UNIT-IV

Network layer: Internet Protocol, IPv6, ARP, DHCP, ICMP, Routing algorithms: Distance vector, Link state, Metrics, Inter-domain routing. Sub netting, Super netting, Classless addressing, Network Address Translation.

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 network layer is responsible for the delivery of individual packets from the source to the destination 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.

IPv6

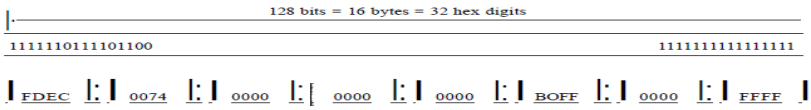
- IP address is your digital identity. It’s a network address for your computer so the Internet knows where to send you emails, data, etc.
- *IP address determines who and where you are in the network of billions of digital devices that are connected to the Internet.*

Structure

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.

Hexadecimal Colon Notation

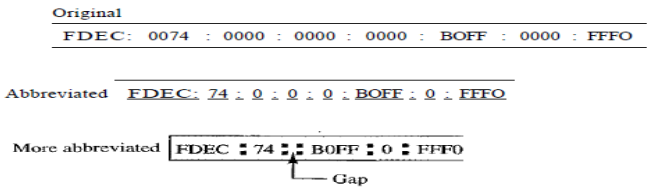
- To make addresses more readable, IPv6 specifies hexadecimal colon notation. In this notation,
- 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal
- notation requires four hexadecimal digits



Abbreviation

- It is very long, many of the digits are zeros.
- The leading zeros of a section (four digits between two colons) can be omitted.
- Only the leading zeros can be dropped, not the trailing zeros

Abbreviated IPv6 addresses



Address Space

- IPv6 has a much larger address space 2128 addresses are available.
- The designers ofIPv6 divided the address into several categories. A few leftmost bits, called the *type prefix*, in each address define its category.

Table 19.5 *Type prefixes for 1Pv6 addresses*

Type Prefix	*Type*	*Fraction*
00000000	Reserved	1/256
00000001	Unassigned	1/256
0000001	ISO network addresses	1/128
0000010	IPX (Novell) network addresses	1/128
0000011	Unassigned	1/128
00001	Unassigned	1/32
0001	Reserved	*1/16*
001	Reserved	1/8
010	Provider-based unicast addresses	*1/8*

Types of IPV6 Addresses

Unicast addresses

→A unicast address defines a single computer.
→The packet sent to a unicast address must be delivered to that specific computer.
→IPv6 defines two types of unicast address:
→Geo-graphically based
→Provider-based

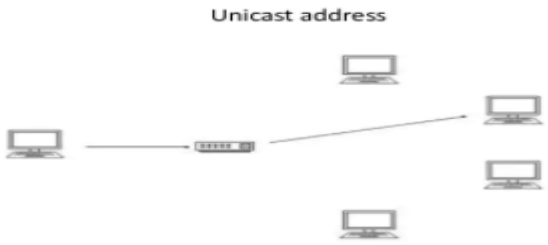
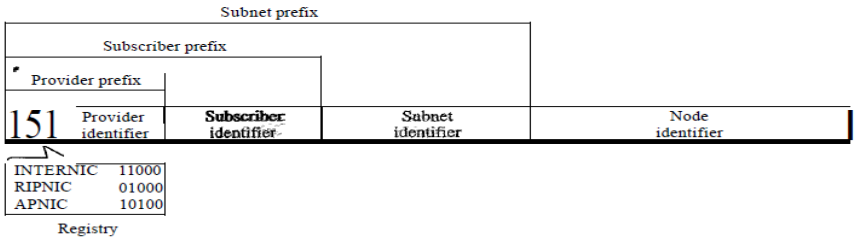


Figure 19.16 *Prefixes for provider-based unicast address*



Fields for the provider based are as follows

o **Type identifier.** This 3-bit field defines the address as a provider-base.d address.

o **Registry identifier.** This 5-bit field

- Three registry centers:. INTERNIC ,RIPNIC ,APNIC

Provider identifier. This variable-length field identifies the provider for Internet access (such as an ISP). A 16-bit length is recommended for this field.

o Subscriber identifier. When an organization subscribes to the Internet through a provider, it is assigned a subscriber identification. A 24-bit length is recommended for this field.

o Subnet identifier. The subnet identifier defines a specific subnet work under the territory of the subscriber. A 32-bit length is recommended for this field.

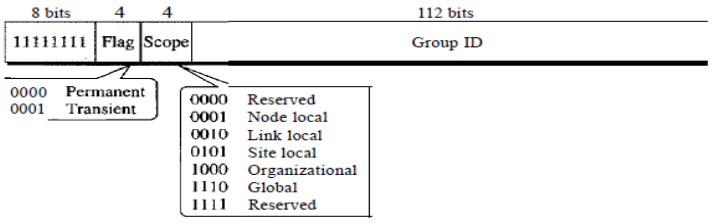
o Node identifier:48 bit field. Define the identity of the node connected to a subnet.

Multicast Addresses

Multicast Addresses

→Used to define a group of hosts instead of just one.

Figure 19.17 *Multicast address in IPv6*



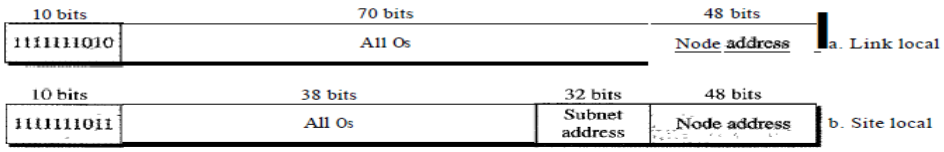
→A packet sent to a multicast address must be delivered to each member of the group.
→Second field is a flag that defines the group address , either permanent or transient.
→A permenent group address is defined by the Internet authorities and can be accessed at all times.
→A transient group address, on the other hand is used only temporarily.

Local Addresses

→It is used when an organization wants to use IPv6 protocol without being connected to the global Internet.

→They provide addressing for private network.

Figure 19.19 *Local addresses in IPv6*



A link local address is used in an isolated subnet; a site local address is used in an isolated site with several subnets

FEATURES

- Larger Address Space
- No Broadcast
- Anycast Support
- Mobility
- Extensibility

Advantages of IPv6

Reliability

Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.

Stringer Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.

- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

Disadvantages of IPv6

Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.

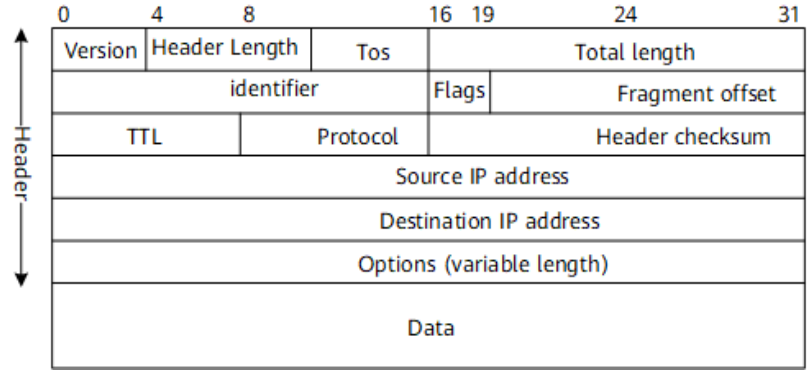
Communication: IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible

The major differences between IPv4 and IPv6 are:

IPv4 (Internet Protocol Version 4)	**IPv6 (Internet Protocol Version 6)**
Encryption and authentication is not provided in IPv4 (Internet Protocol Version 4).	Encryption and authentication is provided in IPv6 (Internet Protocol Version 6)
Header of IPv4 is 20 – 60 bytes.	Header of IPv6 is fixed at 40 bytes
Checksumfield is available in IPv4.	Checksumfield is not available in IPv6.
Packet flow identification is not available in IPv4 (Internet Protocol Version 4).	Packet flow identification is available in IPv6. Flow label field is available in the header.

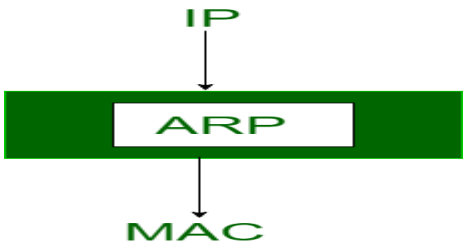
IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots.	An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits.
Sender and forwarding routers performs fragmentation in IPv4	Fragmentation is performed only by the sender in IPv6.
In IPv4, security features relies on application	In IPv6, there is an inbuilt security feature named IPSEC.
End to end connection integrity cannot be achieved in IPv4.	End to end connection integrity can be done in IPv6.
IPv4 supports DHCP and Manual address configuration	IPv6 supports renumbering and auto address configuration.
IPv4 addresses are 32-bit long	IPv6 addresses are 128 bits long.
The address space in IPv4 is 4.29 ×109	The address space in IPv6 is 3.4 ×1038
IPv4 has a broadcast message transmission scheme.	Multicast and Anycast message transmission scheme is available in IPv6

Ipv4 header format



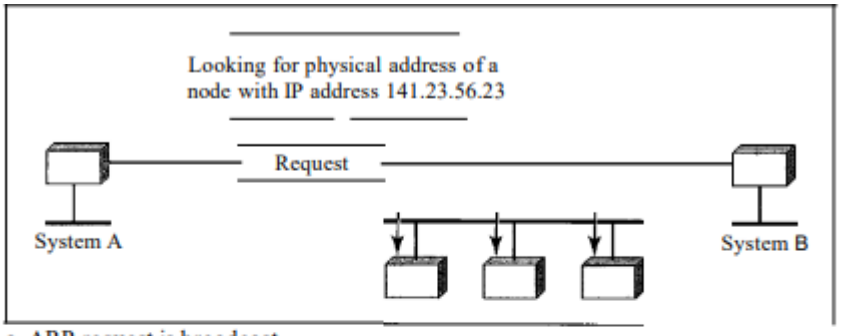
ARP

Address Resolution Protocol is one of the most important protocols of the network layer in the OSI model which helps in finding the MAC(Media Access Control) address given the IP address of the system i.e. the main duty of the ARP is **to convert the 32-bit IP address(for IPv4) to 48-bit address i.e. the MAC address**.0ARP (address Resolution Protocol) is main protocol in the TCP/IP suite in the network layer of the OSI model. It is **used to obtain the Media Access Control address (MAC) of the host system**. It establishes a mapping between IP address and MAC address of the host system in the database.

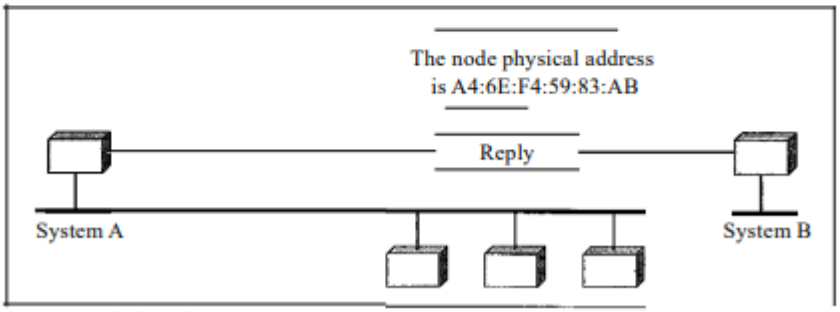


Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packe

ARP operation



a. ARP request is broadcast

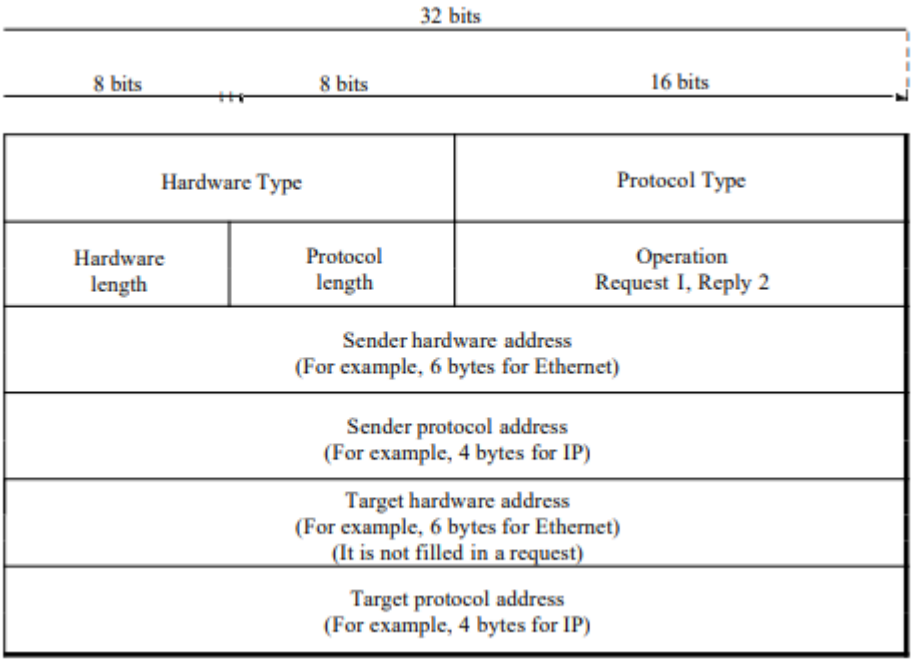


b. ARP reply is unicast

In Figure 21.1a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IF address of 141.23.56.23.

This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure 21.1 b. System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination by using the physical address it received

Packet Format



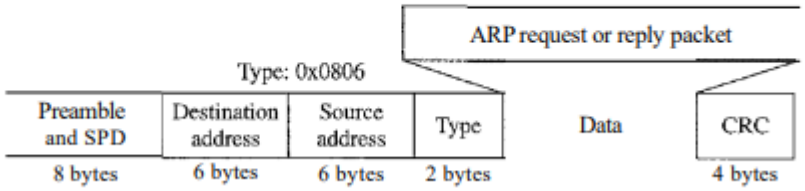
Thc fields arc as follows:

- Hardware type. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
- Protocol type. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 0800_{16}. ARP can be used with any higher-level protocol.
- Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
- Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) andARP reply (2).
- Sender hardware address. This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
- Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- Target hardware address. This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is alIOs because the sender does not know the physical address of the target.
- Target protocol address. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

Encapsulation

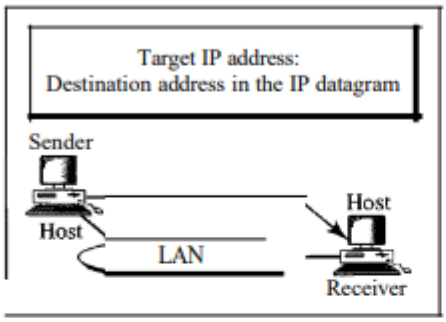
An ARP packet is encapsulated directly into a data link frame. For example, in Figure 21.3 an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame are an ARP packet.

Figure 21.3 *Encapsulation of ARP packet*

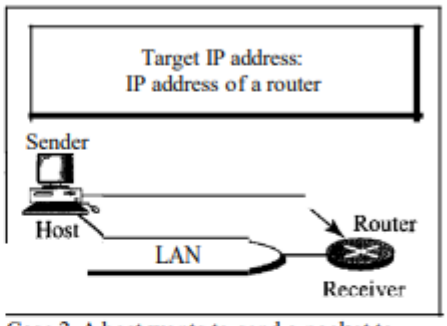


Four Different Cases

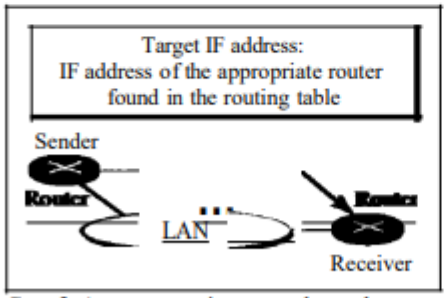
Figure 21.4 *Four cases using ARP*



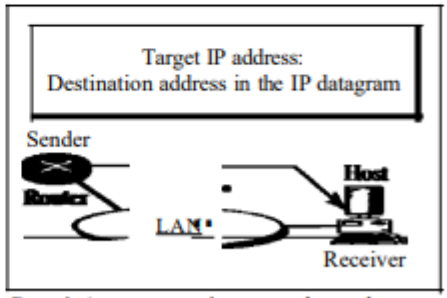
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

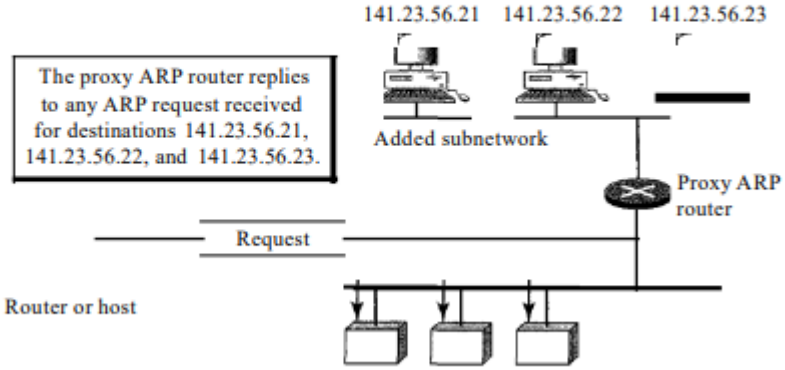


Case 4. A router receives a packet to be sent to a host on the same network.

ProxyARP

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router. Let us give an example. In Figure 21.6 the ARP installed on the right-hand host will answer only to anARP request with a target IP address of 141.23.56.23.

Figure 21.6 *Proxy ARP*



However, the administrator may need to create a subnet without changing the whole system to recognize subnetted addresses. One solution is to add a router running a proxy ARP. In this case, the router acts on behalf of all the hosts installed on the subnet. When it receives an ARP request with a target IP address that matches the address of one of its proteges (141.23.56.21, 141.23.56.22, or 141.23.56.23), it sends an ARP reply and announces its hardware address as the target hardware address. When the router receives the IP packet, it sends the packet to the appropriate host.

ARP: ARP stands for (**Address Resolution Protocol**) it is responsible to find the hardware address of a host from a know IP address there are three basic **ARP** terms.
The important terms associated with **ARP** are:
(i) Reverse ARP

(ii) Proxy ARP

(iii) Inverse ARP

1. **ARP Cache:** After resolving the MAC address, the ARP sends it to the source where it is stored in a table for future reference. The subsequent communications can use the MAC address from the table
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across the destination MAC address or not.
   1. The physical address of the sender.
   2. The IP address of the sender.
   3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.

4. The IP address of the receiver

4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

- **CASE-1:** The sender is a host and wants to send a packet to another host on the same network.
  - Use ARP to find another host's physical address
- **CASE-2:** The sender is a host and wants to send a packet to another host on another network.
  - The sender looks at its routing table.
  - Find the IP address of the next-hop (router) for this destination.
  - Use ARP to find the router's physical address
- **CASE-3:** the sender is a router and received a datagram destined for a host on another network.
  - The router checks its routing table.
  - Find the IP address of the next router.

Advantages of using ARP

- We can easily find out the MAC address of the device if we know the IP address of that device.
- It is not necessary to configure the address of the end nodes for the MAC address. We can find it when needed.

Disadvantages of using ARP

- ARP attacks such as ARP spoofing and ARP denial of service may occur.

RARP

RARP Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.

Dynamic Host Configuration Protocol.

Every computer on a network has to have an I.P. address.

2 ways that a computer can be assigned an I.P. address.

DHCP (IPV4/V6)

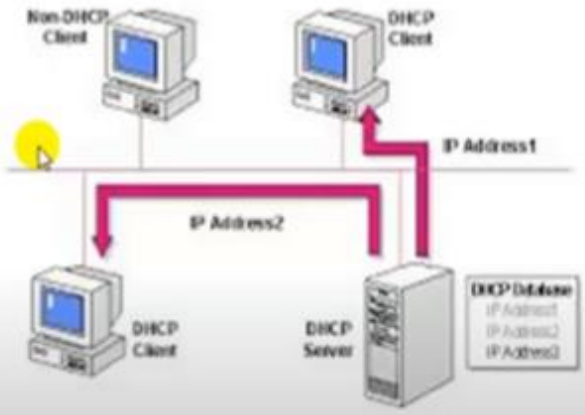
NETWORK ONLINE ACADEMY

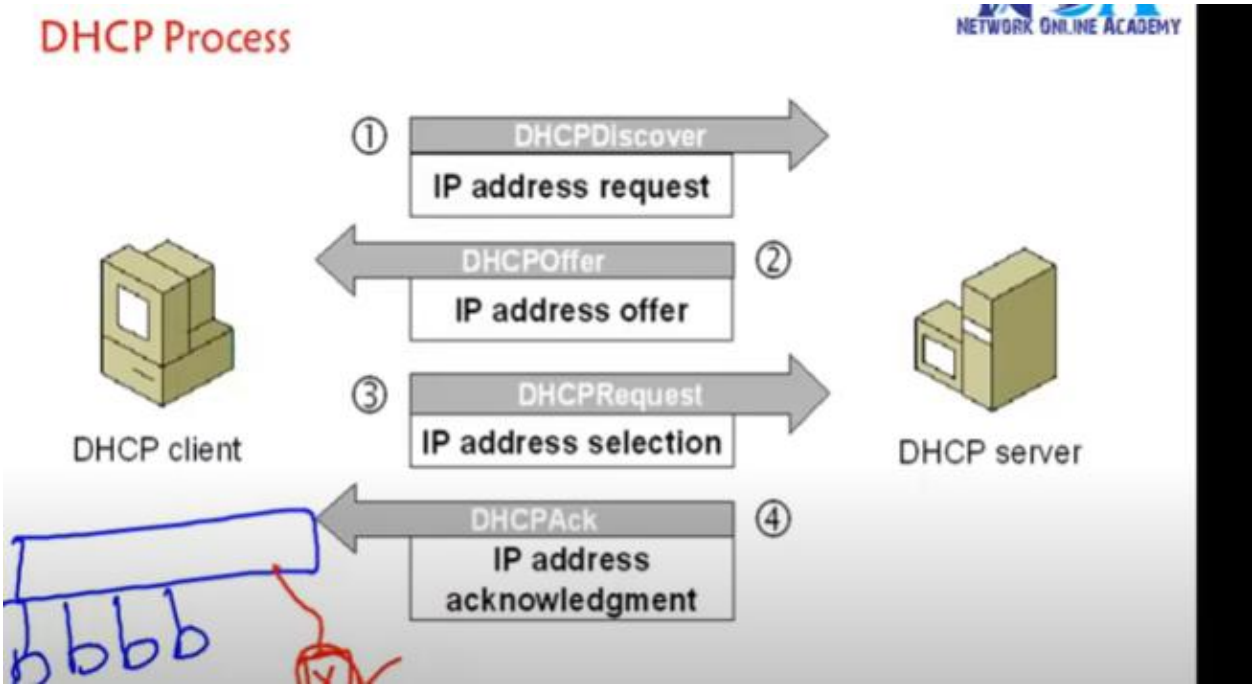
allows a server to dynamically distribute IP addressing and configuration information to clients.

- IP Address
- Subnet Mask
- Default Gateway
- DNS server

Advantages :

- Centralized network client configuration
- easier IP address management
- Reduced network administration.
- large network support





The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.

- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

DHCP provides static and dynamic address allocation that can be manual or automatic.

Static Address Allocation In this capacity DHCP acts as BOOTP does. It is backwardcompatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.

Dynamic Address Allocation DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

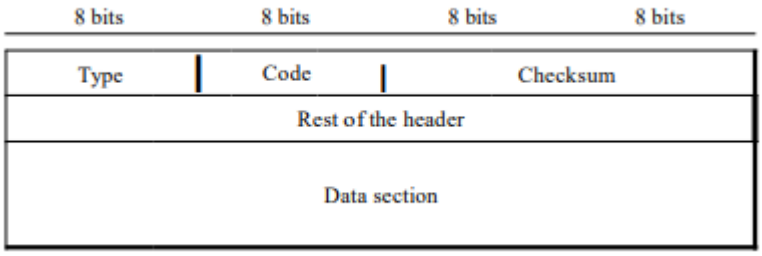
ICMP

The IP protocol has no error-reporting or error-correcting mechanism.

The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protoco1.

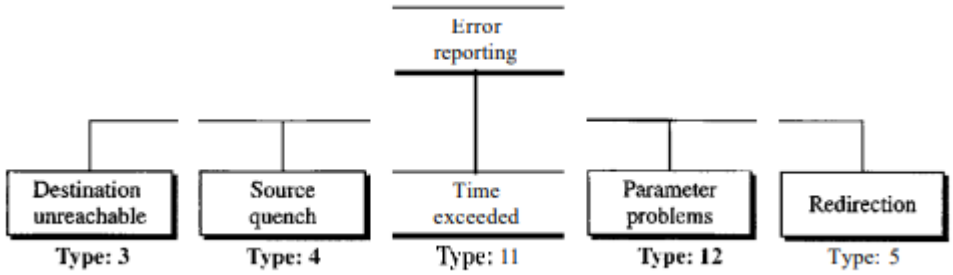
Types of Messages ICMP messages are divided into two broad categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages

Message Format An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all.



Error Reporting One of the main responsibilities of ICMP is to report errors. Although technology has produced increasingly reliable transmission media

ICMP always reports error messages to the original source.



Destination Unreachable

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram

Source Quench

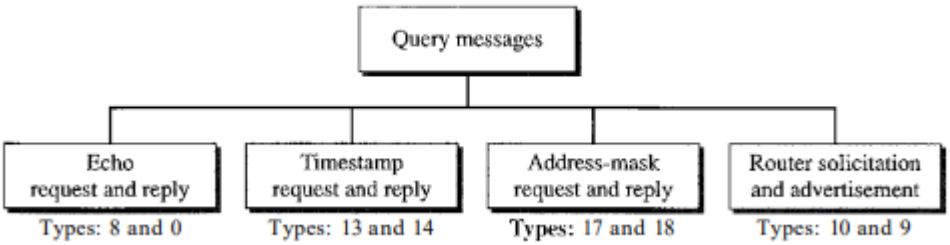
The IP protocol is a connectionless protocol. There is no communication between the source host, which produces the datagram, the routers, which forward it, and the destination host, which processes it.

Time Exceeded The time-exceeded message is generated in two cases: As we see in Chapter 22, routers use routing tables to find the next hop (next router) that must receive the packet

Parameter Problem Any ambiguity in the header part of a datagram can Create serious problems as the datagram travels through the Internet

Redirection When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate route

Query In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages



Link State Routing –

Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Features of link state routing protocols –

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection of information gathered from the link-state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results in the shortest path
- **Routing table –** A list of known paths and interfaces.

Calculation of shortest path –

To find the shortest path, each node needs to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree-like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.

- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats Step 2. and Step 3. until all the nodes are added to the tree

Link State protocols in comparison to Distance Vector protocols have:

1. It requires a large amount of memory.
2. Shortest path computations require many CPU circles.
3. If a network uses little bandwidth; it quickly reacts to topology changes
4. All items in the database must be sent to neighbors to form link-state packets.
5. All neighbors must be trusted in the topology.
6. Authentication mechanisms can be used to avoid undesired adjacency and problems.
7. No split horizon techniques are possible in the link-state routing.

- Open Shortest Path First (OSPF) is a unicast routing protocol developed by a working group of the Internet Engineering Task Force (IETF).
- It is an intradomain routing protocol.
- It is an open-source protocol.
- It is similar to Routing Information Protocol (RIP)
- OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6).
- OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol
- IP datagram that carries the messages from OSPF sets the value of the protocol field to 89
- OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm
- OSPF has two versions – version 1 and version 2. Version 2 is used mostly

OSPF Messages – OSPF is a very complex protocol. It uses five different types of messages. These are as follows:

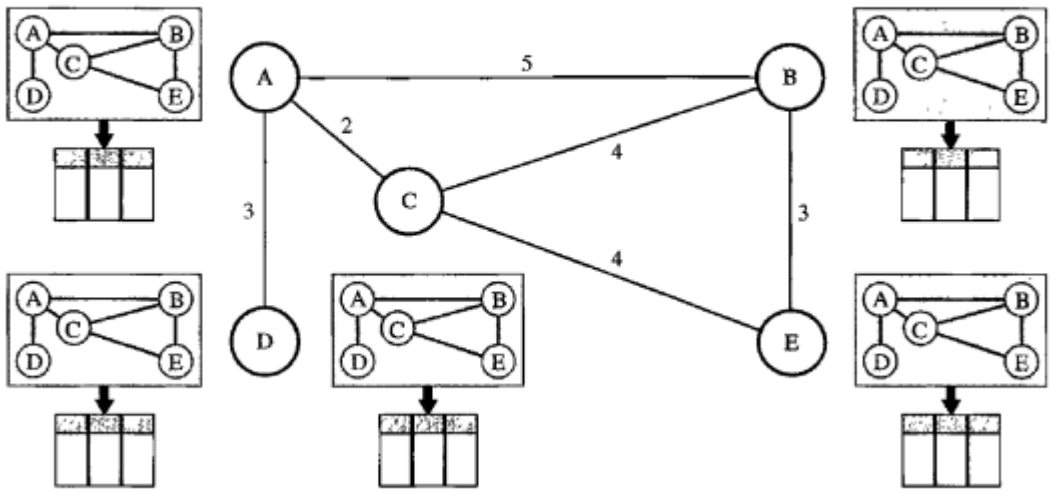
1. **Hello message (Type 1) –** It is used by the routers to introduce themselves to the other routers.
2. **Database description message (Type 2) –** It is normally sent in response to the Hello message.
3. **Link-state request message (Type 3) –** It is used by the routers that need information about specific Link-State packets.

4. **Link-state update message (Type 4) –** It is the main OSPF message for building Link-State Database.

5. **Link-state acknowledgement message (Type 5) –** It is used to create reliability in the OSPF protocol.

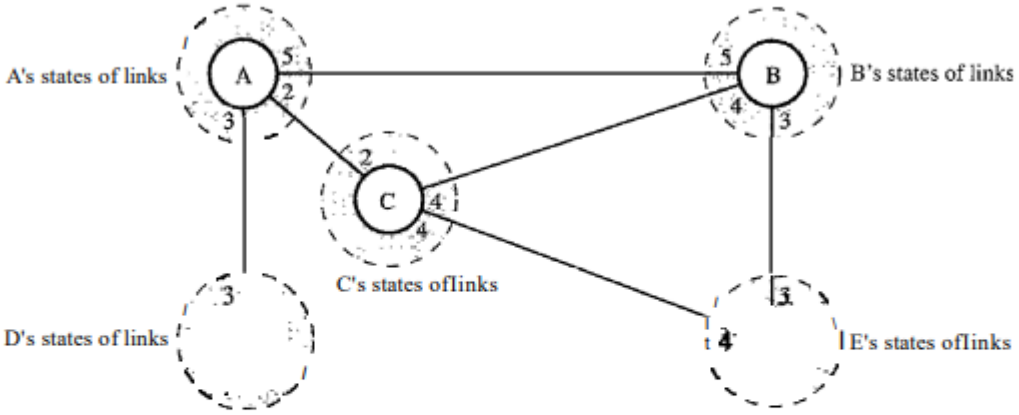
Link State Routing Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domainthe list of nodes and links, how they are connected including the type, cost (metric), and condition of the links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

Figure 22.20 *Concept oflink 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.

Figure 22.21 *Link state knowledge*



Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3. Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4. Node D knows that it is connected only to node A with metric 3. And so on. Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

Building Routing Tables

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

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

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

3. Formation of a shortest path tree for each node.

4. Calculation of a routing table based on the shortest path tree. Creation of Link State Packet (LSP) A link state packet can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount

1. When there is a change in the topology ofthe domain. Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology

. 2. On a periodic basis. The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination. It is done to ensure that old information is removed from the domain. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

Figure 22.22 *Dijkstra algorithm*

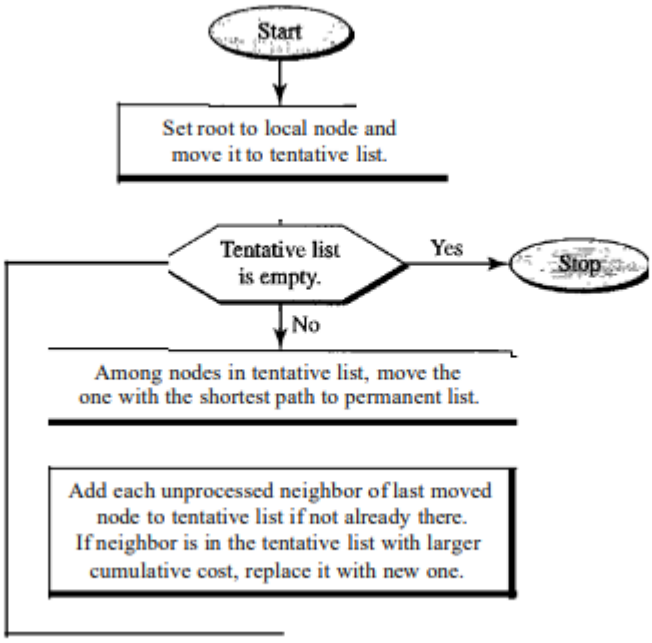


Figure 22.23 *Example offormation ofshortest path tree*

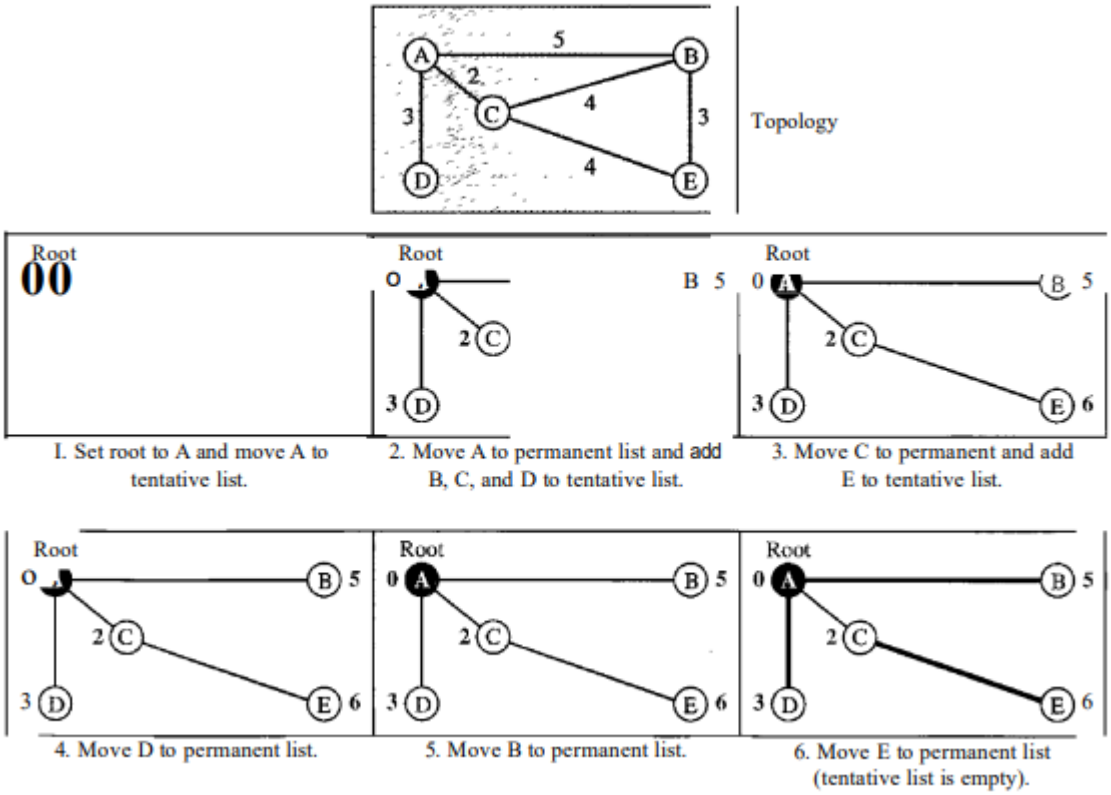


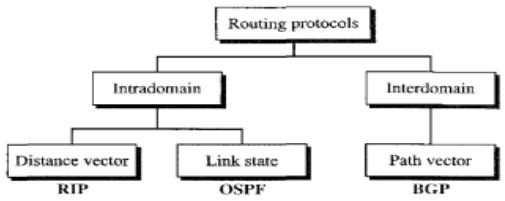
Table 22.2 *Routing table for node A*

Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

Intradomain and interdomain routing protoco

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

Figure 22.13 *Popular routing protocols*



I***ntra-domain routing***

-->routing within an AS(Autonomous System).
-->ignores the internet outside the autonomous system.
-->protocols for intra domain routing are also called **interior gateway** protocols.
-->popular protocols are **RIP** ams **OSPF**.

Inter-domain routing

-->routing between AS's.

-->assumes that the internet consists of a collection of interconnected AS's.

-->protocol for inter domain routing are also called **exterior gateway** protocols.

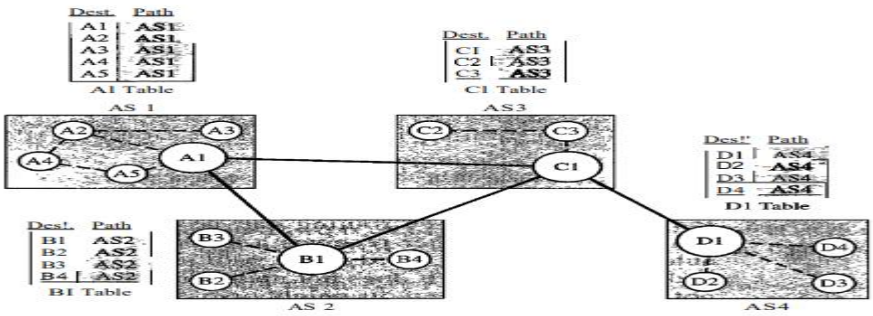
-->routing protocols are **BGP**.

A path vector protocol

I t does not rely on the cost of reaching a given destination to determine whether each path available is loop free or not. Instead, path vector protocols rely on analysis of the path to reach the destination to learn if it is loop free or not

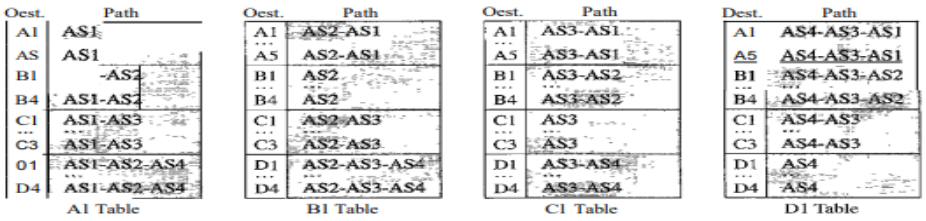
Initialization At the beginning, each speaker node can know only the reachability of nodes inside its autonomous system. Figure 22.30 shows the initial tables for each speaker node in a system made of four ASs.

Figure 22.30 *Initial routing tables in path vector routing*



Loop prevention. The instability of distance vector routing and the creation of loops can be avoided in path vector routing. When a router receives a message, it checks to see if its autonomous system is in the path list to the destination. If it is, looping is involved and the message is ignored.

Figure 22.31 *Stabilized tables for three autonomous systems*



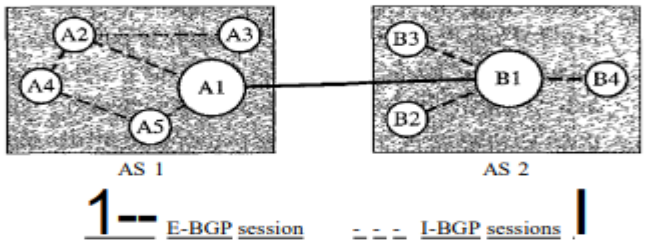
BGP Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.

Types of Autonomous Systems As we said before, the Internet is divided into hierarchical domains called autonomous systems. For example, a large corporation that manages its own network and has full control over it is an autonomous system. A local ISP that provides services to local customers is an autonomous system. We can divide autonomous systems into three categories: stub, multihomed, and transit.

- **Stub** AS. A stub AS has only one connection to another AS. The interdomain data traffic in a stub AS can be either created or terminated in the AS. The hosts in the AS can send data traffic to other ASs. The hosts in the AS can receive data coming from hosts in other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS

- Multihomed AS. A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
- Transit AS. A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

Figure 22.32 *Internal and external BGP sessions*



The session established between AS 1 and AS2 is an E-BOP session. The two speaker routers exchange information they know about networks in the Internet. However, these two routers need to collect information from other routers in the autonomous systems. This is done using I-BOP sessions.

Classless Addressing

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

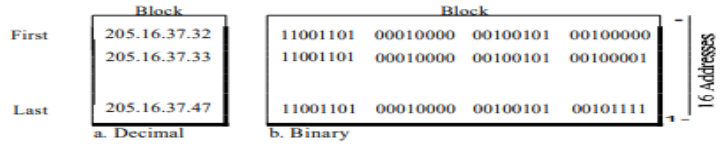
Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...).
3. The first address must be evenly divisible by the number of addresses.

Example 19.5

Figure 19.3 shows a block of addresses, in both binary and dotted-decimal notation, granted to a small business that needs 16 addresses.

Figure 19.3 *A block of 16 addresses granted to a small organization*



Mask

A better way to define a block of addresses is to select any address in the block and the mask. As we discussed before, a mask is a 32-bit number in which the n leftmost bits

In 1Pv4 addressing, a block of addresses can be defined as
x.y.z.tln
in which x.y.z.t defines one of the addresses and the *In* defines the mask.

First Address The first address in the block can be found by setting the 32 - n rightmost bits in the binary notation of the address to Os.

The first address in the block can be found by setting the rightmost 32 - n bits to Os.

Last Address The last address in the block can be found by setting the 32 - n rightmost bits in the binary notation of the address to Is.

The last address in the block can be found by setting the rightmost 32 - n bits to Is.

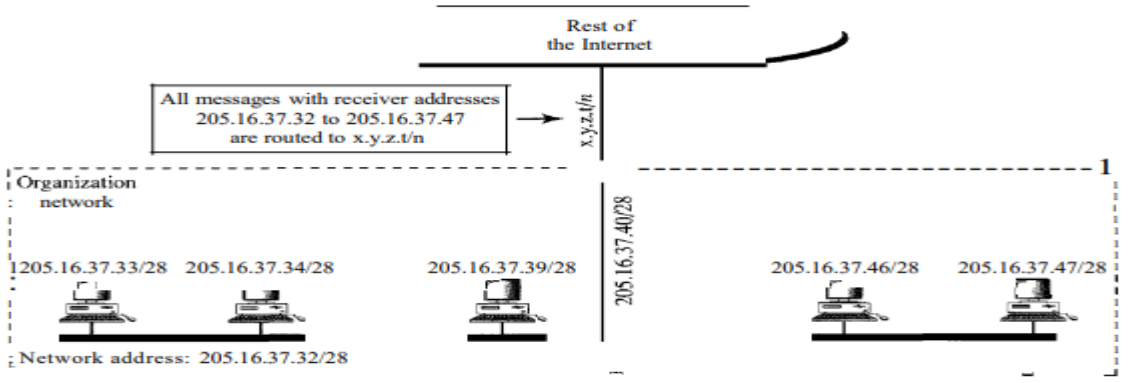
Number of Addresses The number of addresses in the block is the difference between the last and first address. It can easily be found using the formula 2^{32-n}.

The number of addresses in the block can be found by using the formula 2^{32-n}.

Network Addresses

A very important concept in IP addressing is the network address. When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet. The first address in the class, how-

Figure 19.4 *A network configuration for the block 205.16.37.32/28*

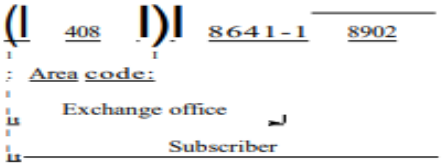


The organization network is connected to the Internet via a router. The router has two addresses. One belongs to the granted block; the other belongs to the network that is at the other side of the router. We call the second address *x.y.z.t/n* because we do not know anything about the network it is connected to at the other side. All messages destined for addresses in the organization block (205.16.37.32 to 205.16.37.47) are sent, directly or indirectly, to *x.y.z.t/n*. We say directly or indirectly because we do not know the structure of the network to which the other side of the router is connected.

Hierarchy

IP addresses, like other addresses or identifiers we encounter these days, have levels of hierarchy. For example, a telephone network in North America has three levels of hier-

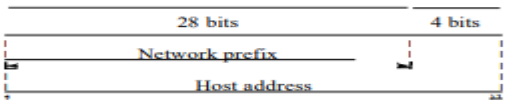
Figure 19.5 *Hierarchy in a telephone network in North America*



Two-Level Hierarchy: No Subnetting

An IP address can define only two levels of hierarchy when not subnetted. The *n* leftmost bits of the address *x.y.z.tJn* define the network (organization network); the 32 - *n*

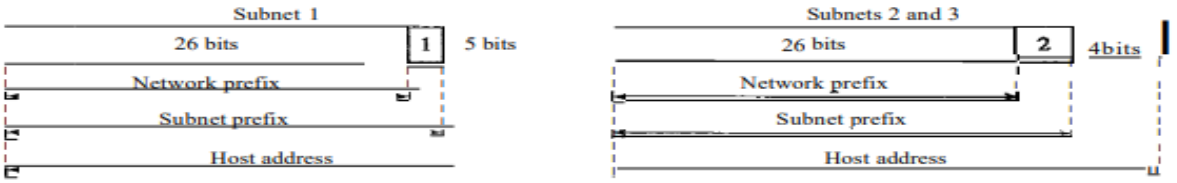
Figure 19.6 *Two levels of hierarchy in an IPv4 address*



The prefix is common to all addresses in the network; the suffix changes from one device to another.

Each address in the block can be considered as a two-level hierarchical structure:
the leftmost *n* bits (prefix) define the network;
the rightmost 32 - *n* bits define the host.

Figure 19.8 *Three-level hierarchy in an IPv4 address*



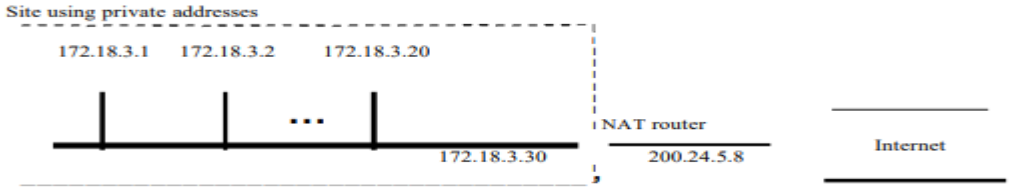
Network Address **Translation** (NAT)

The number of home users and small businesses that want to use the Internet is ever increasing. In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time. An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a

Table 19.3 *Addresses for private networks*

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

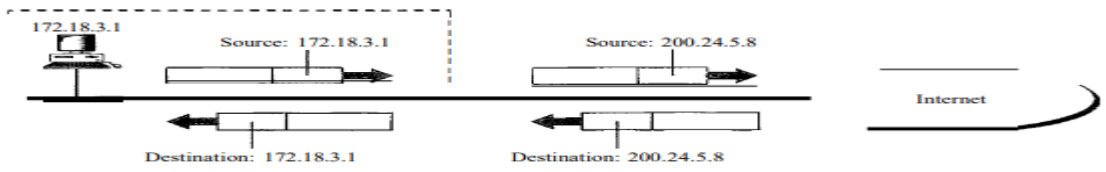
Figure 19.10 *A NAT implementation*



Address Translation

All the outgoing packets go through the NAT router, which replaces the *source address* in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the *destination address* in the packet (the NAT router global address) with the appropriate private address. Figure 19.11 shows an example of address translation.

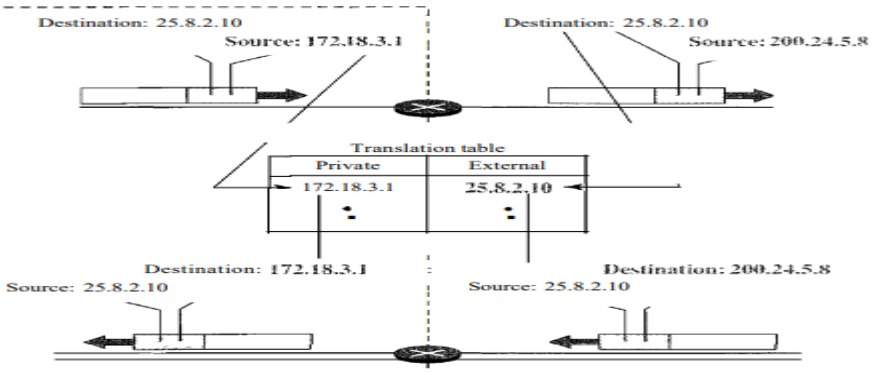
Figure 19.11 *Addresses in a NAT*



Translation Table

The reader may have noticed that translating the source addresses for outgoing packets is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses,

Figure 19.12 *NAT address translation*



25.8.3.2. If the translation table has five columns, instead of two, that include the source and destination port numbers of the transport layer protocol, the ambiguity is eliminated. We discuss port numbers in Chapter 23. Table 19.4 shows an example of such a table.

Table 19.4 *Five-column translation table*

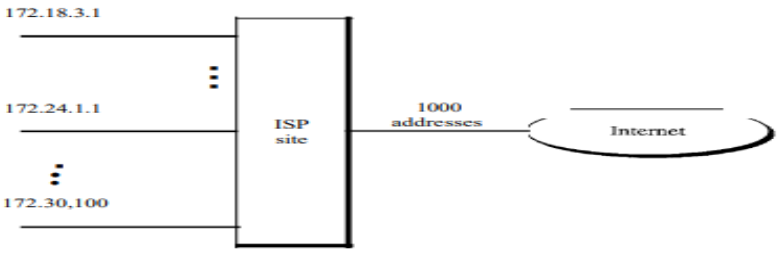
Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

Note that when the response from HTTP comes back, the combination of source address (25.8.3.2) and destination port number (1400) defines the-private network host to which the response should be directed. Note also that for this translation to work, the temporary port numbers (1400 and 1401) must be unique.

NAT and ISP

An ISP that serves dial-up customers can use NAT technology to conserve addresses. For example, suppose an ISP is granted 1000 addresses, but has 100,000 customers. Each of the customers is assigned a private network address. The ISP translates each of the 100,000 source addresses in outgoing packets to one of the 1000 global addresses; it translates the global destination address in incoming packets to the corresponding private address. Figure 19.13 shows this concept.

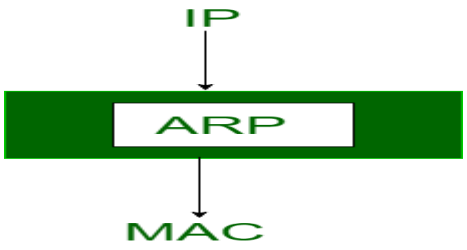
Figure 19.13 *An ISP and NAT*



S.NO	Subnetting	Supernetting
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in supernetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

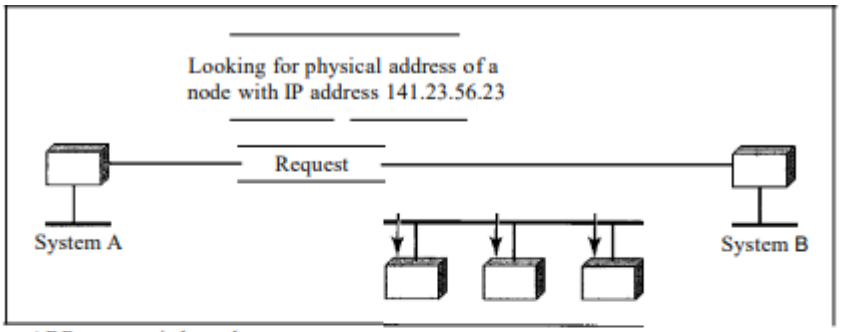
ARp

ARP (address Resolution Protocol) is main protocol in the TCP/IP suite in the network layer of the OSI model. It is **used to obtain the Media Access Control address (MAC) of the host system**. It establishes a mapping between IP address and MAC address of the host system in the database.

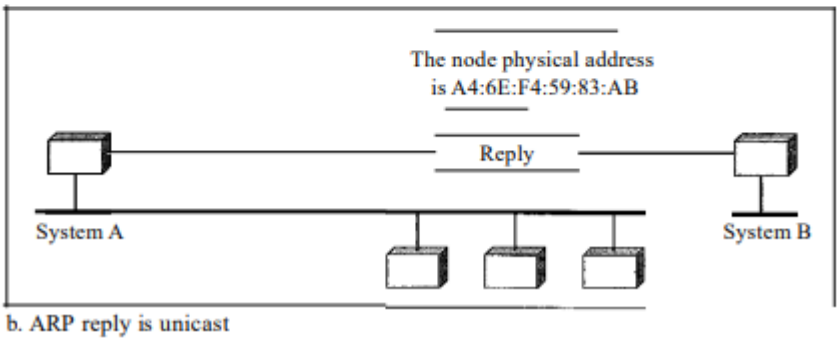


Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packe

ARP operation



a. ARP request is broadcast

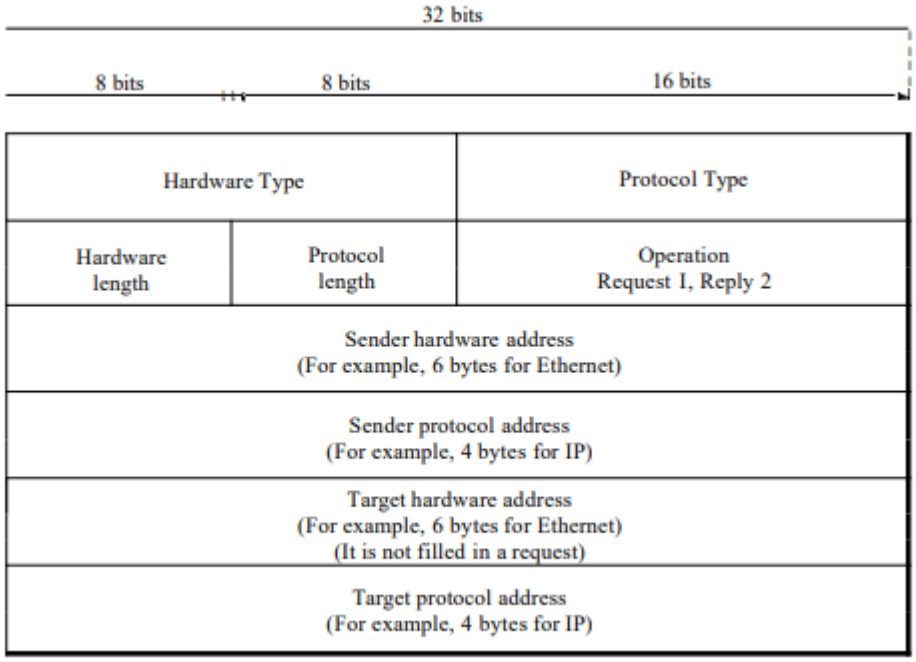


b. ARP reply is unicast

In Figure 21.1a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IF address of 141.23.56.23.

This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure 21.1 b. System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination by using the physical address it received

Packet Format



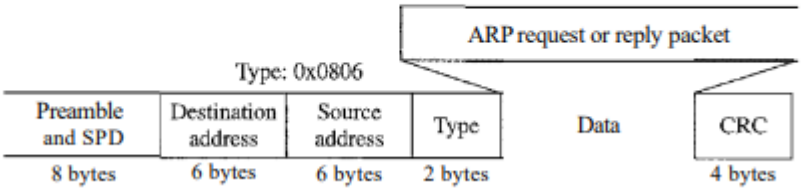
Thc fields arc as follows:

- Hardware type. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
- Protocol type. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 0800_{16}. ARP can be used with any higher-level protocol.
- Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
- Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) andARP reply (2).
- Sender hardware address. This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
- Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- Target hardware address. This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is allOs because the sender does not know the physical address of the target.
- Target protocol address. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

Encapsulation

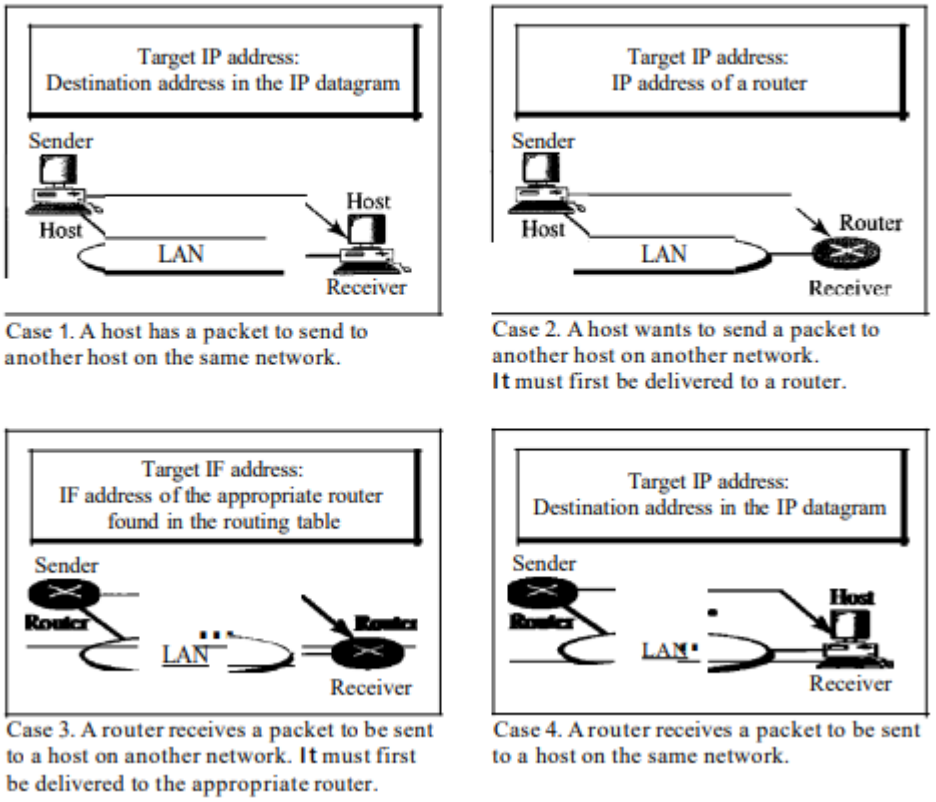
An ARP packet is encapsulated directly into a data link frame. For example, in Figure 21.3 an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame are an ARP packet.

Figure 21.3 *Encapsulation ofARP packet*



Four Different Cases

Figure 21.4 *Four cases using ARP*



Case 1. A host has a packet to send to another host on the same network.

Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.

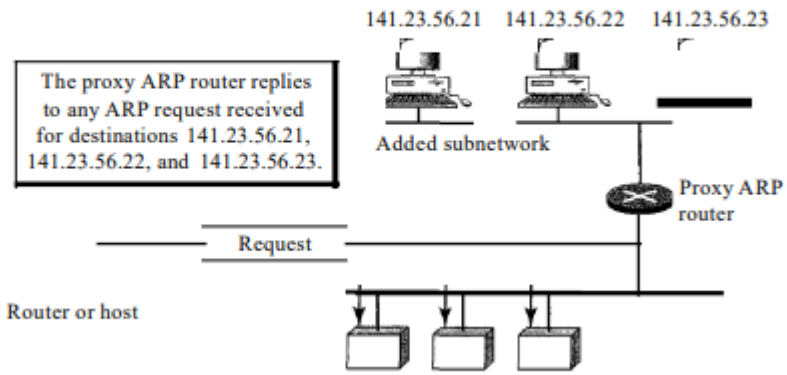
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

Case 4. A router receives a packet to be sent to a host on the same network.

ProxyARP

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router. Let us give an example. In Figure 21.6 the ARP installed on the right-hand host will answer only to anARP request with a target IP address of 141.23.56.23.

Figure 21.6 *Proxy ARP*



However, the administrator may need to create a subnet without changing the whole system to recognize subnetted addresses. One solution is to add a router running a proxy ARP. In this case, the router acts on behalf of all the hosts installed on the subnet. When it receives an ARP request with a target IP address that matches the address of one of its proteges (141.23.56.21, 141.23.56.22, or 141.23.56.23), it sends an ARP reply and announces its hardware address as the target hardware address. When the router receives the IP packet, it sends the packet to the appropriate host.

ARP: ARP stands for (**Address Resolution Protocol**) it is responsible to find the hardware address of a host from a know IP address there are three basic **ARP** terms.
The important terms associated with **ARP** are:
(i) Reverse ARP

(ii) Proxy ARP

(iii) Inverse ARP

5. **ARP Cache:** After resolving the MAC address, the ARP sends it to the source where it is stored in a table for future reference. The subsequent communications can use the MAC address from the table
6. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
7. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across the destination MAC address or not.
   1. The physical address of the sender.
   2. The IP address of the sender.
   3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.
   4. The IP address of the receiver
8. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

- **CASE-1:** The sender is a host and wants to send a packet to another host on the same network.

- Use ARP to find another host's physical address
- **CASE-2:** The sender is a host and wants to send a packet to another host on another network.
  - The sender looks at its routing table.
  - Find the IP address of the next-hop (router) for this destination.
  - Use ARP to find the router's physical address
- **CASE-3:** the sender is a router and received a datagram destined for a host on another network.
  - The router checks its routing table.
  - Find the IP address of the next router.

Advantages of using ARP

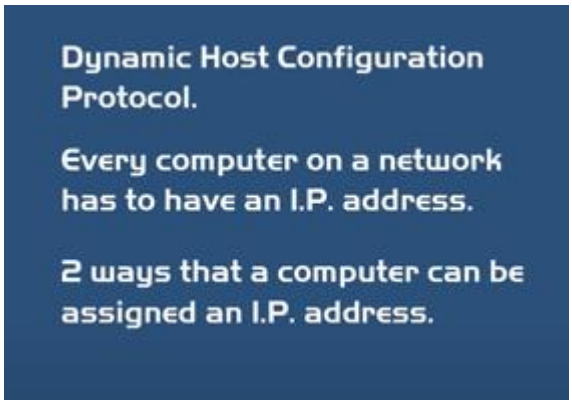
- We can easily find out the MAC address of the device if we know the IP address of that device.
- It is not necessary to configure the address of the end nodes for the MAC address. We can find it when needed.

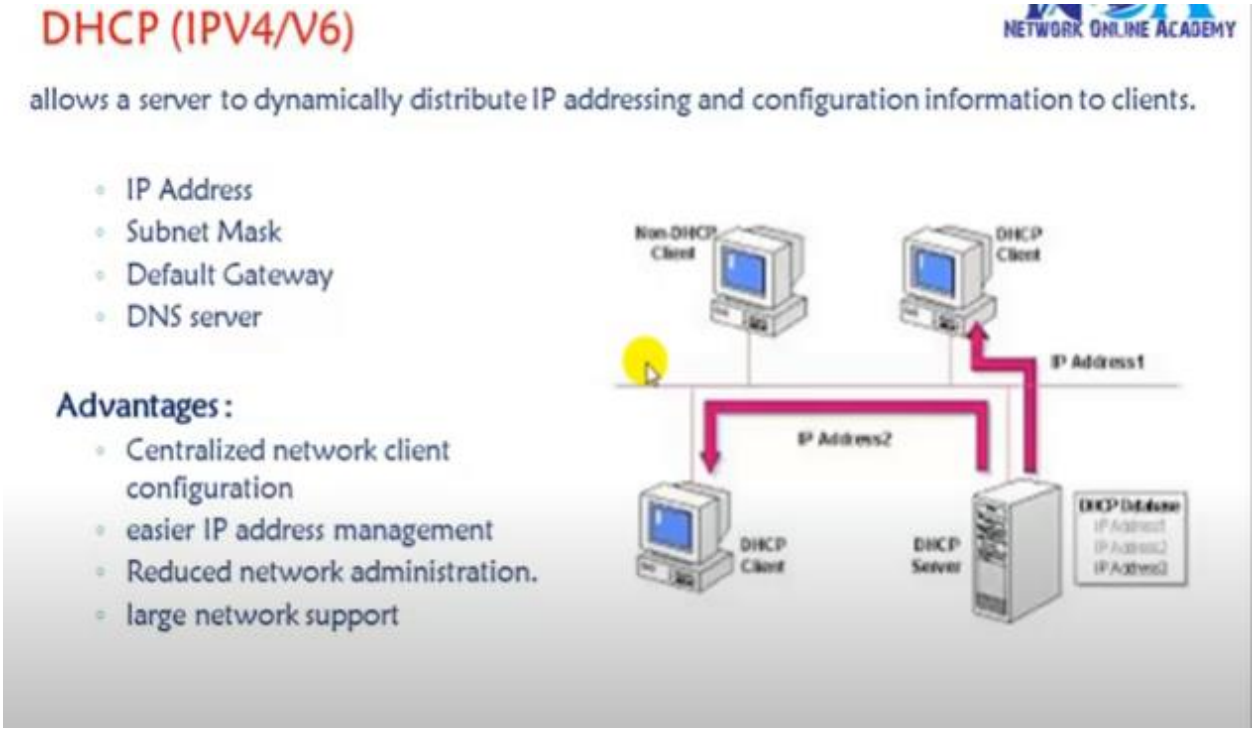
Disadvantages of using ARP

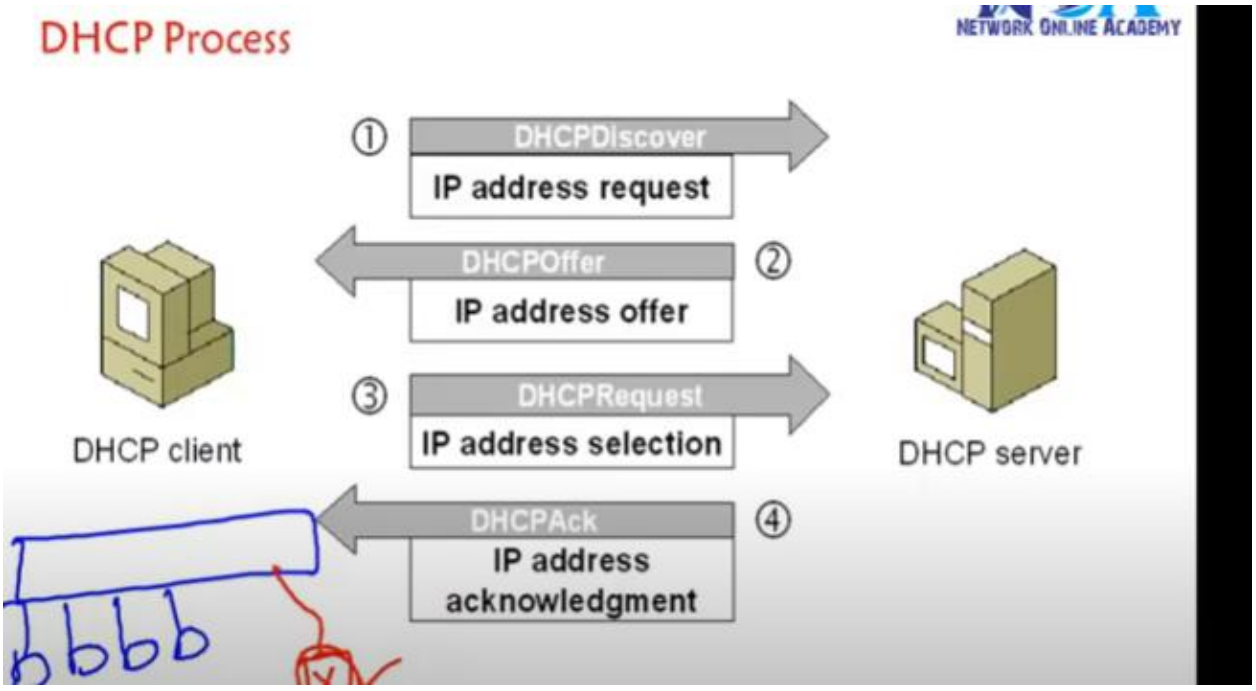
- ARP attacks such as ARP spoofing and ARP denial of service may occur.

RARP

RARP Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.







The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.

- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

DHCP provides static and dynamic address allocation that can be manual or automatic.

Static Address Allocation In this capacity DHCP acts as BOOTP does. It is backwardcompatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.

Dynamic Address Allocation DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

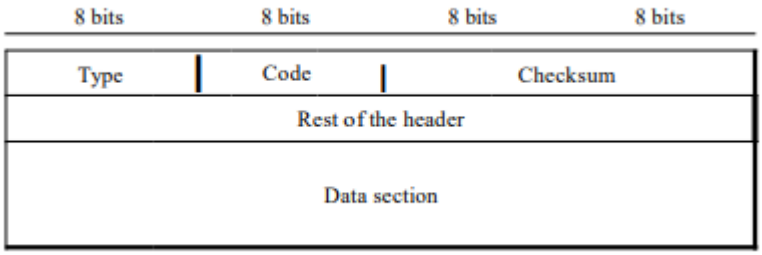
ICMP

The IP protocol has no error-reporting or error-correcting mechanism.

The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protoco1.

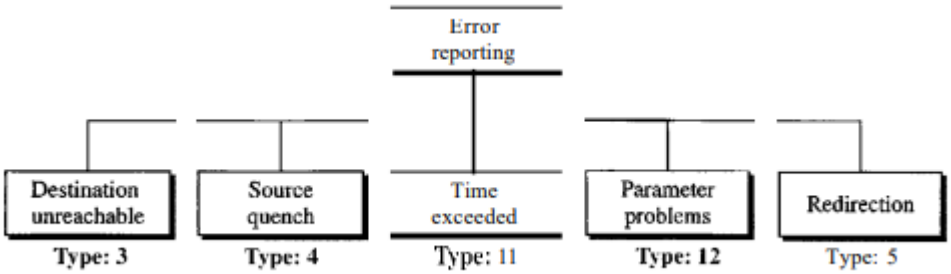
Types of Messages ICMP messages are divided into two broad categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages

Message Format An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all.



Error Reporting One of the main responsibilities of ICMP is to report errors. Although technology has produced increasingly reliable transmission media

ICMP always reports error messages to the original source.



Destination Unreachable

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram

Source Quench

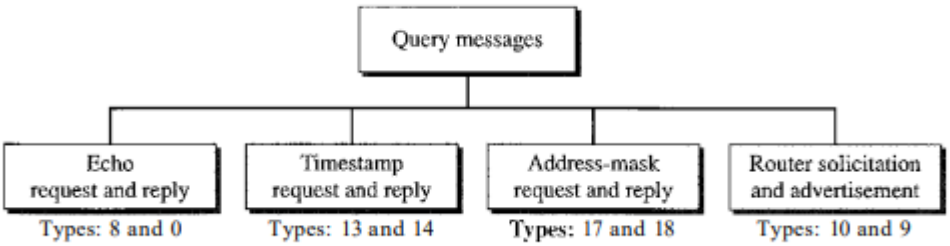
The IP protocol is a connectionless protocol. There is no communication between the source host, which produces the datagram, the routers, which forward it, and the destination host, which processes it.

Time Exceeded The time-exceeded message is generated in two cases: As we see in Chapter 22, routers use routing tables to find the next hop (next router) that must receive the packet

Parameter Problem Any ambiguity in the header part of a datagram can Create serious problems as the datagram travels through the Internet

Redirection When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate route

Query In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages



Link State Routing –

Link state routing is the second family of routing protocols. While distance-vector routers use a

distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Features of link state routing protocols –

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection of information gathered from the link-state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results in the shortest path
- **Routing table –** A list of known paths and interfaces.

Calculation of shortest path –

To find the shortest path, each node needs to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree-like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.
- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats Step 2. and Step 3. until all the nodes are added to the tree

Link State protocols in comparison to Distance Vector protocols have:

8. It requires a large amount of memory.
9. Shortest path computations require many CPU circles.
10. If a network uses little bandwidth; it quickly reacts to topology changes
11. All items in the database must be sent to neighbors to form link-state packets.
12. All neighbors must be trusted in the topology.
13. Authentication mechanisms can be used to avoid undesired adjacency and problems.
14. No split horizon techniques are possible in the link-state routing.

- Open Shortest Path First (OSPF) is a unicast routing protocol developed by a working group of the Internet Engineering Task Force (IETF).
- It is an intradomain routing protocol.
- It is an open-source protocol.

- It is similar to Routing Information Protocol (RIP)
- OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6).
- OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol
- IP datagram that carries the messages from OSPF sets the value of the protocol field to 89
- OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm
- OSPF has two versions – version 1 and version 2. Version 2 is used mostly

OSPF Messages – OSPF is a very complex protocol. It uses five different types of messages. These are as follows:

6. **Hello message (Type 1) –** It is used by the routers to introduce themselves to the other routers.

7. **Database description message (Type 2) –** It is normally sent in response to the Hello message.

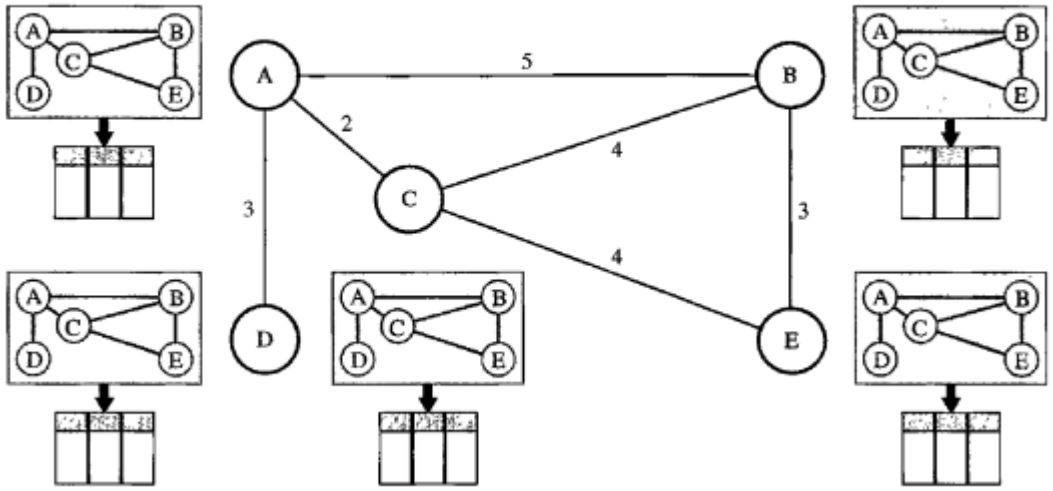
8. **Link-state request message (Type 3) –** It is used by the routers that need information about specific Link-State packets.

9. **Link-state update message (Type 4) –** It is the main OSPF message for building Link-State Database.

10. **Link-state acknowledgement message (Type 5) –** It is used to create reliability in the OSPF protocol.

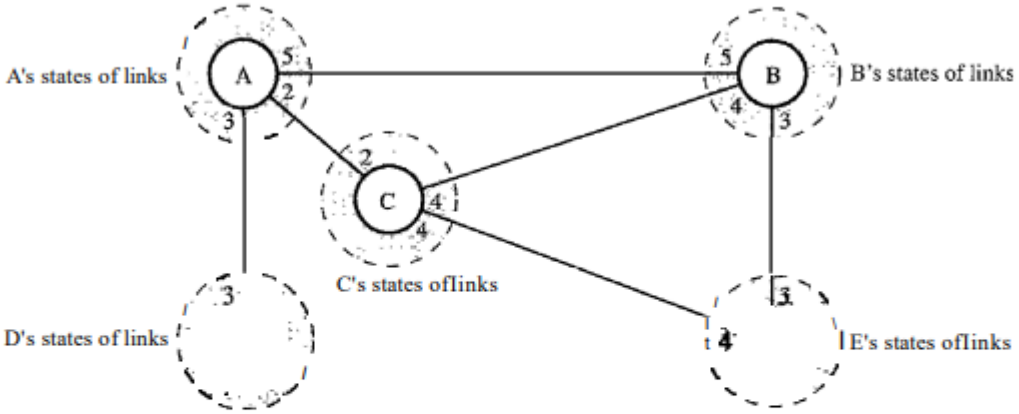
Link State Routing Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domainthe list of nodes and links, how they are connected including the type, cost (metric), and condition of the links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

Figure 22.20 *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.

Figure 22.21 *Link state knowledge*



Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3. Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4. Node D knows that it is connected only to node A with metric 3. And so on. Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

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

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

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

3. Formation of a shortest path tree for each node.

4. Calculation of a routing table based on the shortest path tree. Creation of Link State Packet (LSP) A link state packet can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount

1. When there is a change in the topology ofthe domain. Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology

. 2. On a periodic basis. The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination. It is done to ensure that old information is removed from the domain. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

Figure 22.22 *Dijkstra algorithm*

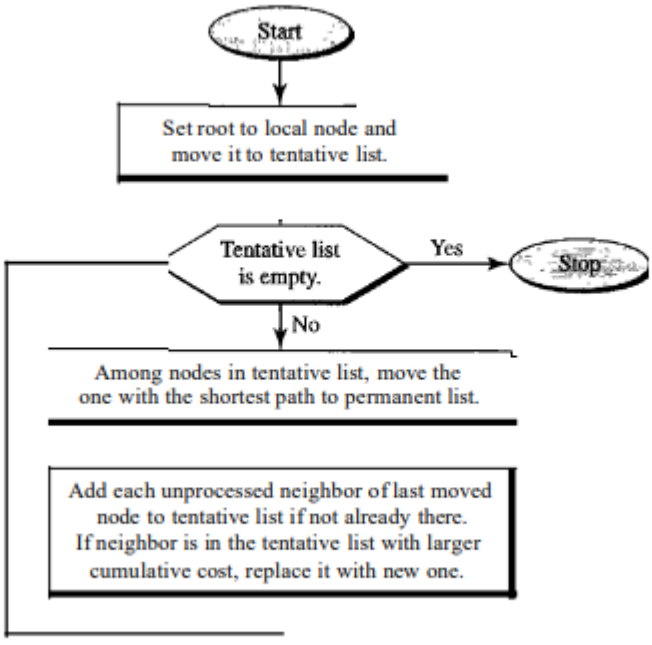


Figure 22.23 *Example of formation of shortest path tree*

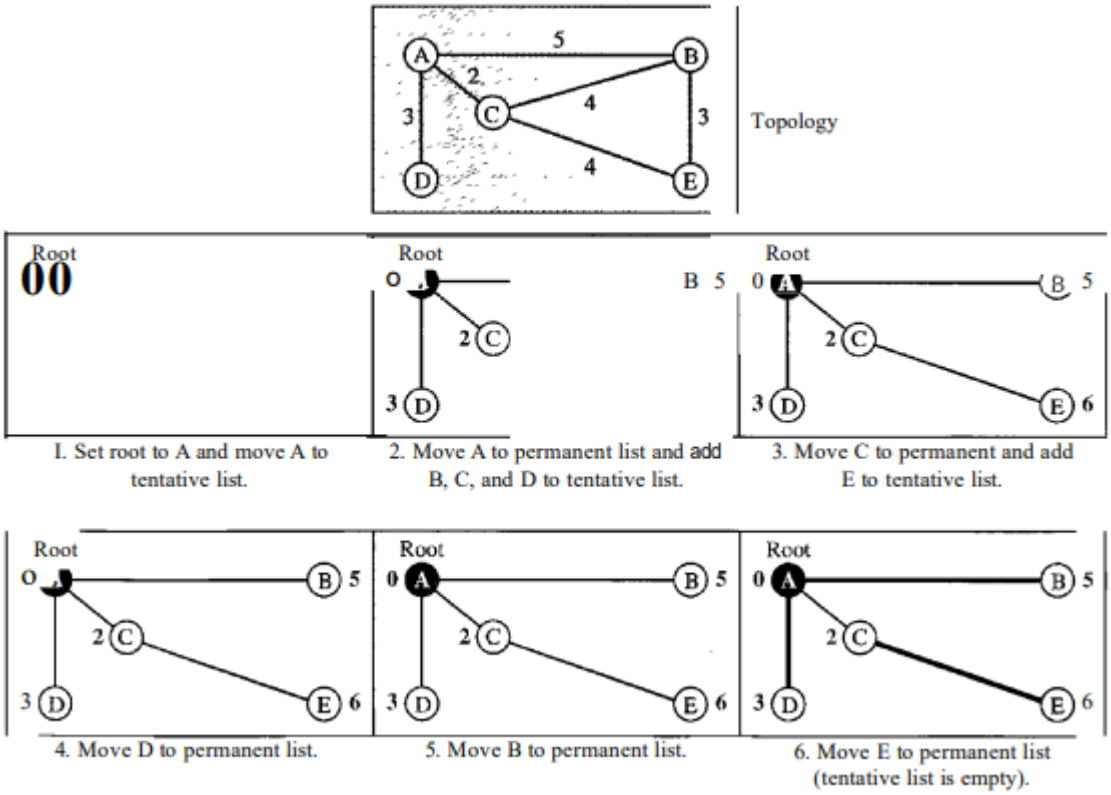


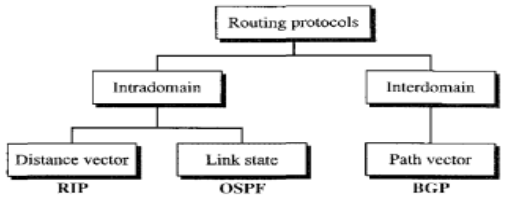
Table 22.2 *Routing table for node A*

Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

Intradomain and interdomain routing protoco

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

Figure 22.13 *Popular routing protocols*



I***ntra-domain routing***

-->routing within an AS(Autonomous System).
-->ignores the internet outside the autonomous system.
-->protocols for intra domain routing are also called **interior gateway** protocols.
-->popular protocols are **RIP** ams **OSPF**.

Inter-domain routing

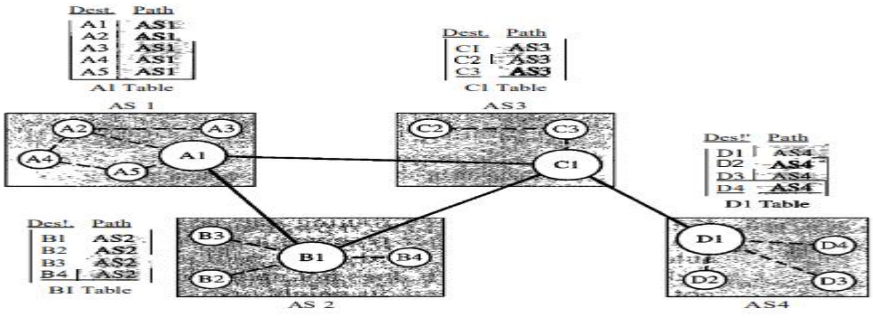
-->routing between AS's.
-->assumes that the internet consists of a collection of interconnected AS's.
-->protocol for inter domain routing are also called **exterior gateway** protocols.
-->routing protocols are **BGP**.

A path vector protocol

I t does not rely on the cost of reaching a given destination to determine whether each path available is loop free or not. Instead, path vector protocols rely on analysis of the path to reach the destination to learn if it is loop free or not

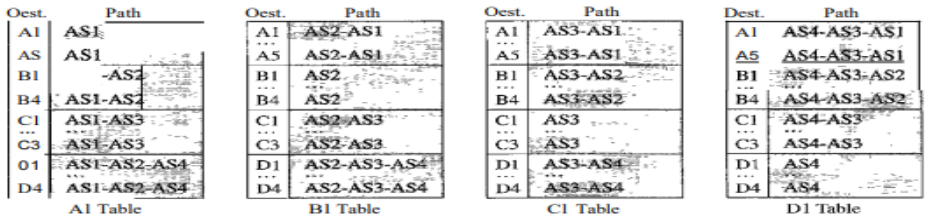
Initialization At the beginning, each speaker node can know only the reachability of nodes inside its autonomous system. Figure 22.30 shows the initial tables for each speaker node in a system made of four ASs.

Figure 22.30 *Initial routing tables in path vector routing*



Loop prevention. The instability of distance vector routing and the creation of loops can be avoided in path vector routing. When a router receives a message, it checks to see if its autonomous system is in the path list to the destination. If it is, looping is involved and the message is ignored.

Figure 22.31 *Stabilized tables for three autonomous systems*



Dest.	Path
A1	AS1
AS	AS1
B1	-AS2
B4	AS1-AS2
C1	AS1-AS3
C3	AS1-AS3
01	AS1-AS2-AS4
D4	AS1-AS2-AS4

A1 Table

Dest.	Path
A1	AS2-AS1
A5	AS2-AS1
B1	AS2
B4	AS2
C1	AS2-AS3
C3	AS2-AS3
D1	AS2-AS3-AS4
D4	AS2-AS3-AS4

B1 Table

Dest.	Path
A1	AS3-AS1
A5	AS3-AS1
B1	AS3-AS2
B4	AS3-AS2
C1	AS3
C3	AS3
D1	AS3-AS4
D4	AS3-AS4

C1 Table

Dest.	Path
A1	AS4-AS3-AS1
A5	AS4-AS3-AS1
B1	AS4-AS3-AS2
B4	AS4-AS3-AS2
C1	AS4-AS3
C3	AS4-AS3
D1	AS4
D4	AS4

D1 Table

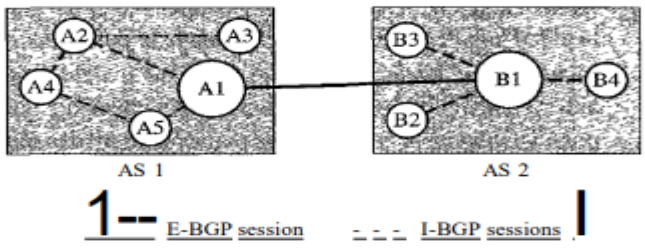
BGP Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.

Types of Autonomous Systems As we said before, the Internet is divided into hierarchical domains called autonomous systems. For example, a large corporation that manages its own network and has full control over it is an autonomous system. A local ISP that provides services to local customers is an autonomous system. We can divide autonomous systems into three categories: stub, multihomed, and transit.

- **Stub** AS. A stub AS has only one connection to another AS. The interdomain data traffic in a stub AS can be either created or terminated in the AS. The hosts in the AS can send data traffic to other ASs. The hosts in the AS can receive data coming from hosts in other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS

- Multihomed AS. A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
- Transit AS. A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

Figure 22.32 *Internal and external BGP sessions*



The session established between AS 1 and AS2 is an E-BOP session. The two speaker routers exchange information they know about networks in the Internet. However, these two routers need to collect information from other routers in the autonomous systems. This is done using I-BOP sessions.

Classless Addressing

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

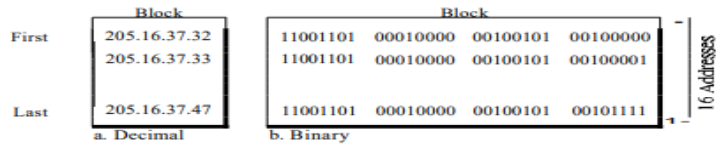
Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).
3. The first address must be evenly divisible by the number of addresses.

Example 19.5

Figure 19.3 shows a block of addresses, in both binary and dotted-decimal notation, granted to a small business that needs 16 addresses.

Figure 19.3 *A block of 16 addresses granted to a small organization*



Mask

A better way to define a block of addresses is to select any address in the block and the mask. As we discussed before, a mask is a 32-bit number in which the *n* leftmost bits

In 1Pv4 addressing, a block of addresses can be defined as
x.y.z.tln
in which x.y.z.t defines one of the addresses and the *In* defines the mask.

First Address The first address in the block can be found by setting the 32 - *n* right-most bits in the binary notation of the address to Os.

The first address in the block can be found by setting the rightmost 32 - *n* bits to Os.

Last Address The last address in the block can be found by setting the 32 - *n* right-most bits in the binary notation of the address to Is.

The last address in the block can be found by setting the rightmost 32 - *n* bits to Is.

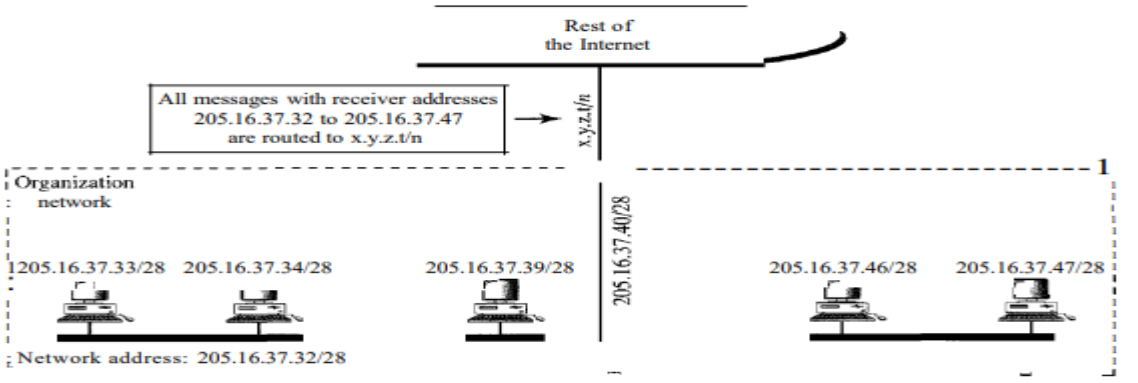
Number of Addresses The number of addresses in the block is the difference between the last and first address. It can easily be found using the formula 2^{32-n}.

The number of addresses in the block can be found by using the formula 2^{32-n}.

Network Addresses

A very important concept in IP addressing is the network address. When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet. The first address in the class, how-

Figure 19.4 *A network configuration for the block 205.16.37.32/28*

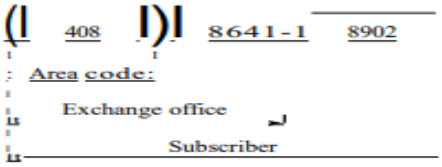


The organization network is connected to the Internet via a router. The router has two addresses. One belongs to the granted block; the other belongs to the network that is at the other side of the router. We call the second address *x.y.z.t/n* because we do not know anything about the network it is connected to at the other side. All messages destined for addresses in the organization block (205.16.37.32 to 205.16.37.47) are sent, directly or indirectly, to *x.y.z.t/n*. We say directly or indirectly because we do not know the structure of the network to which the other side of the router is connected.

Hierarchy

IP addresses, like other addresses or identifiers we encounter these days, have levels of hierarchy. For example, a telephone network in North America has three levels of hier-

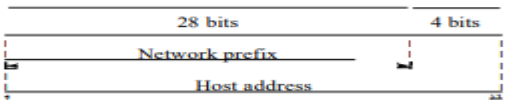
Figure 19.5 *Hierarchy in a telephone network in North America*



Two-Level Hierarchy: No Subnetting

An IP address can define only two levels of hierarchy when not subnetted. The *n* leftmost bits of the address *x.y.z.t/n* define the network (organization network); the 32 - *n*

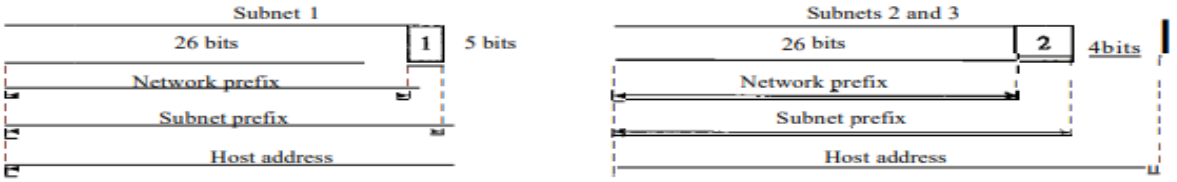
Figure 19.6 *Two levels of hierarchy in an IPv4 address*



The prefix is common to all addresses in the network; the suffix changes from one device to another.

Each address in the block can be considered as a two-level hierarchical structure:
the leftmost *n* bits (prefix) define the network;
the rightmost 32 - *n* bits define the host.

Figure 19.8 *Three-level hierarchy in an IPv4 address*



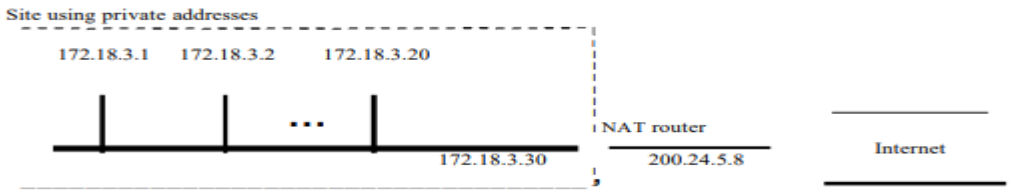
Network Address **Translation** (NAT)

The number of home users and small businesses that want to use the Internet is ever increasing. In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time. An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a

Table 19.3 *Addresses for private networks*

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

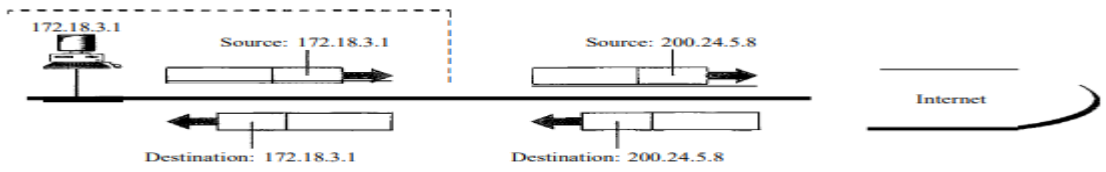
Figure 19.10 *A NAT implementation*



Address Translation

All the outgoing packets go through the NAT router, which replaces the *source address* in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the *destination address* in the packet (the NAT router global address) with the appropriate private address. Figure 19.11 shows an example of address translation.

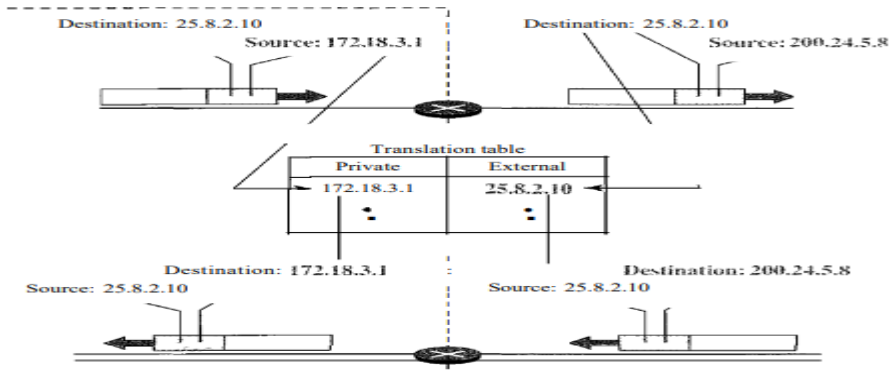
Figure 19.11 *Addresses in a NAT*



Translation Table

The reader may have noticed that translating the source addresses for outgoing packets is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses,

Figure 19.12 *NAT address translation*



25.8.3.2. If the translation table has five columns, instead of two, that include the source and destination port numbers of the transport layer protocol, the ambiguity is eliminated. We discuss port numbers in Chapter 23. Table 19.4 shows an example of such a table.

Table 19.4 *Five-column translation table*

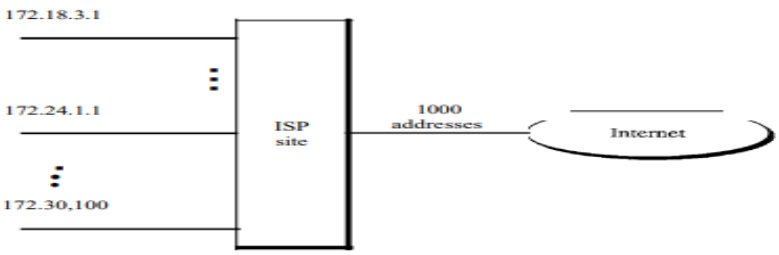
Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

Note that when the response from HTTP comes back, the combination of source address (25.8.3.2) and destination port number (1400) defines the-private network host to which the response should be directed. Note also that for this translation to work, the temporary port numbers (1400 and 1401) must be unique.

NAT and ISP

An ISP that serves dial-up customers can use NAT technology to conserve addresses. For example, suppose an ISP is granted 1000 addresses, but has 100,000 customers. Each of the customers is assigned a private network address. The ISP translates each of the 100,000 source addresses in outgoing packets to one of the 1000 global addresses; it translates the global destination address in incoming packets to the corresponding private address. Figure 19.13 shows this concept.

Figure 19.13 *An ISP and NAT*



S.NO	Subnetting	Supernetting
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in supernetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.