Packet Switching

Unit-III

Lecture -2

Session Objectives

- To discuss about packet switching
- To study the datagram approach and the virtual-circuit approach

Session Outcomes

At the end of this session, participants will be able to

- Discuss packet switching

Agenda

Packet Switching

- Packet-switched network can use two different approaches to route the packets: the datagram approach and the virtual circuit approach

Datagram Approach: Connectionless Service

- The packets in a message may or may not travel the same path to their destination.
- Each packet travelling an independent entity; there is no relationship between packets belonging to the same message.
- The switches in this type of network are called routers.
- A packet belonging to a message may be followed by a packet belonging to the same message or to a different message from the same or from a different source.
- Packet is routed based on the information contained in its header

Connectionless packet-switching

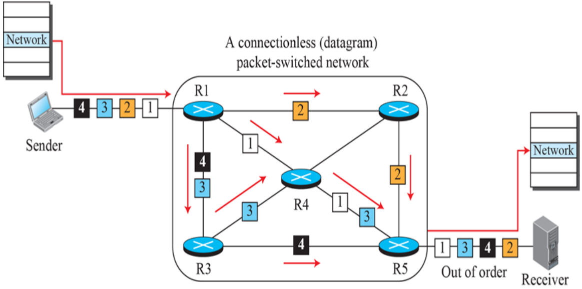


Figure: A connectionless packet-switched network

- Routes the packet based only on the destination address.
- Source address may be used to send an error message to the source if the packet is discarded

Forwarding process

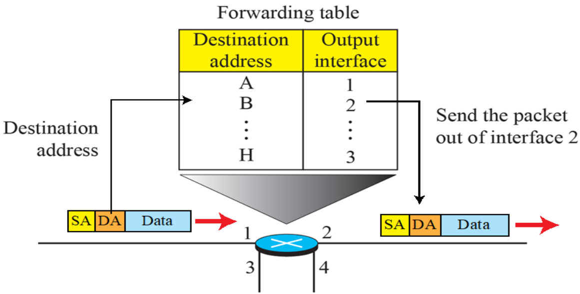


Figure: Forwarding process in a router when used in a connectionless network

Virtual-Circuit Approach: Connection-Oriented Service

- There is a relationship between all packets belonging to a message
- After connection setup, the datagrams can all follow the same path
- Packet has the source and destination addresses, also contain a **flow label, a virtual circuit identifier** that defines the virtual path the packet should follow

Virtual-circuit

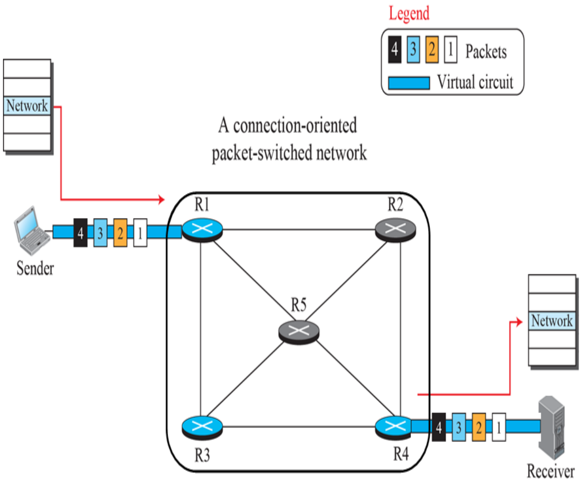


Figure: A virtual-circuit packet-switched network

Forwarding process

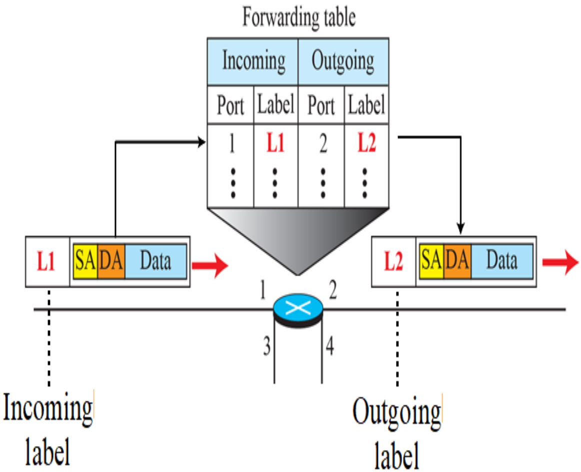
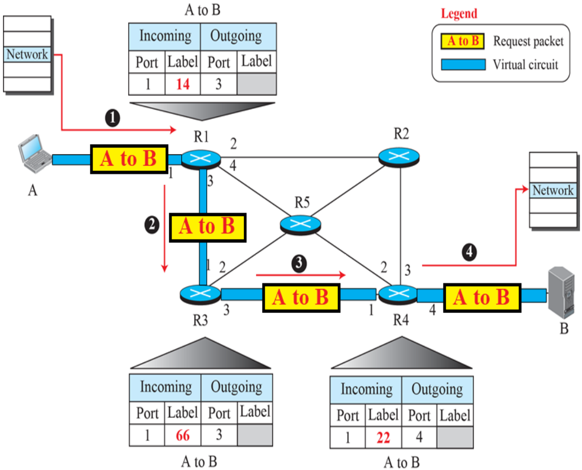


Figure: Forwarding process in a router when used in a virtual-circuit network

Setup Phase

- A router creates an entry for a virtual circuit
- Two auxiliary packets exchanged between the sender and the receiver: the request packet and the acknowledgement



Request packet

1. Source A sends a request packet to router R1.
2. Router R1 receives the request packet
   — knows that a packet from A to B **goes out through port 3**
   — **creates an entry** in its table for this virtual circuit,
   — **fill three of the four columns**
   assigns the incoming port (1)
   — chooses an available incoming label (14)
   the outgoing port (3)
   — does not yet know the outgoing label, done during the acknowledgement step
   — forwards the packet through port 3 to router R3.

Request packet

1. Router R3 receives the setup request packet. The same events happen here as at router R1;
2. Router R4 receives the setup request packet. Again, three columns are completed: incoming port (1), incoming label (22), and outgoing port (4).
3. Destination B receives the setup packet,
   — if it is ready to receive packets from A, it assigns a label to the incoming packets that come from A, in this case 77
   — This label lets the destination know that the packets come from A, and not from other sources.

Acknowledgment Packet

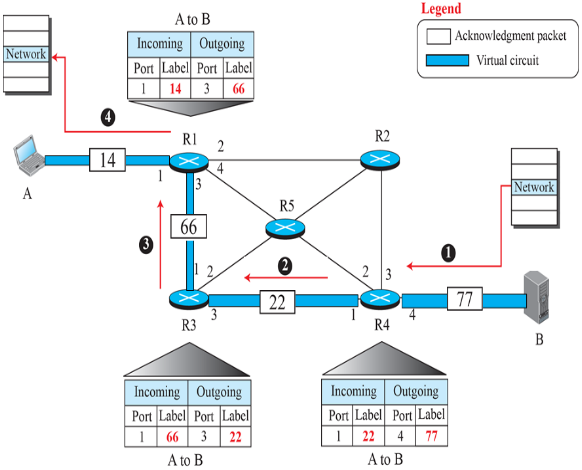
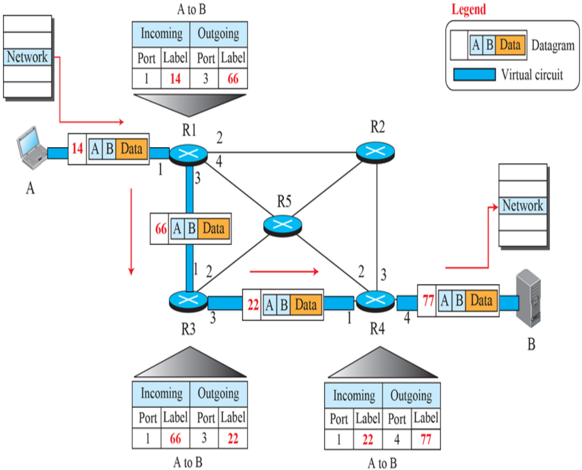


Figure: Sending acknowledgments in a virtual-circuit network

Data-Transfer Phase

- After all routers have created their forwarding table for a specific virtual circuit, the network-layer packets belonging to one message can be sent one after another.



Teardown Phase

- source A, after sending all packets to B, sends a special packet called a teardown packet.
- Destination B responds with a confirmation packet. All routers delete the corresponding entries from their tables.

Presentation Outline

NETWORK-LAYER PERFORMANCE

Performance is measured in terms of delay, throughput, and packet loss.

- Transmission Delay:
  $Delay_{tr}$ = **(Packet length) / (Transmission rate).**
- Propagation Delay:
  $Delay_{pg}$ = **(Distance) / (Propagation speed).**
- Processing Delay:
  $Delay_{pr}$ = **Time required to process a packet in a router or a destination host**
- Queuing Delay:
  $Delay_{qu}$ = **The time a packet waits in input and output queues in a router**

Total delay =
$(n+1)(Delay_{tr} + Delay_{pg} + Delay_{pr}) + (n)(Delay_{qu})$

Throughput

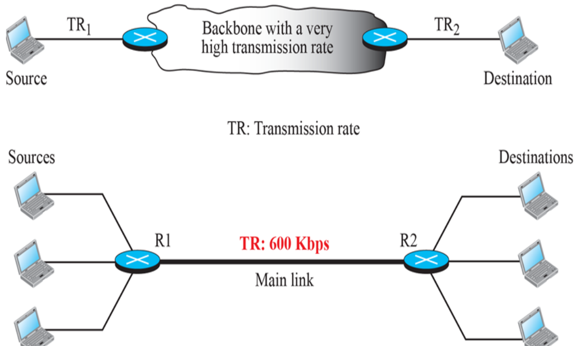
- The number of bits passing through the point in a second, which is actually the transmission rate of data at that point
- **Throughput = minimum (** TR_1**,** TR_2**, . . .** TR_n**)**

TR: Transmission rate

a. A path through three links

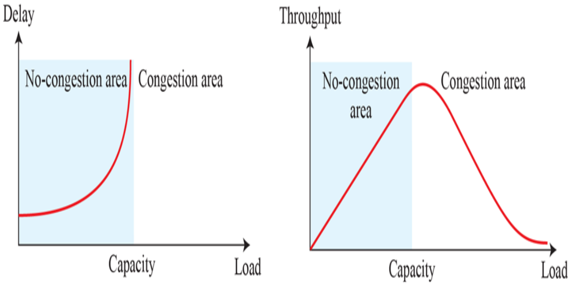
Throughput

- Internet backbone has a very high transmission rate, in the range of gigabits per second.
- The throughput is as minimum transmission rate of the two access links that connect the S and D.
- Router may collect the flow from several sources or distribute the flow between several sources



Congestion Control

- Congestion at the network layer is related to throughput and delay can be measured as functions of load.
- when the load reaches the network capacity, the delay increases sharply — becomes infinite when the load ¿ capacity
- Throughput declines sharply —the discarding of packets by the routers.



a. Delay as a function of load

b. Throughput as a function of load

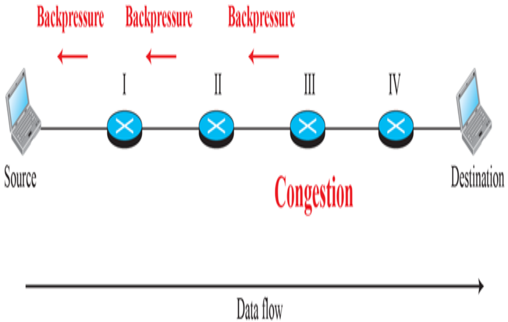
Congestion control mechanisms

Open-loop congestion control (prevention) :

- **Retransmission Policy:** may increase congestion —retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.
- **Window Policy:** Go-Back-N window, when the timer for a packet times out, several packets may be resent. The Selective Repeat window, sends the specific packets that have been lost or corrupted
- **Acknowledgement Policy:** Sending fewer acknowledgements means imposing less load
- **Discarding Policy:** the quality of msg is still preserved and congestion is prevented or alleviated.
- **Admission Policy:** Switches in a flow first check the resource requirement of a flow before admitting it to the network.

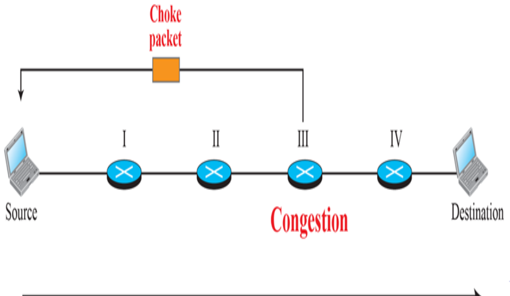
Closed-Loop Congestion Control

- **Backpressure:** refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes
- A node to node congestion control that starts with a node and propagates in the opposite direction towards source
- Can only be implemented in **virtual-circuit** — **cannot** be implemented in a **datagram** network



Closed-Loop Congestion Control: Choke Packet

- A packet sent by a node to the source to inform it of congestion.
- Backpressure: the warning is from one node to its upstream node;choke-packet method, the warning is from the router, which has encountered congestion, directly to the source station
- Intermediate nodes through which the packet has traveled are not warned



Closed-Loop Congestion Control

- **Implicit Signaling:** there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.
- **Explicit Signaling:**
- Choke-packet method, a separate packet is used for this purpose; in the explicit-signaling method, the **signal is included in the packets that carry data.**
- Explicit signaling can occur in either the forward or the backward direction

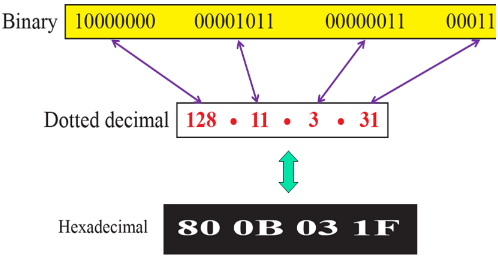
Presentation Outline

IPV4 ADDRESSES

- **Internet address or IP address:** Identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet
- **32-bit address** that uniquely and universally defines the connection of a host or a router to the Internet.
- IP address is the **address of the connection**, not the host or the router, because if the device is moved to another network, the IP address may be changed.
- If a **device has two connections** to the Internet, via two networks, it has **two IPv4 addresses**
- **Address Space:** the total number of addresses used by the protocol; the address space is 2^{32} or 4,294,967,296; **more than 4 billion devices** could be connected to the Internet.

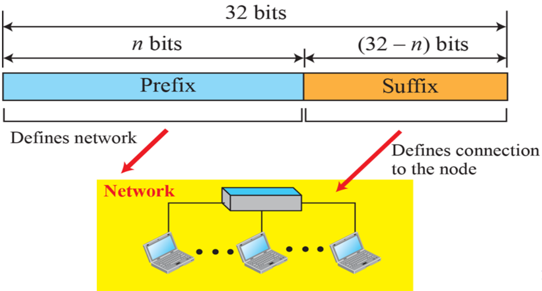
Notation

- Three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).



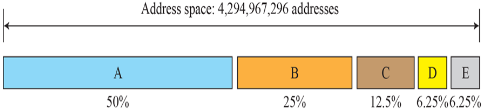
Hierarchy in Addressing

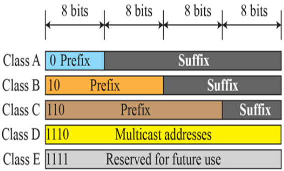
- 32-bit IPv4 address is hierarchical, divided only into two parts.
- The first part called the **prefix**, **defines the network**; the second part called the **suffix, defines the node** (connection of a device to the Internet).
- a fixed-length prefix: **classful addressing.**
- a variable-length network prefix : referred to as **classless addressing**



Classful Addressing

- Three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24).
- The whole address space was divided into five classes (class A, B, C, D, and E),





Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Address Depletion

- The reason that **classful addressing** has become **obsolete** is **address depletion**.
- Addresses were not distributed properly; the addresses being rapidly used up
- class A can be assigned to only 128 organizations in the world, but each organization needs to have a single network with 16,777,216 nodes
- Class B addresses were designed for midsize organizations
- Class C :number of addresses that can be used in each network (256) was so small
- Class E addresses were almost never used, wasting the whole class.

Subnetting and Supernetting

- A class A or class B block is divided into several subnets.
- Each subnet has a larger prefix length than the original network.
- if a network in class A is divided into four subnets, each subnet has a prefix of $nsub = 10$.
- If all of the addresses in a network are not used, subnetting divides the addresses among several organizations.
- While subnetting was devised to divide a **large block into smaller ones**, supernetting was devised to **combine several class C blocks into a larger block** to be attractive to organizations that need more than the 256 addresses available in a class C block

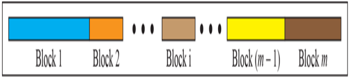
Advantage of Classful Addressing

- Classful addressing had several problems and became obsolete
- Given an address, we can easily find the class of the address and,
- since the prefix length for each class is fixed, we can find the prefix length immediately.
- Prefix length in classful addressing is inherent in the address; no extra information is needed to extract the prefix and the suffix.

Classless Addressing

- larger address : a long-term solution — increase the length of IP addresses : IPv6
- Short-term solution : classless addressing — the class privilege was removed from the distribution to compensate for the address depletion.
- In classless addressing, variable-length blocks are used that belong to no classes
- Can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on
- the whole address space is divided into variable length blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- Restriction: number of addresses in a block needs to be a power of 2.

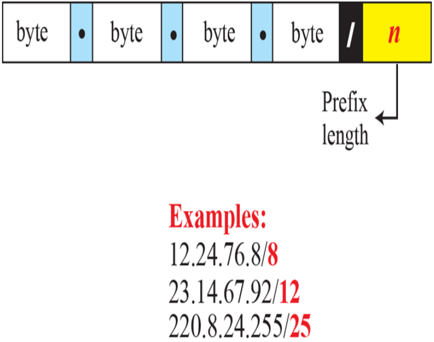
- The prefix length in classless addressing is variable.
- A prefix length that ranges from 0 to 32.
- The size of the network is inversely proportional to the length of the prefix.
- A small prefix means a larger network; a large prefix means a smaller network.



Address space

Prefix Length: Slash Notation

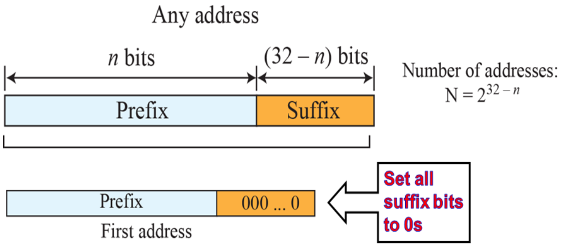
- How to find the prefix length if an address is given.
- We need to separately give the length of the prefix, separated by a slash: slash notation and formally as **classless interdomain routing or CIDR** strategy.
-
-



Extracting Information from an Address

To know three pieces of information about the **block to which the address belongs: the number of addresses, the first address in the block, and the last address.**

1. The number of addresses in the block is found as $N = 2^{32-n}$.
2. To find the first address, we keep the n leftmost bits and set the *(32 - n)* rightmost bits all to 0s.
3. To find the last address, we keep the *n* leftmost bits and set the *(32 - n)* rightmost bits all to 1s.



A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is $2^{32-n} = 25 = 32$ addresses. The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01010010
First address: 167.199.170.64/27	10100111	11000111	10101010	01000000

Address: 167.199.170.82/27	10100111	11000111	10101010	01011111
Last address: 167.199.170.95/27	10100111	11000111	10101010	01011111

Address Mask

- Address mask is a 32-bit number in which the **n** leftmost bits are set to **1s** and the rest of the bits **(32 - n)** are set to **0s.**
- The A computer can easily find the address mask because it is the complement of $(2^{32-n} - 1)$.

1. The number of addresses in the block N = NOT (mask) + 1.
2. The first address in the block = (Any address in the block) AND (mask).
3. The last address in the block = (Any address in the block) OR [(NOT (mask)].

Example

We repeat previous example using the mask. The mask in dotted-decimal notation is 256.256.256.224

Number of addresses in the block:	N = NOT (mask) + 1 = 0.0.0.31 + 1 = 32 addresses
First address:	First = (address) AND (mask) = 167.199.170.82
Last address:	Last = (address) OR (NOT mask) = 167.199.170.255

Example

In classless addressing, an address cannot per se define the block the address belongs to. For example, the address 230.8.24.56 can belong to many blocks. Some of them are shown below with the value of the prefix associated with that block.

Prefix length:16	→	Block:	230.8.0.0	to	230.8.255.255
Prefix length:20	→	Block:	230.8.16.0	to	230.8.31.255
Prefix length:26	→	Block:	230.8.24.0	to	230.8.24.63
Prefix length:27	→	Block:	230.8.24.32	to	230.8.24.63
Prefix length:29	→	Block:	230.8.24.56	to	230.8.24.63
Prefix length:31	→	Block:	230.8.24.56	to	230.8.24.57

Network Address

- The **first address, the network address**, is particularly important because it is used in routing a packet to its destination network.
- When a packet arrives at the router from any source host, the **router needs to know to which network the packet should be sent**: from which interface the packet should be sent out.
- After the network address has been found, the router consults its forwarding table to find the corresponding interface from which the packet should be sent out.
- The **network address is actually the identifier of the network**

Block Allocation

How are the blocks allocated?

- Block allocation is given to a global authority— Internet Corporation for Assigned Names and Numbers (ICANN)
- It assigns a large block of addresses to an ISP
- Two restrictions need to be applied to the allocated block

1. The number of requested addresses, N, = a power of 2. because, $N = 2^{32-n}$ or $n = 32 - log_2 N$. If N is not a power of 2, we cannot have an integer value for n.
2. The requested block needs to be allocated where there is an adequate number of contiguous addresses available in the address space.

However, there is a restriction on choosing the first address in the block.

- The **first address needs to be divisible by the number of addresses** in the block. The reason is that the first address needs to be the prefix followed by (32 - n) number of 0s.
- The decimal value of the first address is then **first address = (prefix in decimal) x** 2^{32-n}**= (prefix in decimal) x N.**

Example

Problem: An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

Solution:

There are $2^{32-24} = 256$ addresses in this block. The first address is 14.24.74.0/24; the last address is 14.24.74.255/24. To satisfy the third requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one.

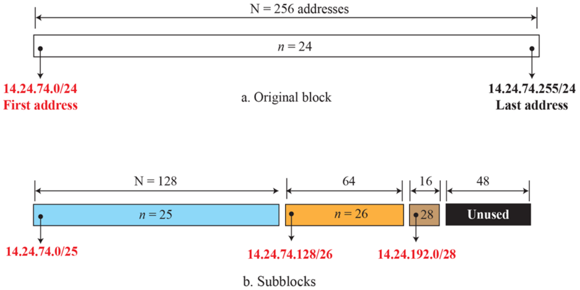
Example

a. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - log_2 128 = 25$. The first address in this block is 14.24.74.0/25; the last address is 14.24.74.127/25.

b. The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - log_2 64 = 26$. The first address in this block is 14.24.74.128/26; the last address is 14.24.74.191/26.

Example

c. The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2 either. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_3 = 32 - log_2 16 = 28$. The first address in this block is 14.24.74.192/28; the last address is 14.24.74.207/28.
Total addresses in the previous subblocks= 208 addresses,−− > 48 addresses are left in reserve. The first address and last address 14.24.74.208 , 14.24.74.255



Address Aggregation

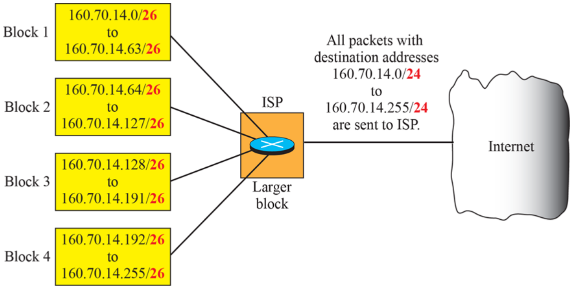
Advantages of the CIDR strategy:

- Address summarization or route summarization:
- When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block.
- ICANN assigns a large block of addresses to an ISP.
- Each ISP in turn divides its assigned block into smaller subblocks and grants the subblocks to its customers

Example of address aggregation

- Four small blocks of addresses are assigned to four organizations by an ISP.
- The ISP combines these four blocks into one single block and advertises the larger block to the rest of the world.
- Any packet destined for this larger block should be sent to this ISP.
- It is the responsibility of the ISP to forward the packet to the appropriate organization.
- This is similar to routing we can find in a postal network.

Example of address aggregation



Special Addresses

five special addresses that are used for special purposes: this-host address, limited-broadcast address, loopback address, private addresses, and multicast addresses.

- **This-host Address**:
  The only address in the block 0.0.0.0/32 is called the this-host address.
- It is used whenever a **host** needs to send an IP datagram but it **does not know its own address** to use as the source address.
- **Limited-broadcast Address**:
  The only address in the block 255.255.255.255/32 is called the limited-broadcast address.
- Used whenever **a router or a host needs to send a datagram to all devices in a network.** The routers in the network, however, block the packet having this address as the destination; the packet cannot travel outside the

Special Addresses

- **Loopback Address**: The block 127.0.0.0/8 is called the loopback address.
- A packet with one of the addresses in this block as the destination address never leaves the host;
- it will remain in the host.
- **Private Addresses**: Four blocks are assigned as private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 169.254.0.0/16.

Presentation Outline

DHCP

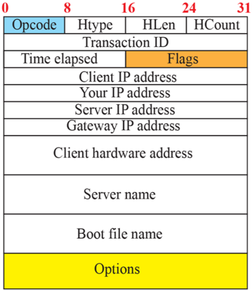
- Address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP).
- DHCP is an application-layer program, using the client-server paradigm, that actually helps TCP/IP at the network layer.
- called a plugand- play protocol
- A network manager can configure DHCP to assign **permanent IP addresses** to the host and routers.
- DHCP can also be configured to provide **temporary, on demand,** IP addresses to hosts

DHCP

- In addition to its IP address, a computer also needs to know the network prefix
- In other words, four pieces of information are normally needed: **the computer address, the prefix, the address of a router, and the IP address of a name server**.
- DHCP can be used to provide these pieces of information to the host

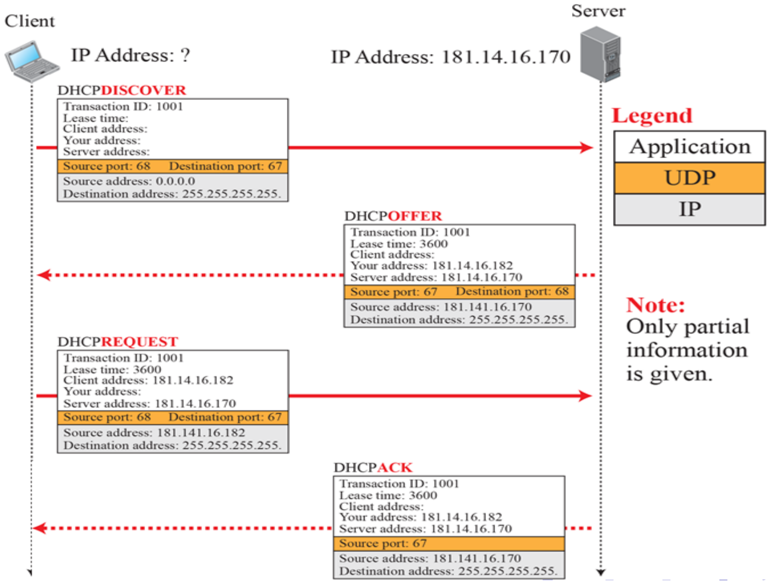
DHCP Message Format

DHCP is a client-server protocol



Fields:
Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Lengh of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by client and repeated by the server
Time elapsed: The number of seconds since the client started to boot
Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used
Client IP address: Set to 0 if the client does not know it
Your IP address: The client IP address sent by the server
Server IP address: A broadcast IP address if client does not know it
Gateway IP address: The address of default router
Server name: A 64-byte domain name of the server
Boot file name: A 128-byte file name holding extra information
Options: A 64-byte field with dual purpose described in text

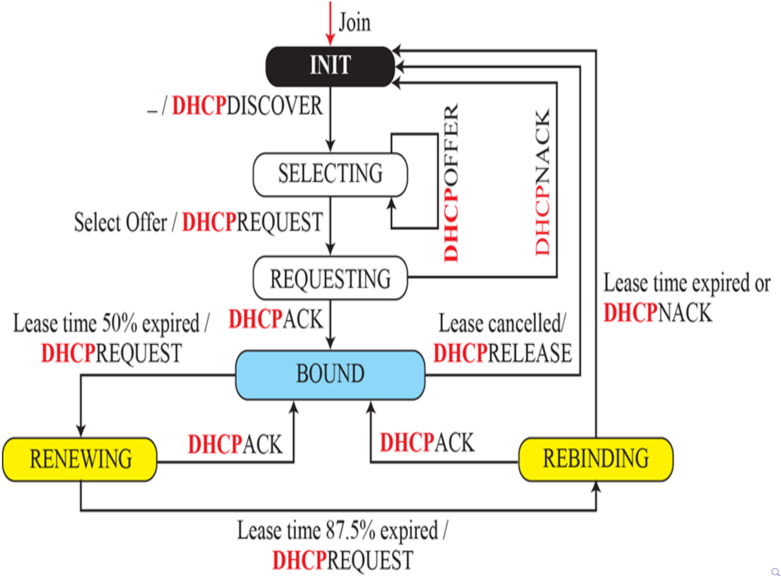
Operation of DHCP



Operation of DHCP

- In the DHCPACK message, the **server defines the pathname of a file** in which the client can find complete information such as the address of the DNS server.
- The client can then **use a file transfer protocol** to obtain the rest of the needed information
- **Error control:** DHCP uses the service of UDP, which is not reliable.
- To provide error control, DHCP uses two strategies. First, DHCP requires that UDP use the checksum.
- Second, the DHCP client uses timers and a retransmission policy if it does not receive the DHCP reply to a request.

Operation of DHCP



Timers

- This procedure requires that the client uses 3 timers: **renewal timer** (set to 50 percent of the lease time), **rebinding timer** (set to 75 percent of the lease time), and **expiration timer** (set to the lease time).

Network Address Resolution (NAT)

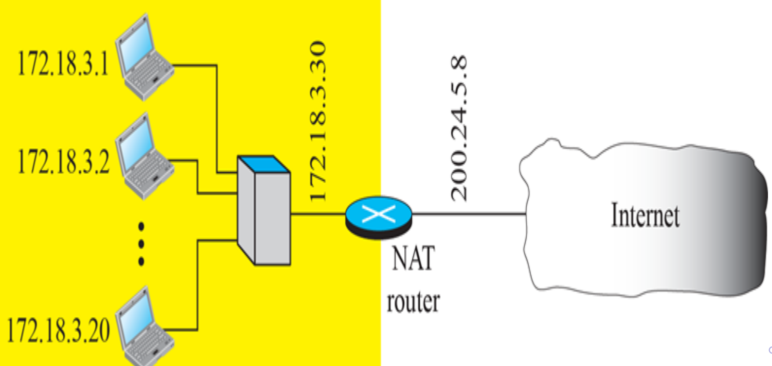
- The distribution of addresses through ISPs has created a new problem.
- Assume that an ISP has granted a small range of addresses to a small business or a household.
- If the business grows or the household needs a larger range, the ISP may not be able to grant the demand because the addresses before and after the range may have already been allocated to other networks.
- Only a portion of computers in a small network need access to the Internet simultaneously.
- This means that the number of allocated addresses does not have to match the number of computers in the network

Network Address Translation (NAT)

- A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks, is Network Address Translation (NAT).
- The technology allows a site to **use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world**.
- The site must have only one connection to the global Internet through a NAT-capable router that runs NAT software.

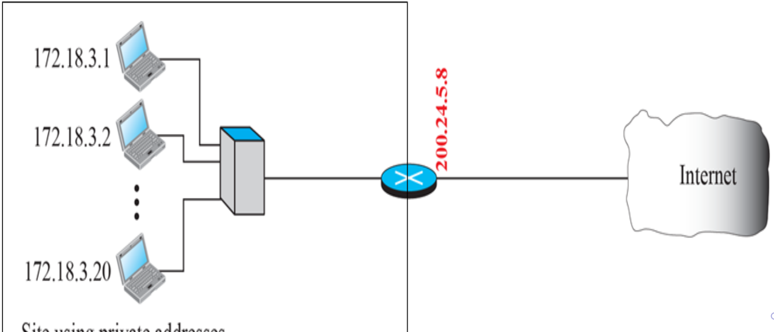
NAT

- The private network uses private addresses.
- The router that connects the network to the global address uses one private address and one global address.
- The private network is invisible to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

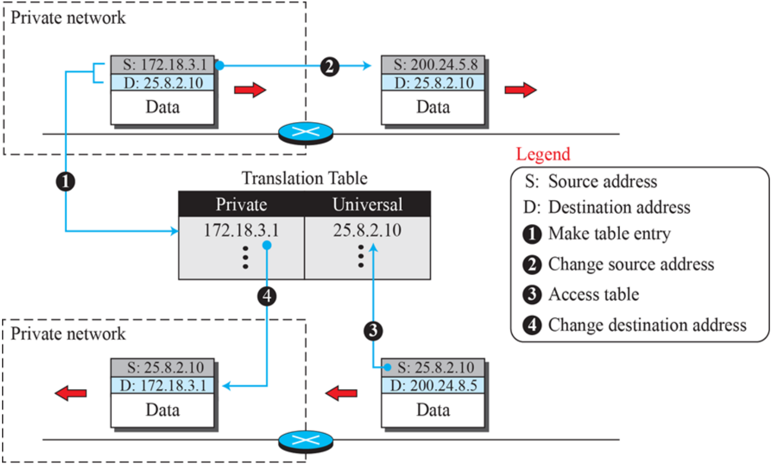


Address Translation

- All of 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.



Translation Table



IP Addresses and Port Addresses inTranslation Table

To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the 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
⋮	⋮	⋮	⋮	⋮

Summary

- The main services provided by the network layer are packetizing and routing the packet from the source to the destination
- Two approaches to packet switching: datagram approach and virtual-circuit approach.
- Performance of the network layer is measured in terms of delay, throughput, and packet loss
- Discussed addressing in IPv4
- Some problems of address shortage in the current version can be temporarily alleviated using DHCP and NAT protocols

Test your Understanding

1. Distinguish between the process of routing a packet from the source to the destination and the process of forwarding a packet at each router
2. If a label in a connection-oriented service is 8 bits, how many virtual circuits can be established at the same time?
3. List four types of delays in a packet-switched network
4. In classless addressing, can two different blocks have the same prefix length?
5. Find the class of the following classful IP addresses: a. 130.34.54.12 b. 200.34.2.1 c. 245.34.2.8

Test your Understanding

1. In classless addressing, what is the size of the block (N) if the value of the prefix length (n) is one of the following? a. $n = 0$ b. $n = 14$ c. $n = 32$
2. In classless addressing, what is the value of the prefix length (n) if the size of the block (N) is one of the following? a. $N = 1$ b. $N = 1024$ c. $N = 232$