key design issue is **determining how packets are routed from source to destination**. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic, being determined anew for each packet, to reflect the current network load.
* If **too many packets** are present in the subnet at the same time, they will get into one another's way, forming **bottlenecks**. The **control of such congestion** also belongs to the network layer.
* Moreover, the **quality of service** provided(delay, transmit time, jitter, etc) is also a network layer issue.
* When a packet has to **travel from one network to another to get to its destination**, many problems can arise such as:
  + The addressing used by the second network may be different from the first one.
  + The second one may not accept the packet at all because it is too large.
  + The protocols may differ, and so on.
* It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

**Logical Addressing**

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

* Network Addressing is one of the major responsibilities of the network layer.
* Network addresses are always logical, i.e., software-based addresses.
* A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
* A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
* Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

 **Let's understand through a simple example.**

* In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
* Each host contains its own interface and IP address.
* All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
* Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

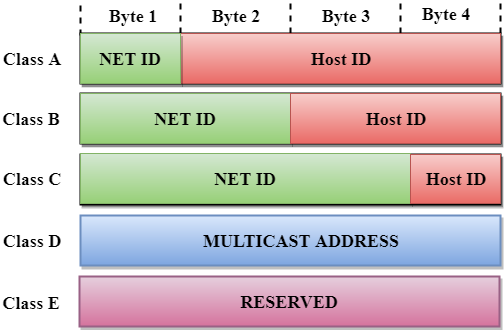
## Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

* Class A
* Class B
* Class C
* Class D
* Class E

**An ip address is divided into two parts:**

* **Network ID:** It represents the number of networks.
* **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

## Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

* The network ID is 8 bits long.
* The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 27 = 128 network address

The total number of hosts in Class A = 224 - 2 = 16,777,214 host address



## Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

* The Network ID is 16 bits long.
* The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 214 = 16384 network address

The total number of hosts in Class B = 216 - 2 = 65534 host address



## Class C

In Class C, an IP address is assigned to only small-sized networks.

* The Network ID is 24 bits long.
* The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 221 = 2097152 network address

The total number of hosts = 28 - 2 = 254 host address



## Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



## Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



## Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

* The Host ID must be unique within any network.
* The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
* The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

* The network ID cannot start with 127 as 127 is used by Class A.
* The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
* The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## Classful Network Architecture

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Class** | **Higher bits** | **NET ID bits** | **HOST ID bits** | **No.of networks** | **No.of hosts per network** | **Range** |
| A | 0 | 8 | 24 | 27 | 224 | 0.0.0.0 to 127.255.255.255 |
| B | 10 | 16 | 16 | 214 | 216 | 128.0.0.0 to 191.255.255.255 |
| C | 110 | 24 | 8 | 221 | 28 | 192.0.0.0 to 223.255.255.255 |
| D | 1110 | Not Defined | Not Defined | Not Defined | Not Defined | 224.0.0.0 to 239.255.255.255 |
| E | 1111 | Not Defined | Not Defined | Not Defined | Not Defined | 240.0.0.0 to 255.255.255.255 |

**Internetworking**

The word “internetworking,” which combines the words “inter” and “networking,” denotes a connection between completely distinct nodes/segments. This connection is made possible by intermediary hardware like routers or gateways. Catenet was the initial title for associate degree internetwork. Private, public, commercial, industrial, and governmental networks frequently connect to one another. Therefore, a degree of internetwork could be a collection of several networks that operate as a single large network and are connected by intermediate networking devices. The trade, goods, and methods used to address the difficulty of creating and managing internet works are referred to as internetworking.

## Types of Internetworking

Internetworking primarily consists of three units: Extranet, Internet, and Intranet. Internet connections may or may not be present on intranets and extranets. The computer network or the extranet area unit is typically protected from being accessed from the internet if it is not approved and if there is a link to the internet. Although it should serve as a portal for access to portions of the associate degree extranet, the internet is not considered to be a part of the computer network or extranet.

### Extranet

It’s a network of the internetwork with a confined scope to one organisation or institution but with limited links to one or more other networks on occasion; however, this is not always the case. It is the lowest degree of internet usage and is typically prohibited in extremely private areas. An extranet may also be referred to as a MAN, WAN, or another type of network, but it cannot include a single local area network; rather, it must make at least one mention of an external network.

### Internet

Internet is a specific internetworking that connects governmental, academic, public, and private networks on a global scale. It is based on the ARPANET, which was created by the ARPA (Advanced Research Projects Agency) of the U.S. Defense Department. It is also the location of the World Wide Web (WWW) and is referred to as the “Internet” to distinguish it from other generic internetworking. Internet users and their service providers utilise IP addresses obtained from address registries that control assignments.

### Intranet

This computer network can be a collection of interconnected networks that employ the Internet Protocol and IP-based software like web browsers as well as FTP tools, all of which are controlled by a single body entity. This body entity blocks access to the computer network for the rest of the world and only allows a select few users. This network most frequently refers to the internal network of a business or other enterprise. To provide users with browse able data, a large computer network can typically have its own internet server.

### Network Layer Addresses

The network addresses can occasionally be seen in both gradable address areas and the more common virtual or logical address area units. The relationship between the network address and the tool is logical and flexible; it typically depends either on the properties of the physical network or on groupings without any physical foundation. For each network-layer protocol that a finished system supports, a network-layer address is required. For each supported network-layer protocol, routers and other internetworking devices require a single network-layer address for every physical network association.

**Tunneling**

Tunneling is a way to move packets from one network to another. Tunneling works via encapsulation: wrapping a packet inside another packet.

In computer networks, a **tunneling protocol** is a communication protocol which allows for the movement of data from one network to another, by exploiting encapsulation. It involves allowing private network communications to be sent across a public network (such as the Internet) through a process called encapsulation.

Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, it can hide the nature of the traffic that is run through a tunnel.

Tunneling is an internetworking strategy that is used when source and destination networks of same type are connected through a network of different type.

• In such a case, the packet from one network reaches the other network via different kind pf network that interconnects them.

• To understand tunneling, let an Ethernet is to be connected to another Ethernet via a WAN.

• The IP packets are to be sent from host 1 of Ethernet 1 to host 2 of Ethernet 2 via a WAN.

• To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2.

• It then inserts this packet into an Ethernet frame. This frame is addressed to the multi-[protocol](https://ecomputernotes.com/computernetworkingnotes/computer-network/protocol) router M1 and is placed on Ethernet.

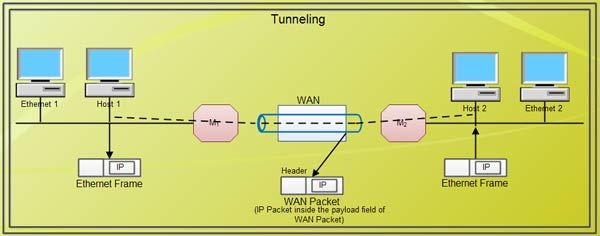
• When this packet reaches, multiprotocol router MI, it removes the IP packet and insert it in the payload field of the WAN network layer packet.

• This WAN network layer packet is then addressed to multi-[protocol](https://ecomputernotes.com/computernetworkingnotes/computer-network/protocol) router M2.

• When this packet reaches M2, it removes the IP packet and inserts it into the Ethernet frame and sends it to host 2.

• In the above process, IP packets do not have to deal with WAN, they just travel from one end 0f the tunnel to the other end. The host 1 and host 2 on two Ethernet also do not have to deal with WAN.

• The multi-protocol routers M1 & M2 understand about IP and WAN packets.



## Tunneling protocols?

In addition to GRE, IPsec, IP-in-IP, and SSH, other tunneling protocols include:

* Point-to-Point Tunneling Protocol (PPTP)
* Secure Socket Tunneling Protocol (SSTP)
* Layer 2 Tunneling Protocol (L2TP)
* Virtual Extensible [Local Area Network](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) (VXLAN)
* **Point-to-Point Tunneling Protocol (PPTP):** PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the “virtual” sense because it is actually being created in a tunneled environment.
* **Layer Two Tunneling Protocol (L2TP):** This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.
* **Layer 2 Tunneling Protocol (L2TP) connections**, which are also called virtual lines, provide cost-effective access for remote users by allowing corporate network systems to manage the IP addresses assigned to its remote users. Further, L2TP connections provide secure access to your system or network when you use them in conjunction with IP Security (IPSec).L2TP **supports two tunnel modes:** the voluntary tunnel and the compulsory tunnel. The major difference between these two tunnel modes is the endpoint. On the voluntary tunnel, the tunnel ends at the remote client whereas the compulsory tunnel ends at the Internet Service Provider (ISP).
* With an L2TP compulsory tunnel, a remote host initiates a connection to its ISP. The ISP then establishes an L2TP connection between the remote user and the corporate network. Although the ISP establishes the connection, you decide how to protect the traffic by using VPN. With a compulsory tunnel, the ISP must support LT2P.
* With an L2TP voluntary tunnel, the connection is created by the remote user, typically by using an L2TP tunneling client. As a result, the remote user sends L2TP packets to its ISP which forwards them on to the corporate network. With a voluntary tunnel, the ISP does not need to support L2TP. The scenario, Protect an L2TP voluntary tunnel with IPSec provides you with an example of how to configure a branch office system to connect to its corporate network through a gateway system with an L2TP tunnel protected by VPN.

## Virtual Extensible LAN (VXLAN) Overview

VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility. VXLAN offers the following benefits:

* **VLAN flexibility in multitenant segments:** It provides a solution to extend Layer 2 segments over the underlying network infrastructure so that tenant workload can be placed across physical pods in the data center.
* **Higher scalability:** VXLAN uses a 24-bit segment ID known as the VXLAN network identifier (VNID), which enables up to 16 million VXLAN segments to coexist in the same administrative domain.
* **Improved network utilization:** VXLAN solved Layer 2 STP limitations. VXLAN packets are transferred through the underlying network based on its Layer 3 header and can take complete advantage of Layer 3 routing, equal-cost multipath (ECMP) routing, and link aggregation protocols to use all available paths.

## Applications of Tunneling

Several protocols use a public network, such as the Internet, to transfer private network data by establishing a VPN (Virtual Private Network), making data transmissions more secure, especially when using unencrypted data.

IPsec (GPRS tunnelling protocol), SSH (Secure Socket Tunnelling Protocol), PPTP (Point-to-Point Tunnelling Protocol), and others are standard protocols, each designed for a specific tunnelling task or purpose.

Some examples of how tunnelling protocols are used are as follows −

* Although a foreign protocol is not supported to run over a specific network, a tunnelling protocol can run IP-v6 over IP-v4.
* When the corporate network does not include the user's physical network address, it is also used to deliver unfeasible fundamental network services, such as a corporate network address) to a remote user.
* Tunnelling allows users to get around a firewall by using an unblocked protocol such as HTTP and the technique of "wrapping" to piggyback/ slip past the firewall rules.
* Another option is to use the HTTP CONNECT tunnel's command/ technique. The HTTP proxy establishes a TCP connection to a specific server when the client issues an HTTP CONNECT command to the proxy server. This security flaw is exploited to use the HTTP proxy to transmit data between the client connection and the designated port. Usually, HTTP proxies enable connections like 443 but deny other proxy servers' access to the CONNECT command.

**Address mapping**

**Address mapping** is a process of determining a logical address knowing the physical address of the device and determining the physical address by knowing the logical address of the device. Address mapping is required when a packet is routed from source host to destination host in the same or different network.

## Types of Address Mapping

* 1. **Static Mapping**
  2. **Dynamic Mapping**

**Static Mapping**

* Static mapping involves in the creation of a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table. This has some limitations because physical addresses may change in the following ways:

A machine could change its NIC, resulting in a new physical address.

* 1. In some LANs, such as Local Talk, the physical address changes every time the computer is turned on.
  2. A mobile computer can move from one physical network to another, resulting in a change in its physical address.
* To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance. In dynamic mapping each time a machine knows one of the two addresses (logical or physical), it can use a protocol to find the other one.

**Dynamic Mapping**

In dynamic mapping usually, the source host knows the logical address of the destination host but to deliver the packet to the destined host its physical address is required as at the physical level the device is identified by its physical address.

So, the source host uses the protocols to identify the physical address of the destination host. Two protocols are designed for dynamic mapping **ARP (Address Resolution Protocol)** and **RARP (Reverse Address Resolution Protocol).**

ARP protocol determines the physical address of a device knowing its logical address. RARP protocol determines the logical address of a device knowing its physical address. We will discuss how this mapping is done.

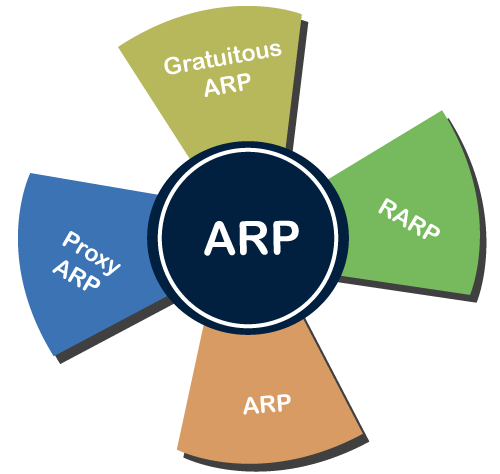
# Address Resolution Protocol (ARP) and its types

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

## Types of ARP

**There are four types of Address Resolution Protocol, which is given below:**

* Proxy ARP
* Gratuitous ARP
* Reverse ARP (RARP)
* Inverse ARP



**Proxy ARP -** Proxy ARP is a method through which a Layer 3 devices may respond to ARP requests for a target that is in a different network from the sender. The Proxy [ARP](https://www.javatpoint.com/address-resolution-protocol) configured router responds to the ARP and map the MAC address of the router with the target [IP](https://www.javatpoint.com/ip-full-form) address and fool the sender that it is reached at its destination.

At the backend, the proxy router sends its packets to the appropriate destination because the packets contain the necessary information.

**Example -** If Host A wants to transmit data to Host B, which is on the different network, then Host A sends an ARP request message to receive a MAC address for Host B. The router responds to Host A with its own MAC address pretend itself as a destination. When the data is transmitted to the destination by Host A, it will send to the gateway so that it sends to Host B. This is known as proxy ARP.

**Gratuitous ARP -** Gratuitous ARP is an ARP request of the host that helps to identify the duplicate IP address. It is a broadcast request for the IP address of the router. If an ARP request is sent by a switch or router to get its IP address and no ARP responses are received, so all other nodes cannot use the IP address allocated to that switch or router. Yet if a router or switch sends an ARP request for its IP address and receives an ARP response, another node uses the IP address allocated to the switch or router.

**There are some primary use cases of gratuitous ARP that are given below:**

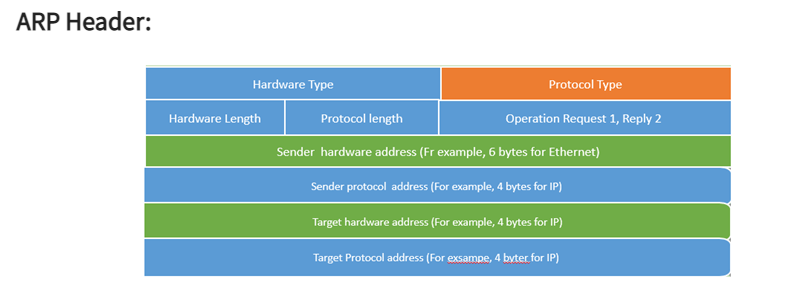
* The gratuitous ARP is used to update the ARP table of other devices.
* It also checks whether the host is using the original IP address or a duplicate one.

**Reverse ARP (RARP) -** It is a networking protocol used by the client system in a local area network (LAN) to request its IPv4 address from the ARP gateway router table. A table is created by the network administrator in the gateway-router that is used to find out the MAC address to the corresponding IP address.

When a new system is set up or any machine that has no memory to store the IP address, then the user has to find the IP address of the device. The device sends a RARP broadcast packet, including its own MAC address in the address field of both the sender and the receiver hardware. A host installed inside of the local network called the RARP-server is prepared to respond to such type of broadcast packet. The RARP server is then trying to locate a mapping table entry in the IP to MAC address. If any entry matches the item in the table, then the RARP server sends the response packet along with the IP address to the requesting computer.

**Inverse ARP (InARP) -** Inverse ARP is inverse of the ARP, and it is used to find the IP addresses of the nodes from the data link layer addresses. These are mainly used for the frame relays, and ATM networks, where Layer 2 virtual circuit addressing are often acquired from Layer 2 signaling. When using these virtual circuits, the relevant Layer 3 addresses are available.

ARP conversions Layer 3 addresses to Layer 2 addresses. However, its opposite address can be defined by InARP. The InARP has a similar packet format as ARP, but operational codes are different.



* Hardware Type–It is 1 for Ethernet.
* Protocol Type–It is a protocol used in the network layer.
* Hardware Address Length–It is the length in bytes so that it would be 6 for Ethernet.
* Protocol Address Length – Its value is 4 bytes.
* Operation Code indicates that the packet is an ARP Request (1) or an ARP Response (2).
* Senders Hardware Address – It is a hardware address of the source node.
* Senders Protocol Address -It is a layer 3 address of the source node.
* Target Hardware Address – It is used in a RARP request, which response impact both the destination’s hardware and layer 3 addresses.
* Target Protocol Address – It is used in an ARP request when the response carries both layer 3 addresses and the destination’s hardware.

Communication protocol

A **communication protocol** is a system of rules that allows two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.

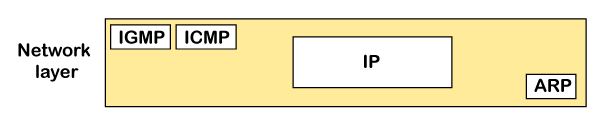
Communicating systems use well-defined formats for exchanging various messages. Each message has an exact meaning intended to elicit a response from a range of possible responses pre-determined for that particular situation. The specified behavior is typically independent of how it is to be implemented. Communication protocols have to be agreed upon by the parties involved. To reach an agreement, a protocol may be developed into a technical standard. A programming language describes the same for computations, so there is a close analogy between protocols and programming languages: *protocols are to communication what programming languages are to computations*. An alternate formulation states that *protocols are to communication what algorithms are to computation*

## Internet Control Message Protocol (ICMP)

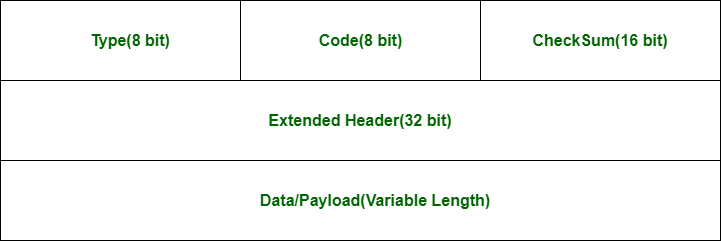
The Internet Control Message Protocol (ICMP) is a [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in [distributed denial-of-service (DDoS) attacks](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/).

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a [packet](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

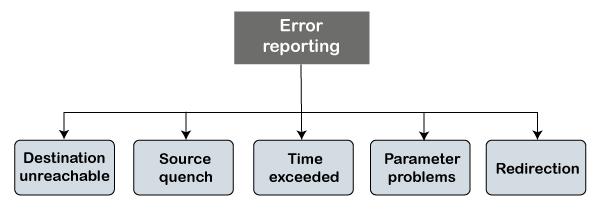
A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the [routing](https://www.cloudflare.com/learning/network-layer/what-is-routing/) path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a ‘hop,’ and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.



**ICMP Packet Format:**



* **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
* **Code:** It is an 8-bit field that defines the subtype of the ICMP message
* **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.
* Types of Error Reporting messages
* **The error reporting messages are broadly classified into the following categories:**



* **Destination unreachable**

The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.

* **Source quench**

There is no flow control or congestion control mechanism in the network layer or the IP protocol. The sender is concerned with only sending the packets, and the sender does not think whether the receiver is ready to receive those packets or is there any congestion occurs in the network layer so that the sender can send a lesser number of packets, so there is no flow control or congestion control mechanism. In this case, ICMP provides feedback, i.e., source quench. Suppose the sender resends the packet at a higher rate, and the router is not able to handle the high data rate. To overcome such a situation, the router sends a source quench message to tell the sender to send the packet at a lower rate.

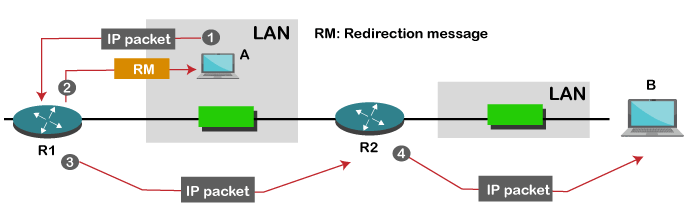
* **Time exceeded**

Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop. The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.

**Parameter problems**

The router and the destination host can send a parameter problem message. This message conveys that some parameters are not properly set.

Redirection



When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message. For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and redirection message to A so that A can update its routing table.

## Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) is a protocol that allows several devices to share one IP address so they can all receive the same data. IGMP is a network layer [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) used to set up multicasting on networks that use the [Internet Protocol](https://www.cloudflare.com/learning/network-layer/internet-protocol/) version 4 (IPv4). Specifically, IGMP allows devices to join a multicasting group.

Computers and other devices connected to a network use IGMP when they want to join a multicast group. A router that supports IGMP listens to IGMP transmissions from devices in order to figure out which devices belong to which multicast groups.

IGMP uses IP addresses that are set aside for multicasting. Multicast IP addresses are in the range between 224.0.0.0 and 239.255.255.255. (In contrast, any cast networks can use any regular IP address.) Each multicast group shares one of these IP addresses. When a router receives a series of packets directed at the shared IP address, it will duplicate those packets, sending copies to all members of the multicast group.

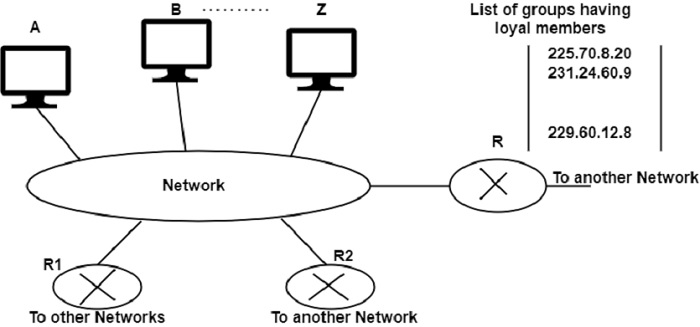
IGMP multicast groups can change at any time. A device can send an IGMP "join group" or "leave group" message at any point.

IGMP works directly on top of the Internet Protocol (IP). Each IGMP packet has both an IGMP header and an IP header. Just like [ICMP](https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/), IGMP does not use a transport layer protocol such as [TCP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) or [UDP](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/).

The IGMP protocol allows for several kinds of IGMP messages:

* Membership reports: Devices send these to a multicast router in order to become a member of a multicast group.
* "Leave group" messages: These messages go from a device to a router and allow devices to leave a multicast group.
* General membership queries: A multicast-capable router sends out these messages to the entire connected network of devices to update multicast group membership for all groups on the network.
* Group-specific membership queries: Routers send these messages to a specific multicast group, instead of the entire network.

IGMP operates locally. A multicast router connected to a network has a list of multicast addresses of the groups with at least one loyal member in that network, as shown in the figure below −



For each group, there is one router that has the duty of distributing the multicast packets destined for that group. This means that if there are three multicast routers connected to a network, their lists of group ids are mutually exclusive.

A host or multicast router can have membership in a group. When a host has membership, it means that one of its processes (an application program) receives multicast packets from some group. When a router has membership, it means that a network connection to one of its other interfaces receives these multicast packets. We say that the host or the router has an interest in the group. In both cases, the host and the router keep a list of group ids and relay their interest to the distributing router.

There are two other multicast routers (R1 and R2) that, depending on the group list maintained by router R, could be the recipients of router R in this network. Routers RI and R2 may be distributors for some of these groups in other networks but not on this network.

## Joining a Group

A host or a router can join a group. A host maintains a list of processes that have membership in a group. When a process wants to join a new group, it sends its request to the host.

The host adds the name of the process and the name of the requested group to its list. If this is the first entry for this particular group, the host sends a membership report message. If this is not the first entry, there is no need to send the membership report. As the host is already a member of the group; it receives multicast packets for this group.

The protocol requires that the membership report be sent twice, one after the other, within a few moments. In this way, if the first one is lost or damaged, the second one replaces it.

## Leaving a Group

When a host sees that no process is interested in a specific group, it sends a leave report. Similarly, when a router sees that none of the networks connected to its interfaces is interested in a specific group, it sends a leave report about that group.

However, when a multicast router receives a leave report, it cannot immediately purge that group from its list. This is because the report comes from just one host or router and there may be other hosts or routers that are still interested in that group. To make sure, the router sends a special query message and inserts the group id, or multicast address, related to the group.

The router allows a specified time for any host or router to respond. If during this time, no interest (membership report) is received, the router assumes that there are no loyal members in the network and purges the group from its list.

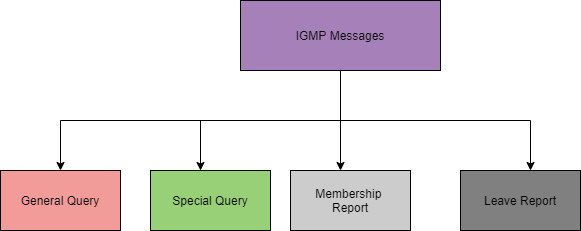
## IGMP Messages

There are two versions of IGMP: IGMPv1 and IGMPv2.

The version IGMPv2 has three types of messages:

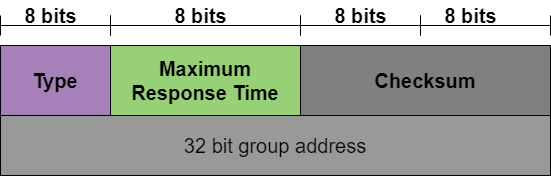
* The Query
* The Membership report
* The Leave report.

There are two types of Query messages:**General and Special**



## Message Format

Let us now take a look at the format of IGMP(Version 2):



**Unicast Routing Protocols**

A routing table can be either static or dynamic. A static table is one with manual entries. A dynamic table*,* on the other hand, is one that is updated automatically when there is a change somewhere in the internet. Today, an internet needs dynamic routing tables. The tables need to be updated as soon as there is a change in the internet. For instance, they need to be updated when a router is down, and they need to be updated whenever a better route has been found.

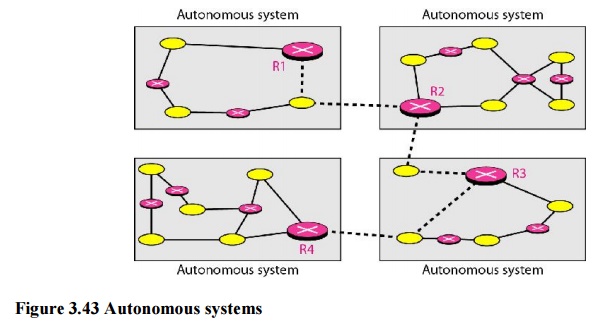
**1. Optimization**

A router receives a packet from a network and passes it to another network. A router is usually attached to several networks. One approach is to assign a cost for passing through a network. We call this cost a metric. However, the metric assigned to each network depends on the type of protocol. Some simple protocols, such as the Routing Information Protocol (RIP), treat all networks as equals. The cost of passing through a network is the same; it is one hop

count. So if a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.

**2. Intra- and Inter-domain Routing**

 An internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intradomain routing. Routing between autonomous systems is referred to as interdomain routing

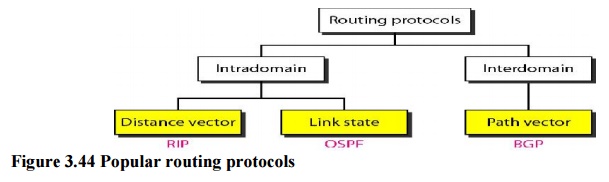


Several intradomain and interdomain routing protocols are in use.

O Two intradomain routing protocols: Distance vector and link state.

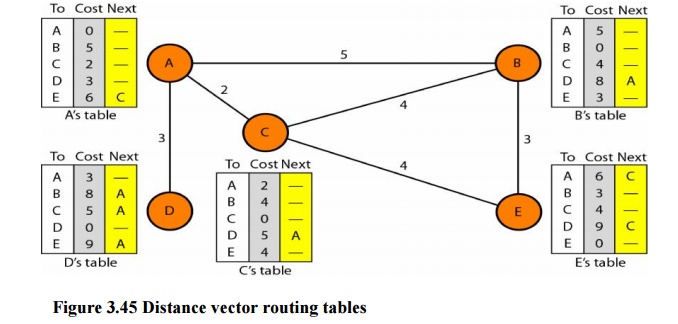
O One interdomain routing protocol: path vector.

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. Open Shortest Path First (OSPF) is an implementation of the link state protocol. Border Gateway Protocol (BGP) is an implementation of the path vector protocol.



**3. Distance Vector Routing**

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).



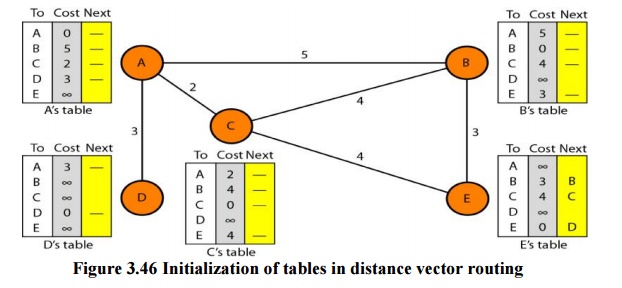
The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

**Initialization**

The tables in Figure 3.45 are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. The distance for any entry that is not a neighbor is marked as infinite (unreachable).

**Sharing**

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.



**Updating**

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

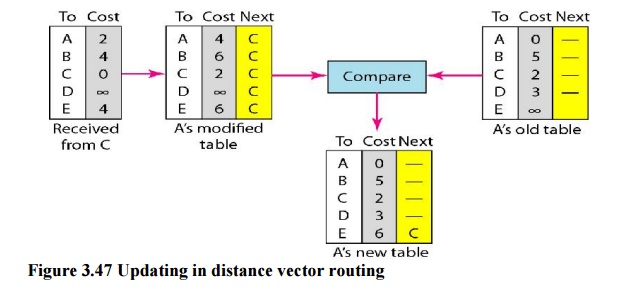
1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is *x* mi, and the distance between A and C is *y* mi, then the distance between A and that destination, via C, is *x* + *y* mi.

2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

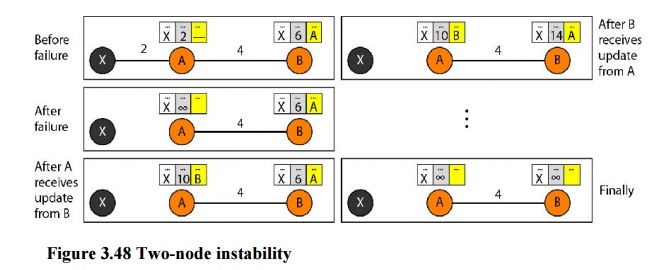
a)        If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

b)       If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3.



**Two-Node Loop Instability**

A problem with distance vector routing is instability, which means that a network using this protocol can become unstable. To understand the problem, let us look at the scenario depicted.

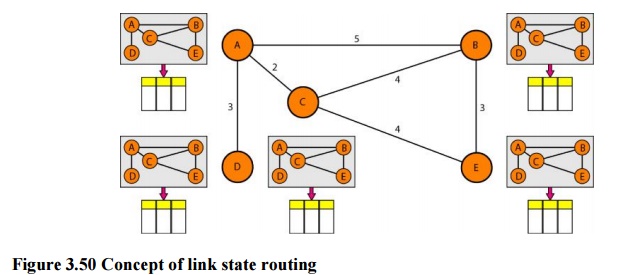


**Defining Infinity**The first obvious solution is to redefine infinity to a smaller number, such as100. For our previous scenario, the system will be stable in less than 20 update s. As a matter of fact, most implementations of the distance vector protocol define the distance between each node to be I and define 16 as infinity. However, this means that the distance vector routing cannot be used in large systems. The size of the network, in each direction, cannot exceed 15 hops.

**Split Horizon**Another solution is called split horizon. In this strategy, instead of flooding thetable through each interface, each node sends only part of its table through each interface. If, according to its table, node B thinks that the optimum route to reach X is via A, it does not need to advertise this piece of information to A; the information has corne from A (A already knows). Taking information from node A, modifying it, and sending it back to node A creates the confusion. In our scenario, node B eliminates the last line of its routing table before it sends it to A. In this case, node A keeps the value of infinity as the distance to X.

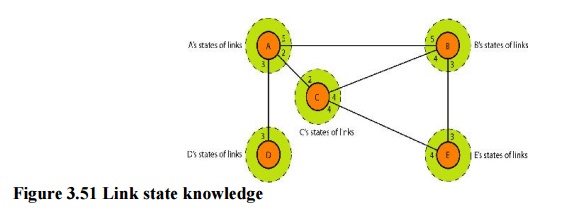
**4. Link State Routing**

 Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.



**Figure 3.50 Concept of link state routing**

The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination



**Building Routing Tables:**

**In link state routing,**four sets of actions are required to ensure that each node has therouting table showing the least-cost node to every other node.

 a) Creation of the states of the links by each node, called the link state packet (LSP).

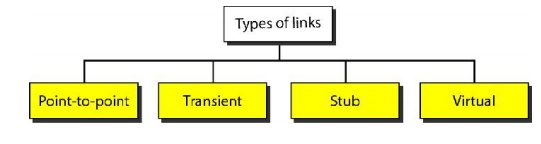
b)Dissemination of LSPs to every other router, called **flooding,** in an efficient and  reliable way.

c) Formation of a shortest path tree for each node.

d)Calculation of a routing table based on the shortest path tree.

**Types of Links**

 In OSPF terminology, a connection is called a *link.* Four types of links have been defined: point-to-point, transient, stub, and virtual.



**Figure 3.52 Types of links**

A point-to-point link connects two routers without any other host or router in between. In other words, the purpose of the link (network) is just to connect the two routers. An example of this type of link is two routers connected by a telephone line or a T line. There is no need to assign a network address to this type of link. Graphically, the routers are represented by nodes, and the link is represented by a bidirectional edge connecting the nodes. The metrics, which are usually the same, are shown at the two ends, one for each direction. In other words, each router has only one neighbor at the other side of the link.

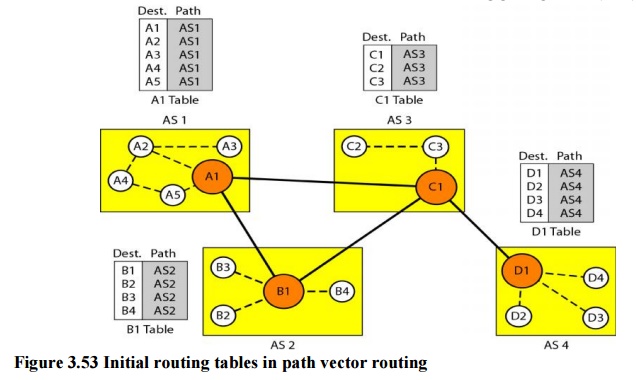
**5. Path Vector Routing**

Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

Path vector routing proved to be useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node in each autonomous system that acts on behalf of the entire autonomous system.

**Initialization**

At the beginning, each speaker node can know only the reach ability of nodes inside its autonomous system

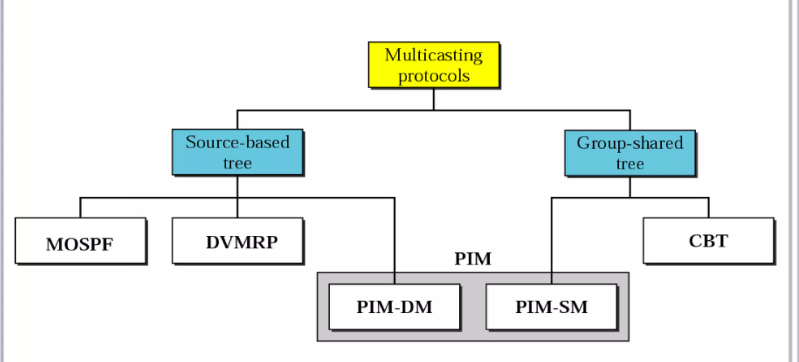


**Figure 3.53 Initial routing tables in path vector routing**

Node Al is the speaker node for AS1, B1 for AS2, C1 for AS3, and Dl for AS4. Node Al creates an initial table that shows Al to A5 are located in ASI and can be reached through it. Node B1 advertises that Bl to B4 are located in AS2 and can be reached through Bl. And so on.

**Multicast Routing Protocols**

A multicast routing protocol is one type of service provider that functions as a client within the framework of the router architecture. The routing architecture is designed to be extended by such router client modules.



* **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.

Common shortest path algorithms are:

* Dijkstra's algorithm
* Bellman Ford algorithm
* Floyd Warshall algorithm