Chapter 19

Network Layer: Logical Addressing

19-1 IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

Topics discussed in this section:

Address Space
Notations
Classful Addressing
Classless Addressing
Network Address Translation (NAT)

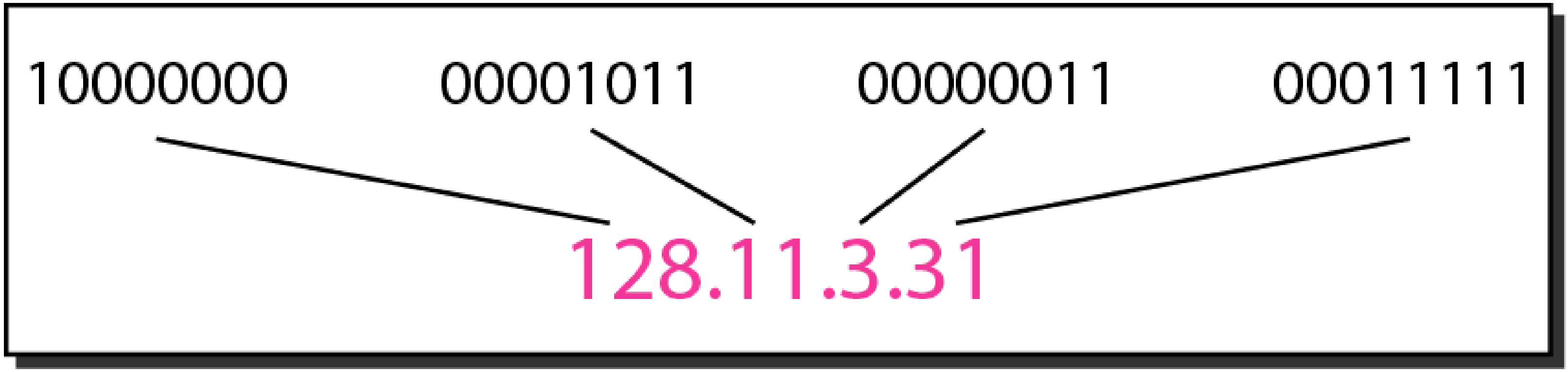
IPV4 Address

- An IPv4 address is 32 bits long.
- The IPv4 addresses are unique and universal.
- The address space of IPv4 is 2^{32} or 4,294,967,296

IPV4 Address

Notation

- **Binary Notation :**
  - The IPV4 address is displayed as 32 bits.
  - Each octet is often referred to as a byte.
- **Dotted-Decimal Notation**
  - To make the IPV4 address more compact and easier to read, Internet addresses are written in decimal form with a decimal point (dot) separating the byte.



Notation (cont'd)

- Hexadecimal Notation

0111 0101   1001 0101   0001 1101   1110 1010

75   95   1D   EA

0x75951DEA

- 8 hexadecimal digits

- Used in network programming

Classful Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.
  - If the address is given in binary notation, the first few bits can tell us the class of the address.
  - If the address is given in decimal-dotted notation, the first byte defines the class.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

128
64
32
16
16

b. Dotted-decimal notation

Classful Addressing

Classful Addresses

- Unicast Communication - A, B, C Class

  (~must be delivered to specific computer)
- Multicast Communication – D Class

  (~must be delivered to each member of the group)
- For reserve – E Class

Classful Addressing

Classes and blocks

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.

Table 19.1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Classful Addressing

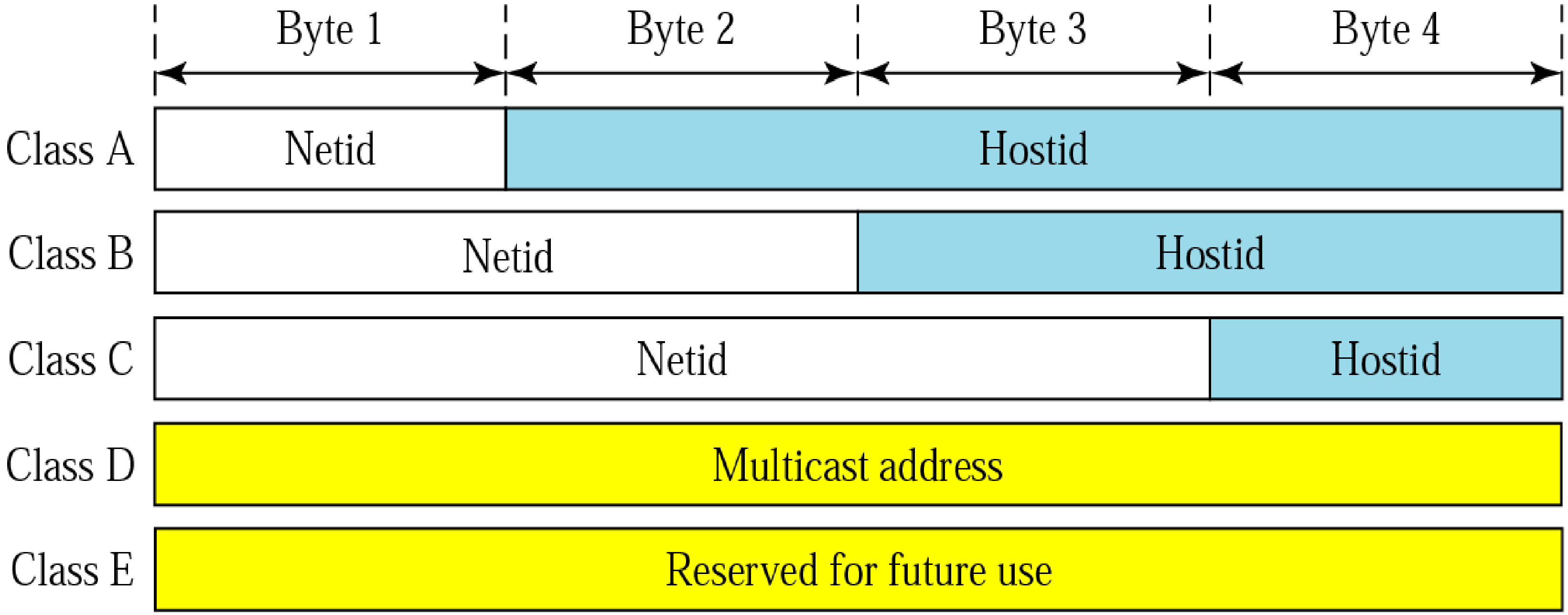
- Class A addresses were designed for large organizations
  - The most of the addresses were wasted and were not used.
- Class B addresses were designed for midsize organizations
  - Class B is also too large for many organizations.
- Class C addresses were designed for small organizations
  - Class C is too small for many organizations.
- Class D addresses were designed for multicasting
  - Each addresses in this class is used to define one group of hosts on the Internet.
- Class E addresses were reserved for future use.
  - Only a few used, resulting in another waste of addresses.

In classful addressing, a large part of the available addresses were wasted.

Classful Addressing

Netid and Hostid

- IP address in class A,B, or C is divided into netID and hostID.
  - netID defines a Network, and hostID defines a host in the networks.



MASK

- **Mask**

  - **When a router receives a packet with a destination address, it needs to route the packet.**
  - **The routing is based on the network address and subnetwork address.**
    - **The router outside the organization has a routing table with one column based on the network addresses;**
    - **The router inside the organization has a routing table based on the subnetwork addresses.**
  - **The mask is a 32-bit binary number, and the mask can help to find the network and subnetwork address.**
    - **The routers outside the organization use a Default Mask to find the network address and,**
    - **The routers inside the organization use a Subnet Mask to find the subnetwork address..**

Default Mask

Default Mask

- A default mask is a 32-bit binary number, and the default mask for each class are as follows; 255.0.0.0, 255.255.0.0, 255.255.255.0.
- Default mask gives the network address when ANDed with an address in the block.
  - If the bit in the mask is 1, the corresponding bit in the address is retained in the output (no change)
  - If the mask is 0, a 0 bit in the output is the result.

Table 19.1 Default masks

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

CIDR (Classless Inter-domain Routing)

Subnet Mask

Subnetting

- A network is divided into several smaller networks with each subnetwork (or subnet) having its subnetwork address

Subnet Mask :

- We change some of the leftmost 0s in the default mask to make a subnet mask.
- The number of subnets is determined by the number of extra 1s.
  - If the number of extra 1s in n, the number of subnets is 2^n.
  - If the number of subnets is N, the number of extra 1s is $\log_2 N$.

255.255.0.0

Default Mask	11111111	11111111	00000000	00000000
			16	

255.255.224.0

Subnet Mask	11111111	11111111	111	00000	00000000
			3	13	

$2^n = 2^3 = 8$ subnets

Supernetting and Address depletion

- **Supernetting**
  - **Combining several class C addresses to create a larger range of addresses**
- **Address Depletion**
  - **The fast growth of the Internet led to the near depletion of the available addresses.**
  - **Classful addressing, which is almost obsolete, is replaced with classless addressing.**

Network Address

❑ Network Addresses

- ❖ The first address in a block is normally not assigned to any device;
- ❖ It is used as the network address that represents the organization to the rest of the world.

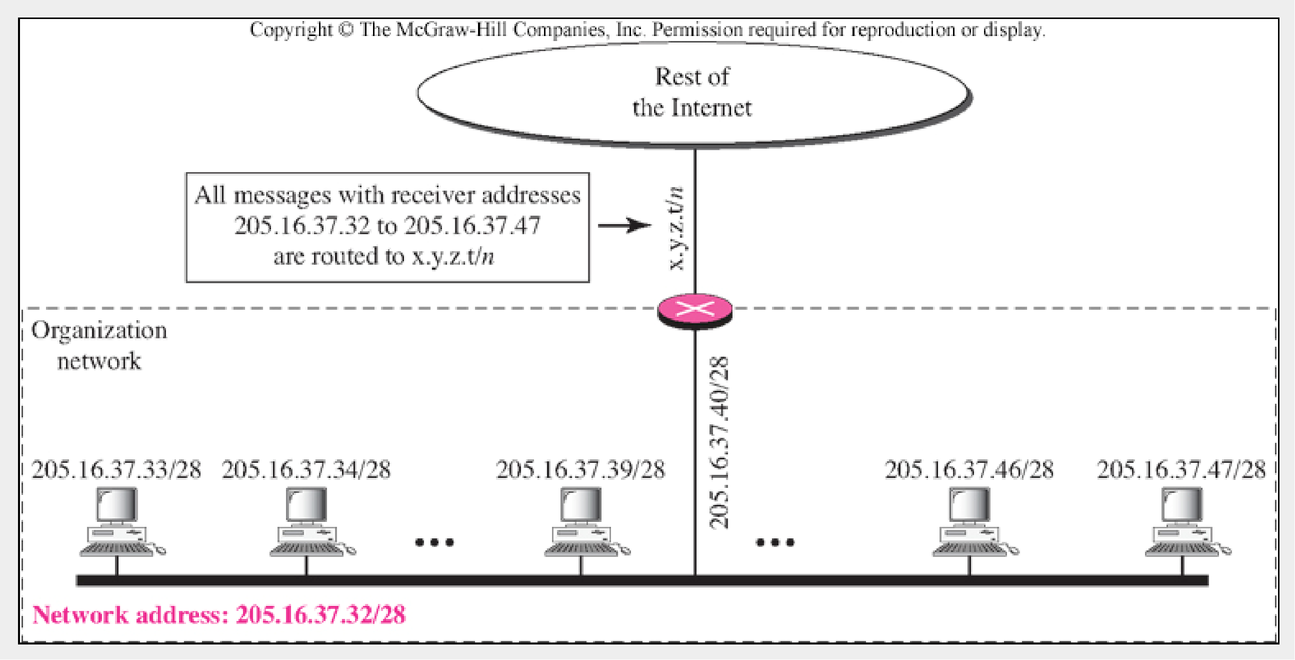


Figure 19.4 *A network configuration for the block 205.16.37.32/28*

Network Address

❑ Hierarchy

- IP addresses have levels of hierarchy.
- For example, a telephone network has three levels of hierarchy.
  - The leftmost 3 digits define the area code, the next 3 digits define the exchange, the last 4 digits define the connection of the local loop to the central office.

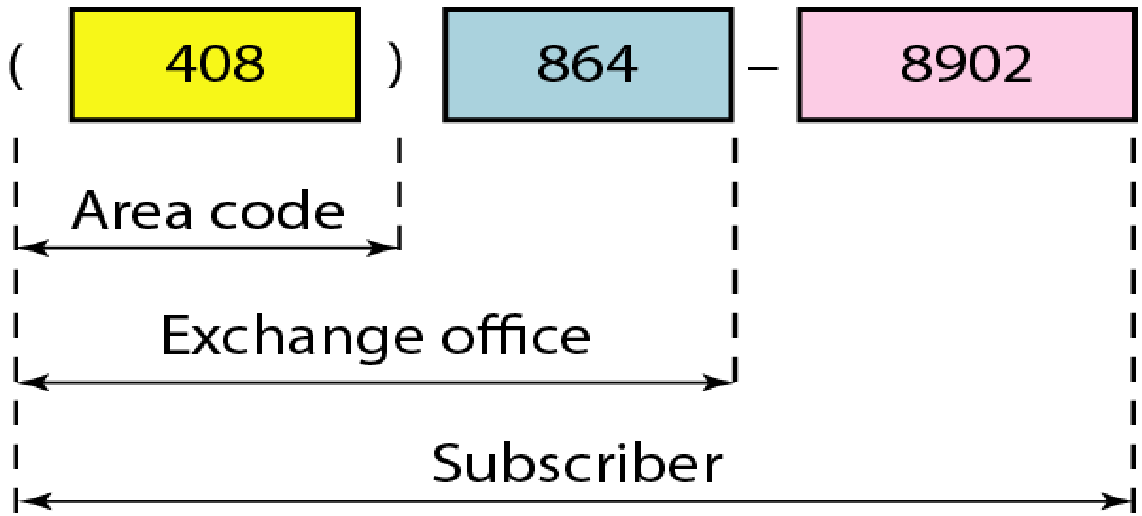


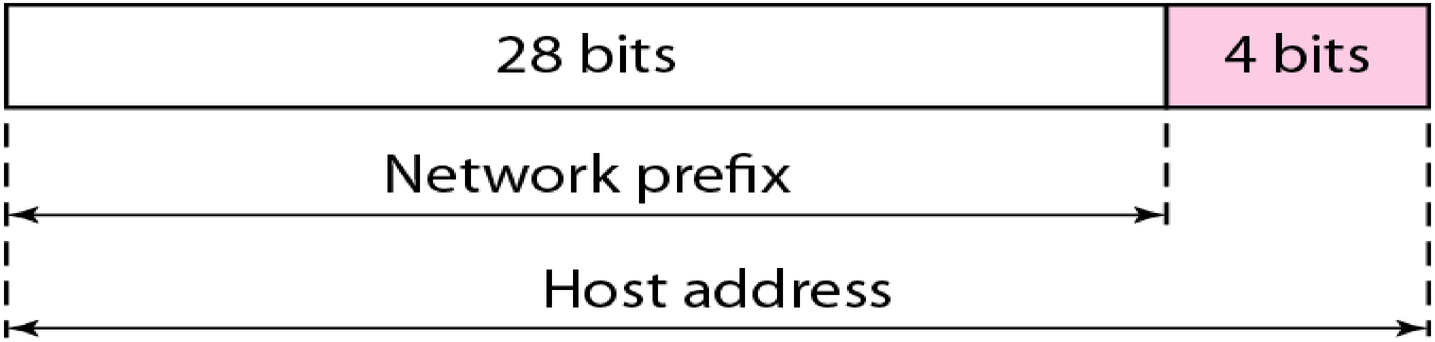
Figure 19.5 *Two levels of hierarchy in an IPv4 address*

Subnetting and Supernetting

Two-level Hierarchy : No Subnetting

- Each IP address in the block can define only two-level of hierarchy when not subnetted.
  - the leftmost *n* bits (prefix) define the network;
  - the rightmost 32 − n bits define the host.
- The part of the address that defines the network is called the Prefix;
- The part that defines the host is called the Suffix.
- The prefix is common to all addresses in the network; the suffix changes from one device to another.

Figure 19.6 *A frame in a character-oriented protocol*



Subnetting and Supernetting

❑ Three-Levels of Hierarchy : Subnetting

- ❖ **Creating clusters of networks (called subnets)**

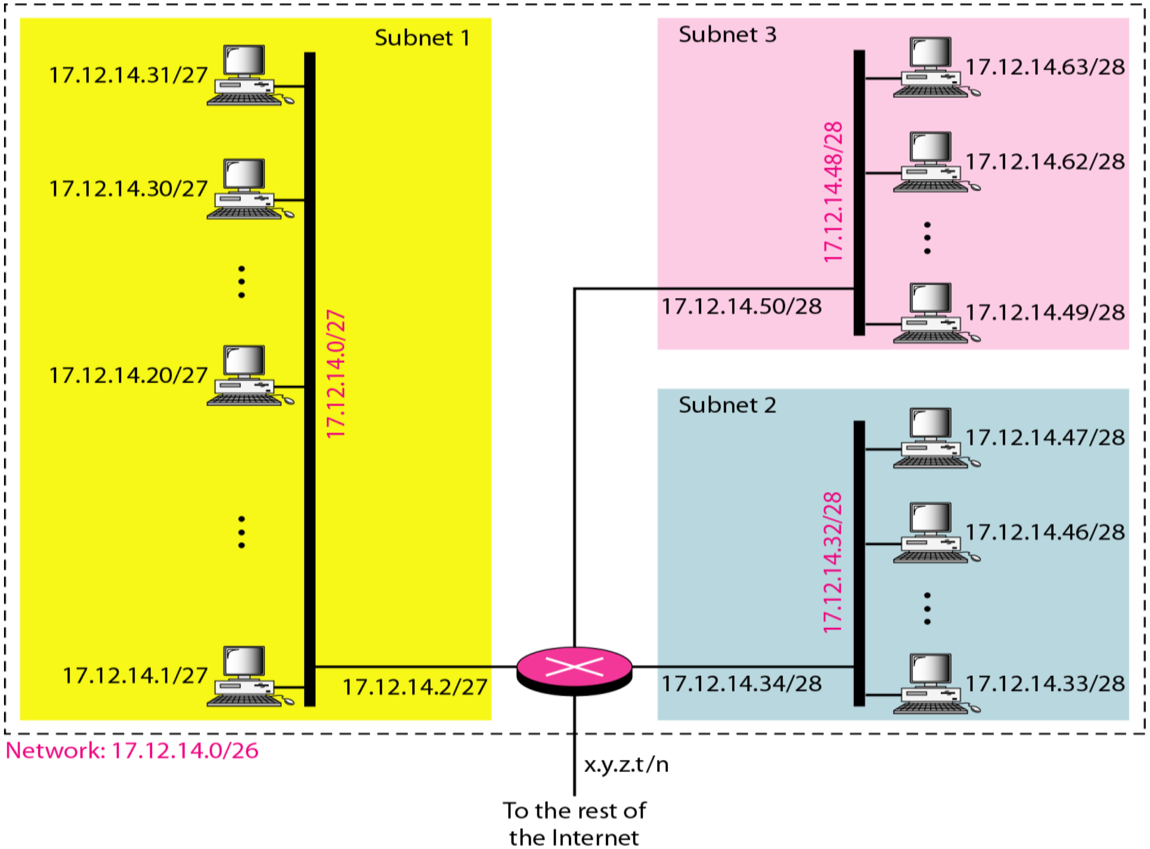


Figure 19.7 *Configuration and addresses in a subnetted network*

Subnetting and Supernetting

- We have three levels of hierarchy through subnetting.
  - The subnet prefix length can differ for the subnets.

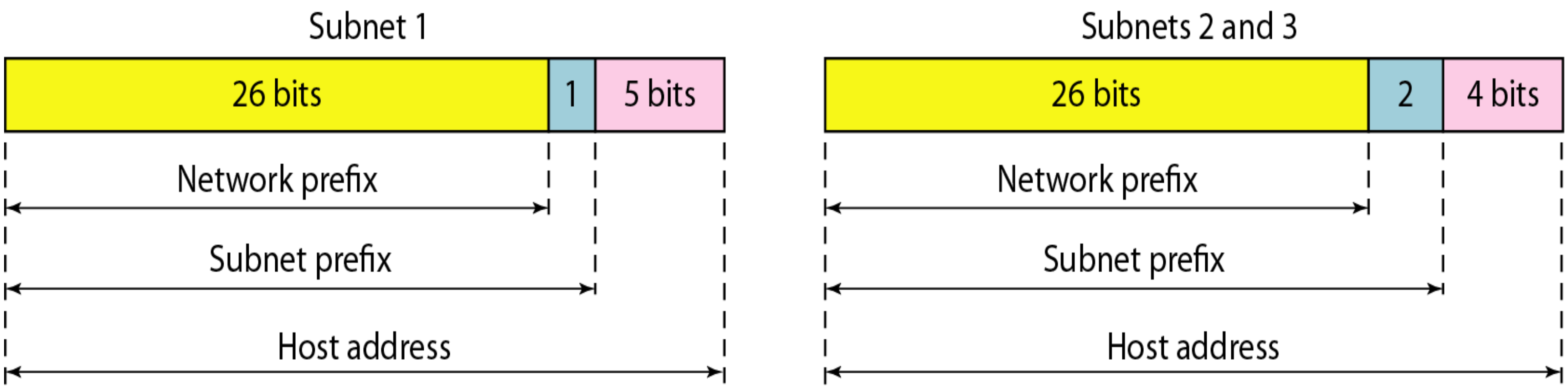
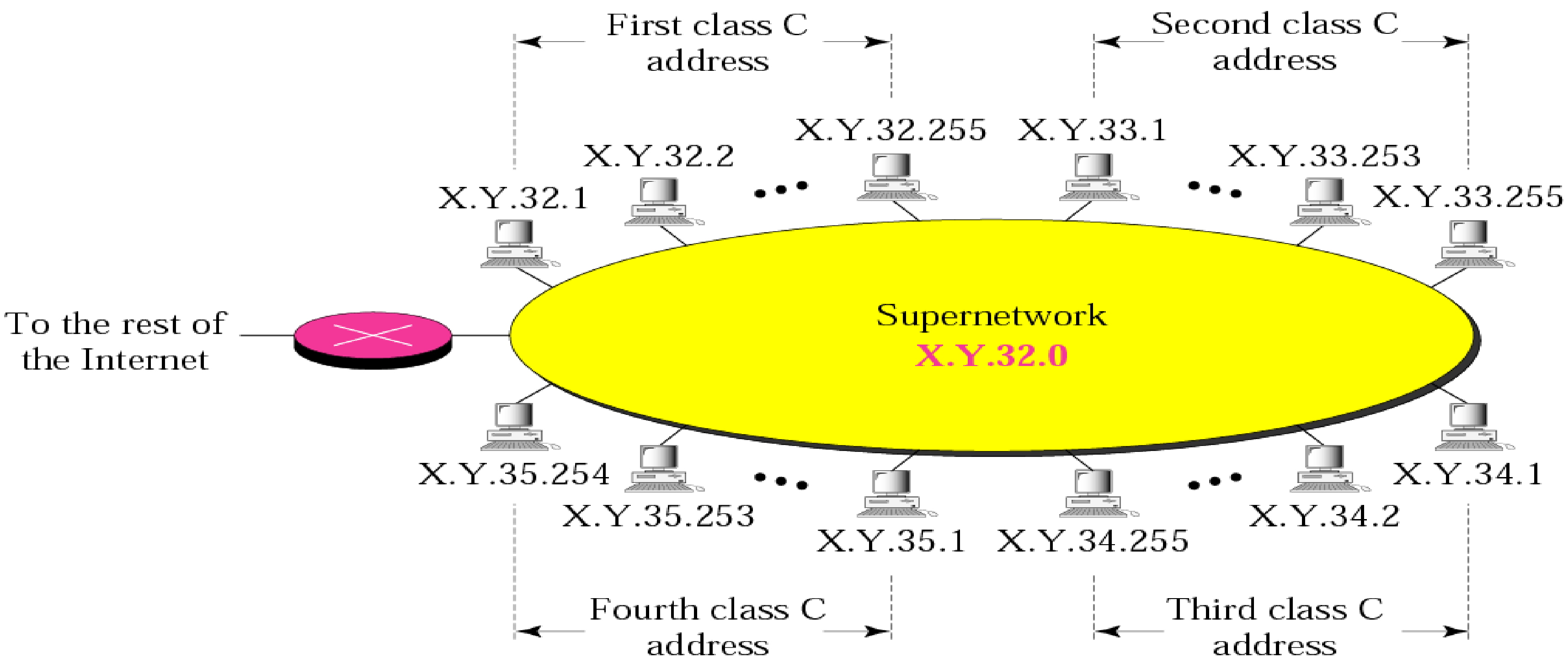


Figure 19.8 *Three-level hierarchy in an IPv4 address*

Supernetting

- A maximum number of Class C is 256 addresses,
- If organization needed more addresses, The Supernetting can combine several class C blocks to create a larger range of addresses.

  (The mask changes from /24 to /22)



Network Address Translation (NAT)

Network Address Translation (NAT)

- NAT enables a user to have a large set of address internally and one address, or a small set of addresses, externally.
- The Internet authorities have reserved 3 sets of addresses as private addresses.
  - Any organization can use an address out of this set without permission from the Internet authorities.
  - They are unique inside the organization, but they are not unique globally.
  - No router will forward this packet as the destination address.

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}

Network Address Translation (NAT)

❑NAT Implementation

❖ The router that connects the network to the global address uses one private address and one global address.

❖The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

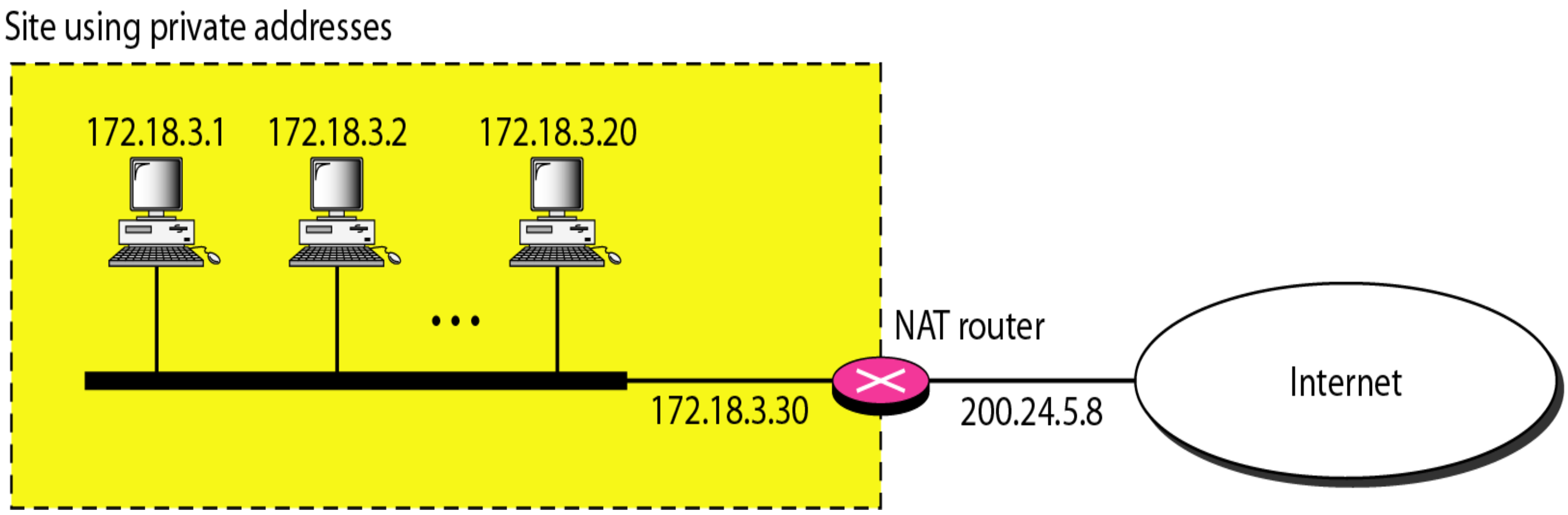


Figure 19.10 *A NAT implementation*

Network Address Translation (NAT)

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 addresses in the packet with the appropriate private address.

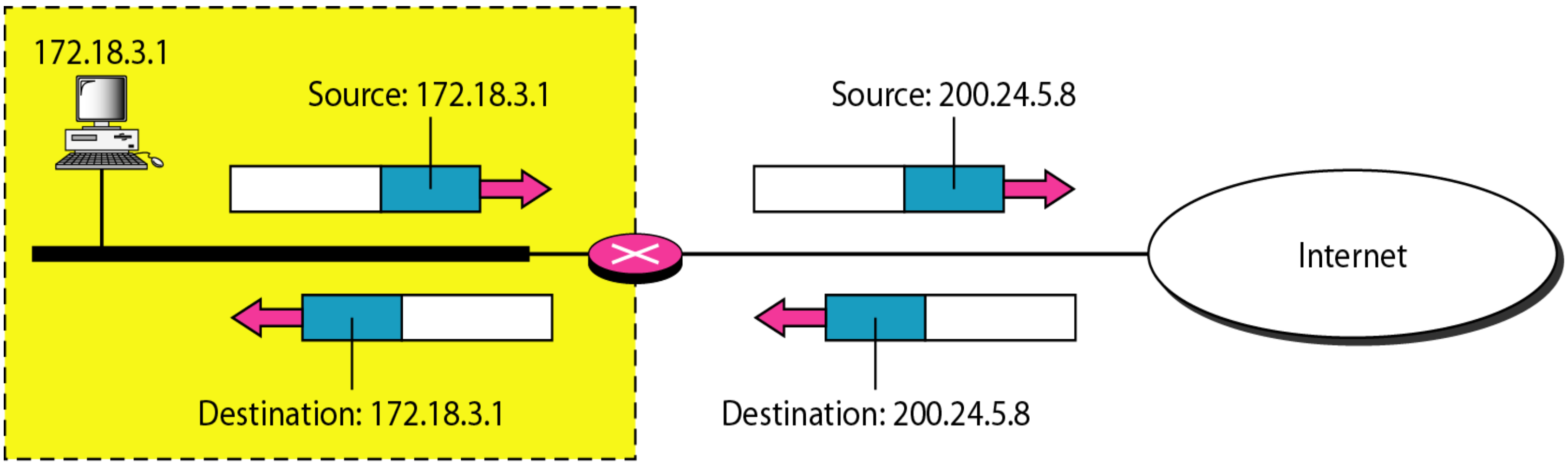


Figure 19.11 *Addresses in a NAT*

Network Address Translation (NAT)

❑Translation Table

❖ When the router translates the source address of the outgoing packet, it also makes note of the destination address – where the packet is going.

❖When the response comes back from the destination, the router uses the source address of the packet to find the private address of the packet.

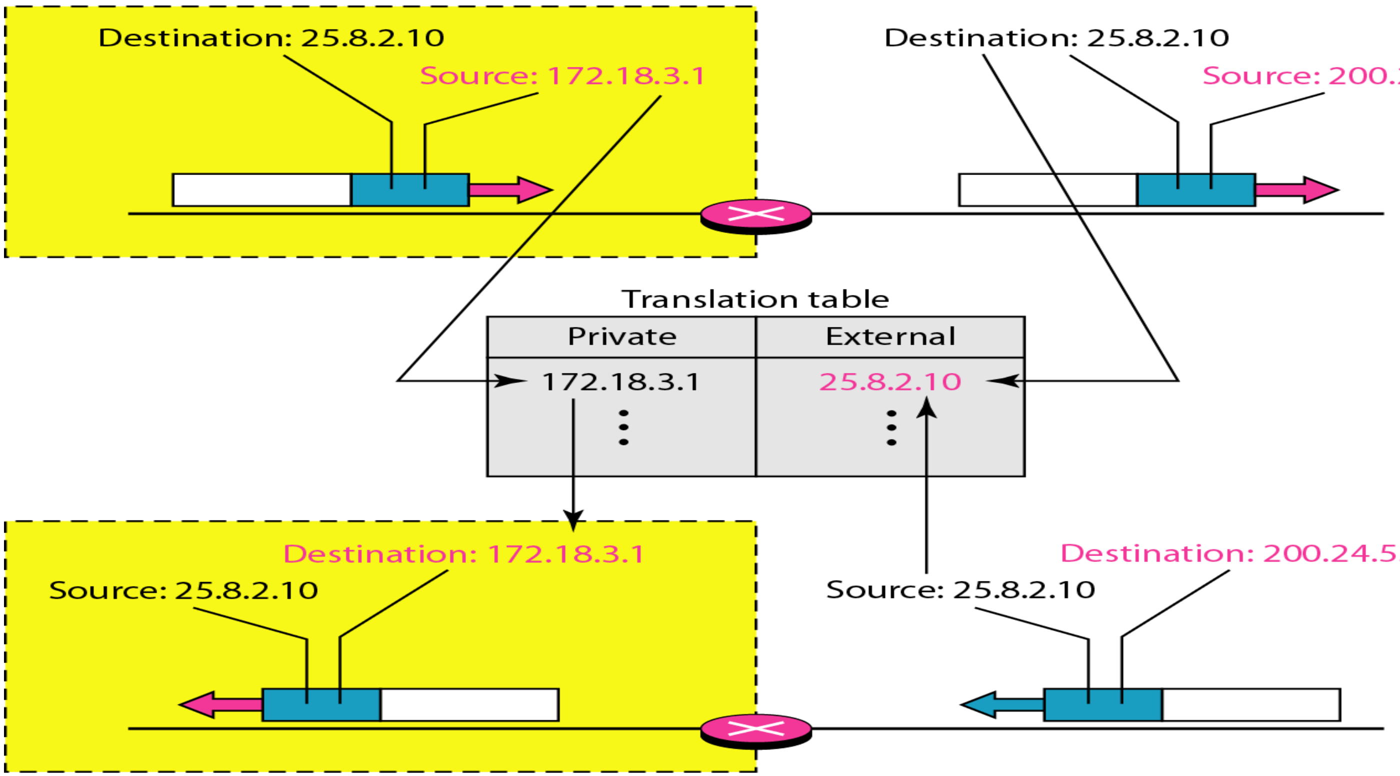


Figure 19.12 *NAT address translation*

Network Address Translation (NAT)

- Using both IP addresses and port numbers

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
. . .	. . .	. . .	. . .	. . .

19-2 IPv6 ADDRESSES

Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6.

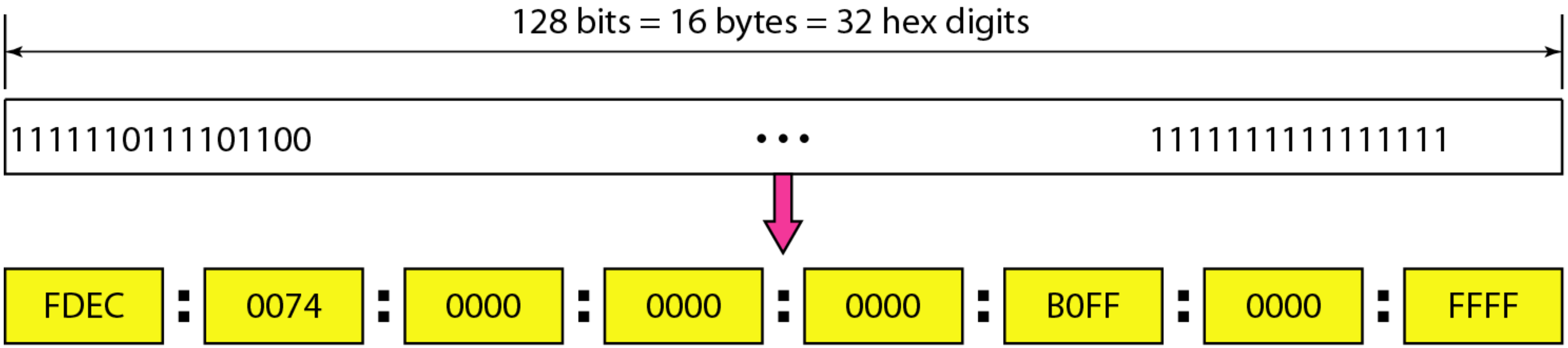
Topics discussed in this section:

Structure
Address Space

Structure - IPv6

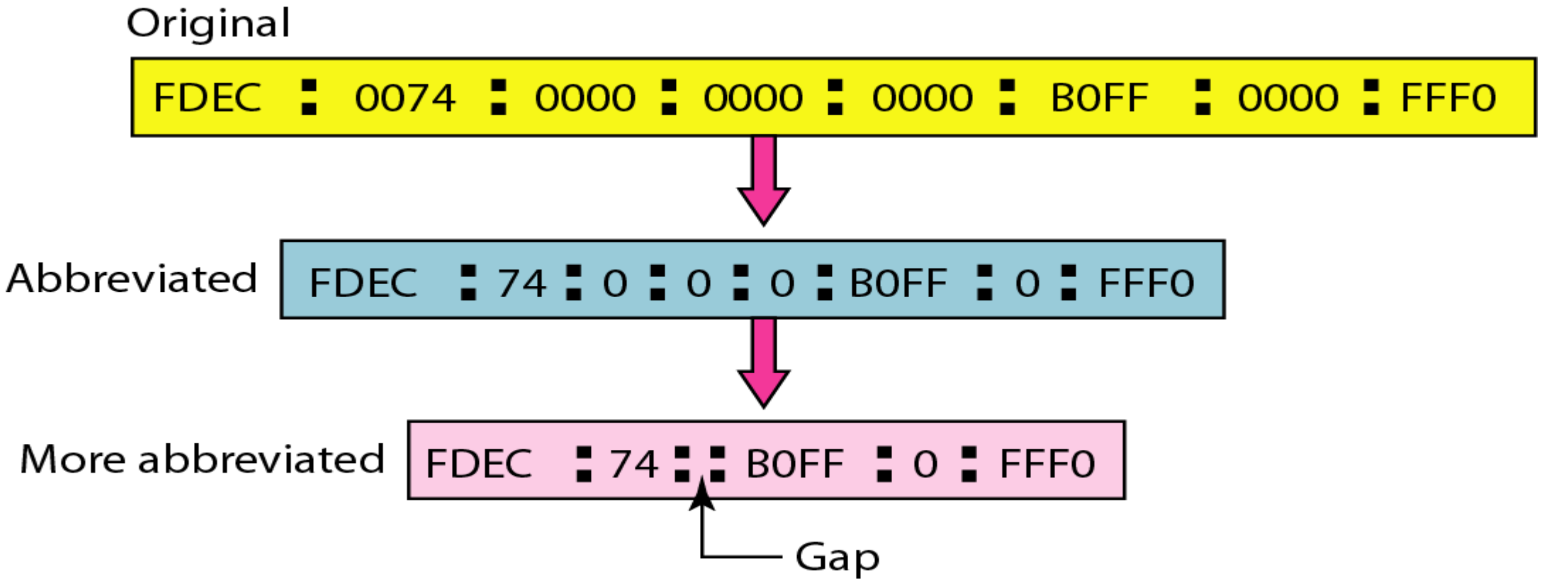
- An IPv6 address consists of 16 bytes (Octets); it is 128 bits long.

- Hexadeximal Colon Notation
  - In this notation, 128 bits is divided into eight sections, each 2 bytes in length.
  - Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.



Abbreviation

- Although the IP address, even in hexadecimal format, 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.



Address Space

- **IPv6 has a much lager address space; 2^{128} addresses are available.**

Summary (1)

- At the Network layer, a global identification system that uniquely identifies every host and router is necessary for delivery of packet from host to host.
- An IPv4 address is 32 bits long and uniquely and universally defines a host or router on the Internet.
- In classful addressing, the portion of the IP address that identifies the network is called the netid.
- In classful addressing, the portion of the IP address that identifies the host or router on the network is called the hosted.
- An IP address defines a device's connection to a network.
- There are five classes in IPv4 addresses. Classes A, B, and C differ in the number of hosts allowed per network. Class D is for multicasting and Class E is reserved.

Summary(2)

- The class of an address is easily determined by examination of the first byte.
- Addresses in classes A, B, or C are mostly used for unicast communication.
- Address in class D are used for multicast communication.
- Subnetting devides on large network into several smaller ones, adding an intermediate level of hierarchy in IP addressing.
- Supernetting combines several networks into one large one.
- In classless addressing, we can divided the address space into variable-length blocks.

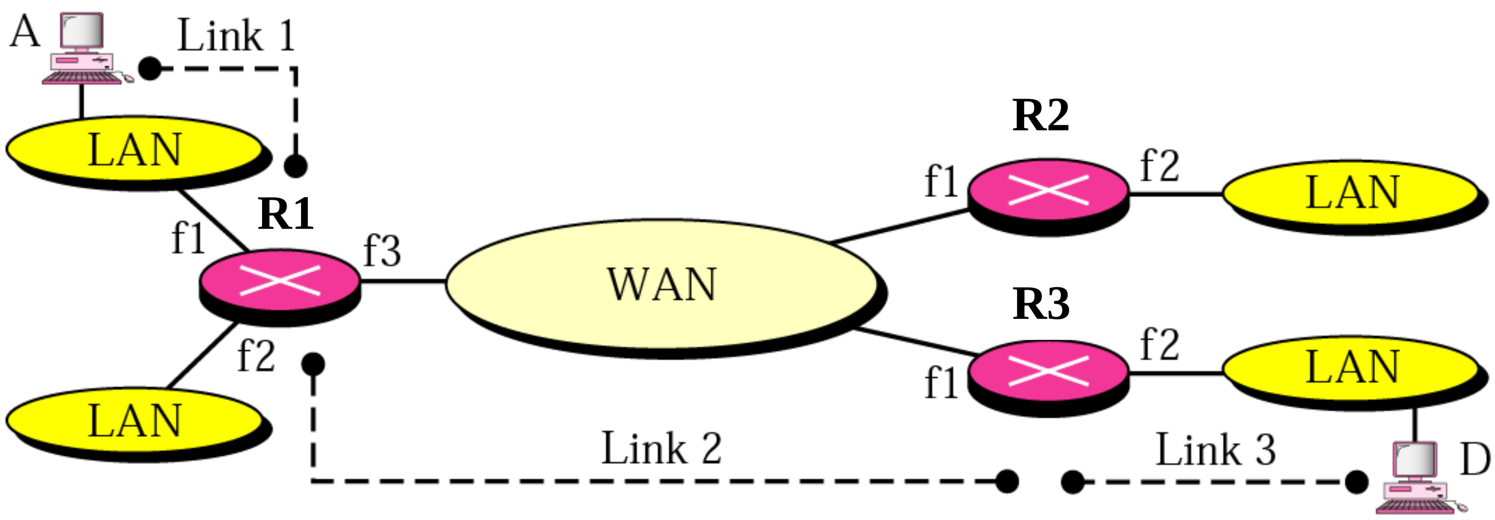
Chapter 20

Network Layer: Internet Protocol

Internetworking

- **Internetworking**
  - The physical and data link layers of a network operate locally.
  - These two layers are jointly responsible for data delivery on the network from one node to the next.

R



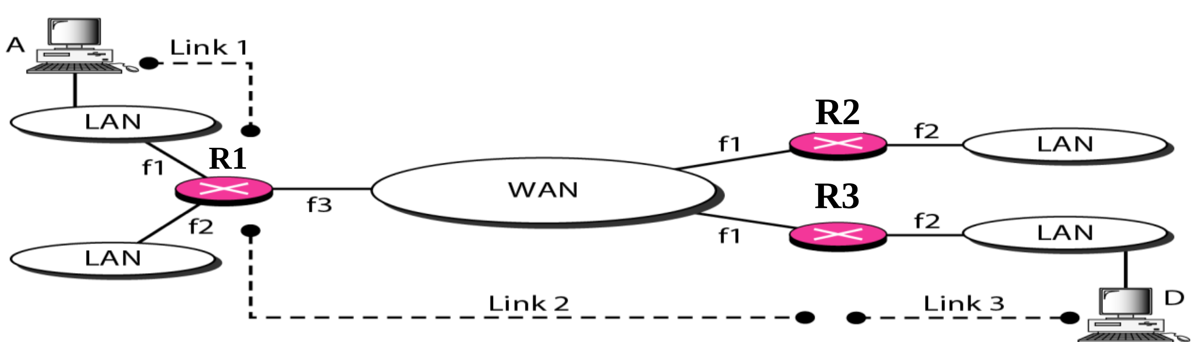
Internetworking

- **When data arrive at interface f1 of R1, how does R1 know that interface f3 is the outgoing interface ?**

  - **There is no provision in the data link (or physical) layer to help R1 make the right decision. The frame dose not carry any routing information either.**

  - **The frame contains the MAC address of the A and R1.**

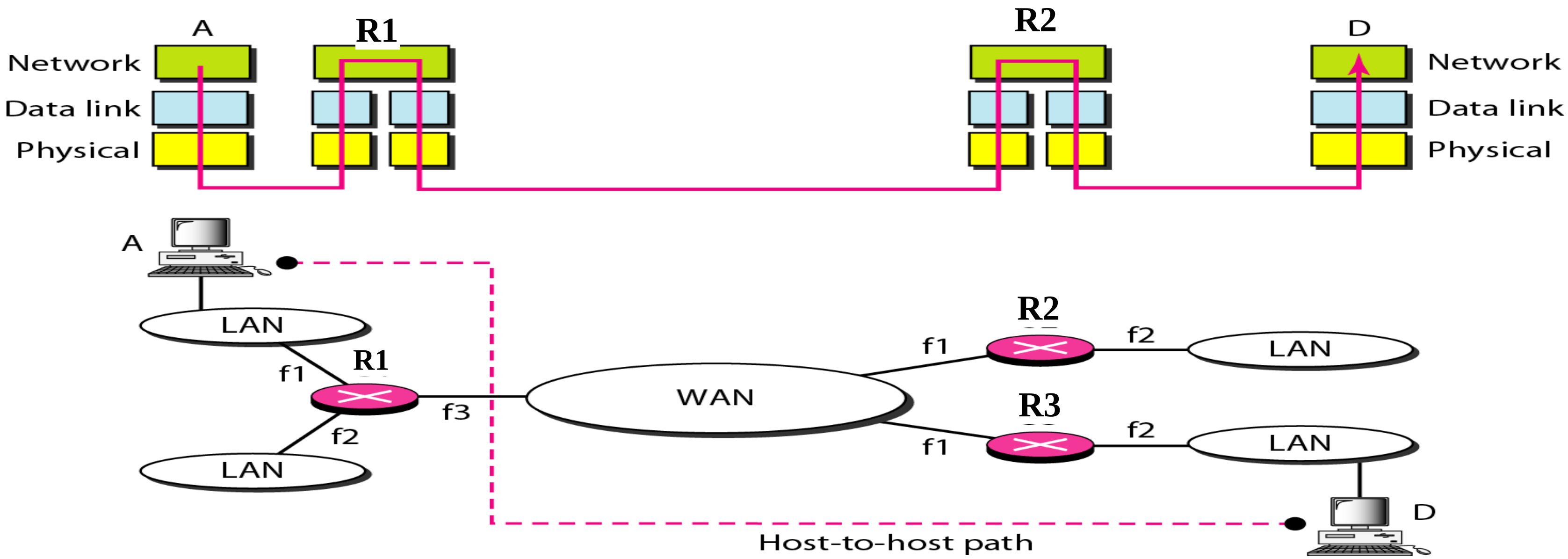
- **A LAN or a WAN carry the frame through one link.**



Internetworking

❑ Need for Network Layer

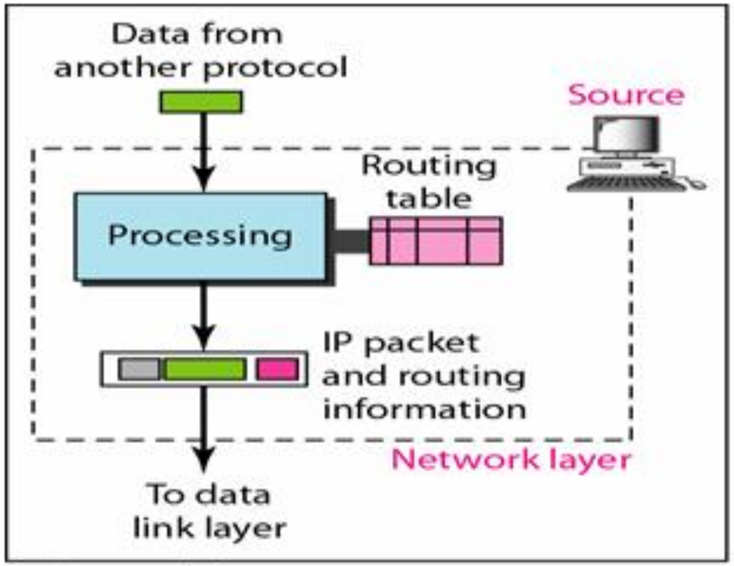
- To solve the problem of delivery through several links, the network layer (or the inter network layer, as it is sometimes called) was designed.
- The network layer is responsible for host-to-host delivery and for routing the packets through the routers or switches.



Internetworking

Network layer at the source

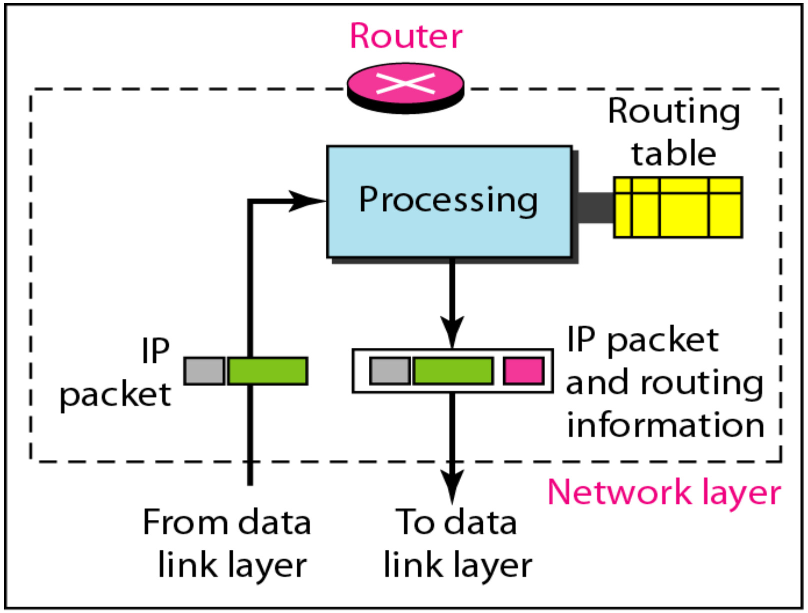
- The network layer is responsible for creating a packet from the data coming from another protocol.
- The header of the packet contains, among other information, the logical addresses of the source and destination.
- The network layer is responsible for checking its routing table to find the routing information.
- If the packet is too large, the packet is fragmented.



a. Network layer at source

Internetworking

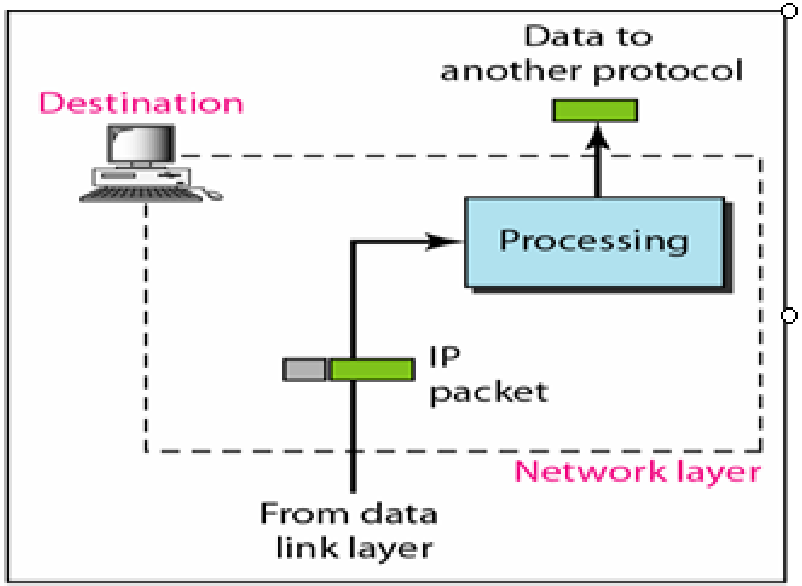
- Network layer at the switch or router
  - The network layer is responsible for routing the packet.
  - When a packet arrives, the router or switch consults its routing table and finds the interface from which the packet must be sent.
  - The packet, after some changes in the header, with the routing information is passed to the data link layer again.



c. Network layer at a router

Internetworking

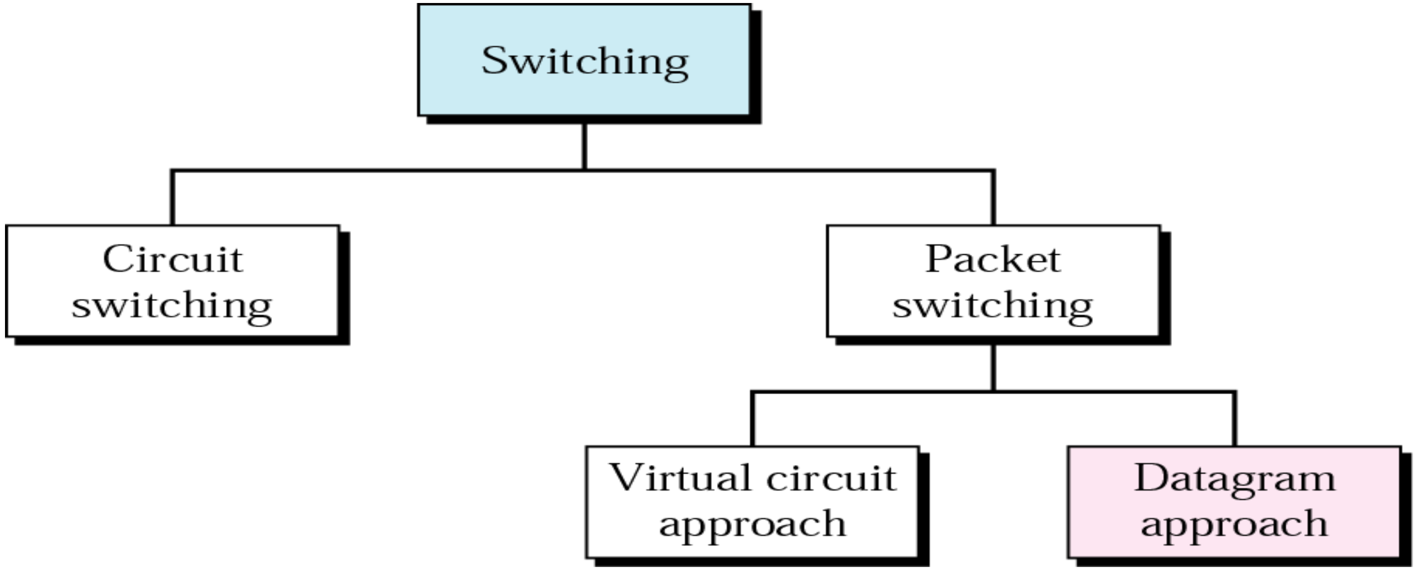
- **Network layer at the destination**
  - **The network layer is responsible for address verification;**
  - **It makes sure that the destination address on the packet is the same as the address of the host.**
  - **If he packet is a fragment, the network layer waits until all fragments have arrived, and then reassembles them and delivers the reassembled packet to the transport layer.**



b. Network layer at destination

Internet as a Datagram Network

- The Internet, at the network layer, is a packet switched network.
- The Internet has chosen the datagram approach to switching in the network layer.
- It uses the universal addresses defined in the network layer to route packets from the source to the destination.



Internet as a Connectionless Network

- Connection-oriented service
  - The source first makes a connection with the destination before sending a packet.
  - When the connection is established, a sequence of packets can be sent one after another.
  - They are sent on the same path in sequential order.
  - When all packets of a message have been delivered, the connection is terminated.

Internet as a Connectionless Network

Connection-oriented service

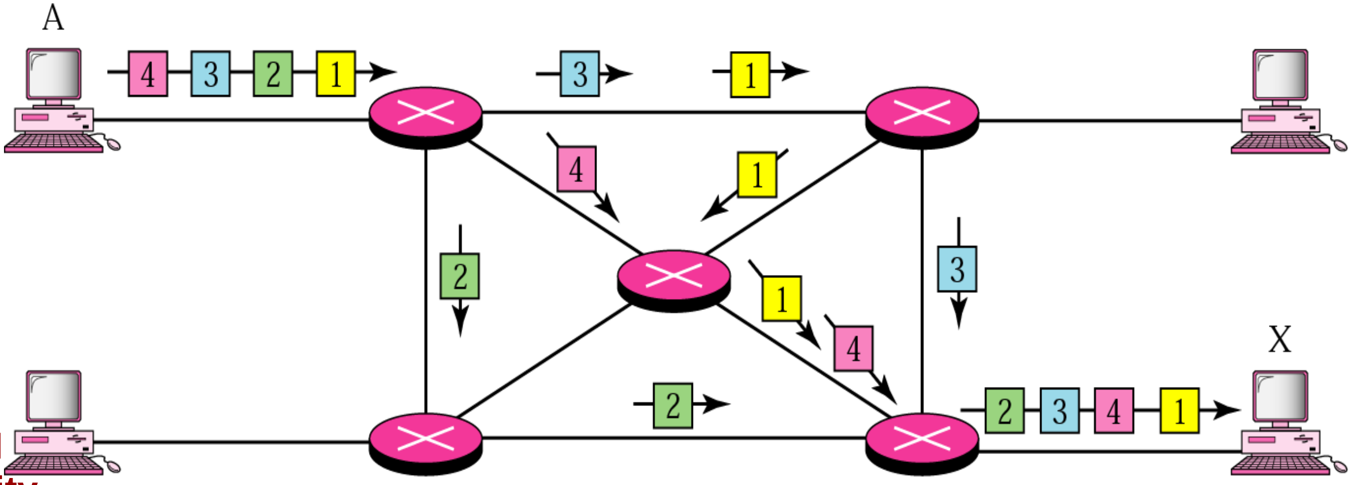
- The source first makes a connection with the destination before sending a packet.
- When the connection is established, a sequence of packets can be sent one after another.
- They are sent on the same path in sequential order.
- When all packets of a message have been delivered, the connection is terminated.

Internet as a Connectionless Network

- **Connectionless service**

  - **The network layer protocol treats each packet independently, with each packet having no relationship to any other packet.**
  - **The packets in a message may or may not travel the same path to their destination.**
  - **This type of service is used in the datagram approach to packet switching.**

  - **Communication at the network layer in the Internet is connectionless.**



20-2 IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.

Topics discussed in this section:

Datagram
Fragmentation
Checksum
Options

IPv4

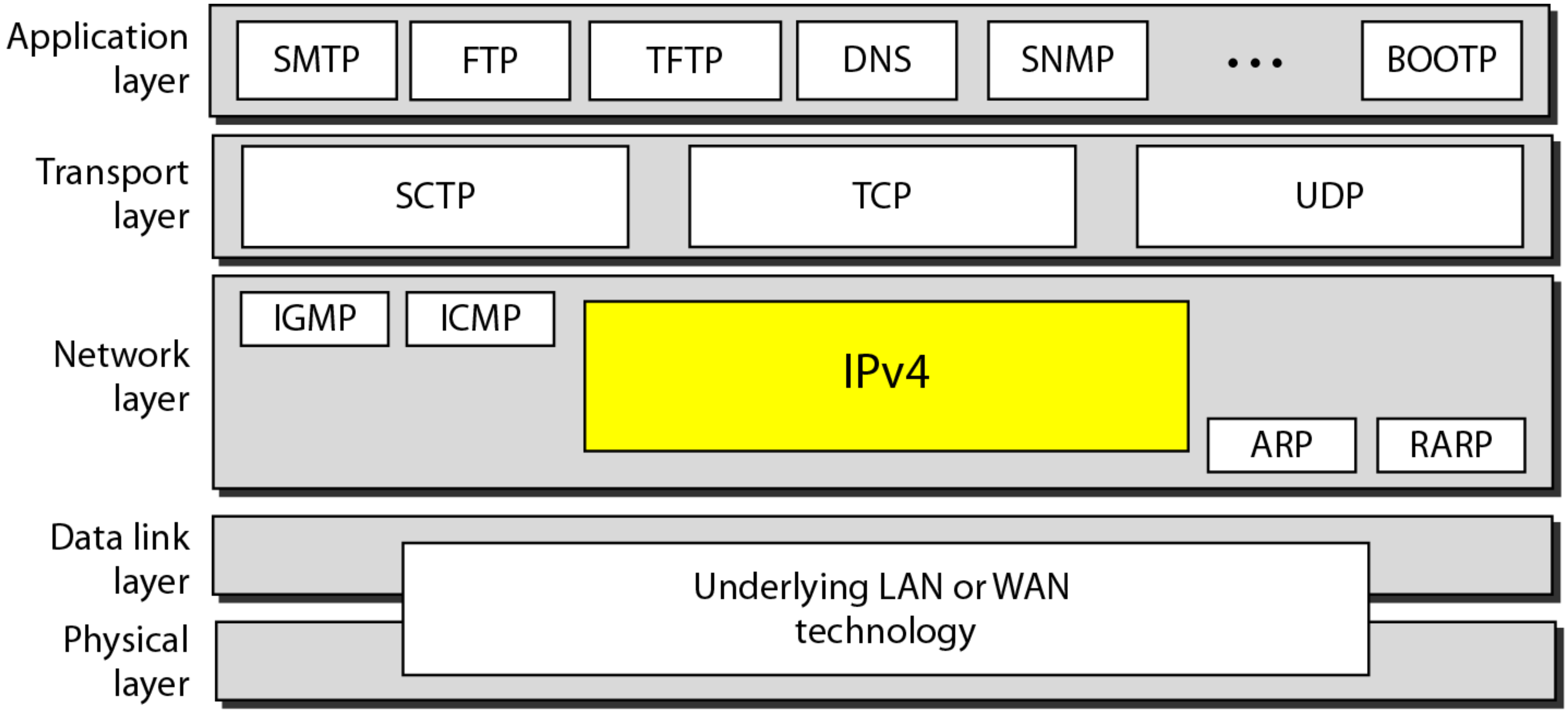


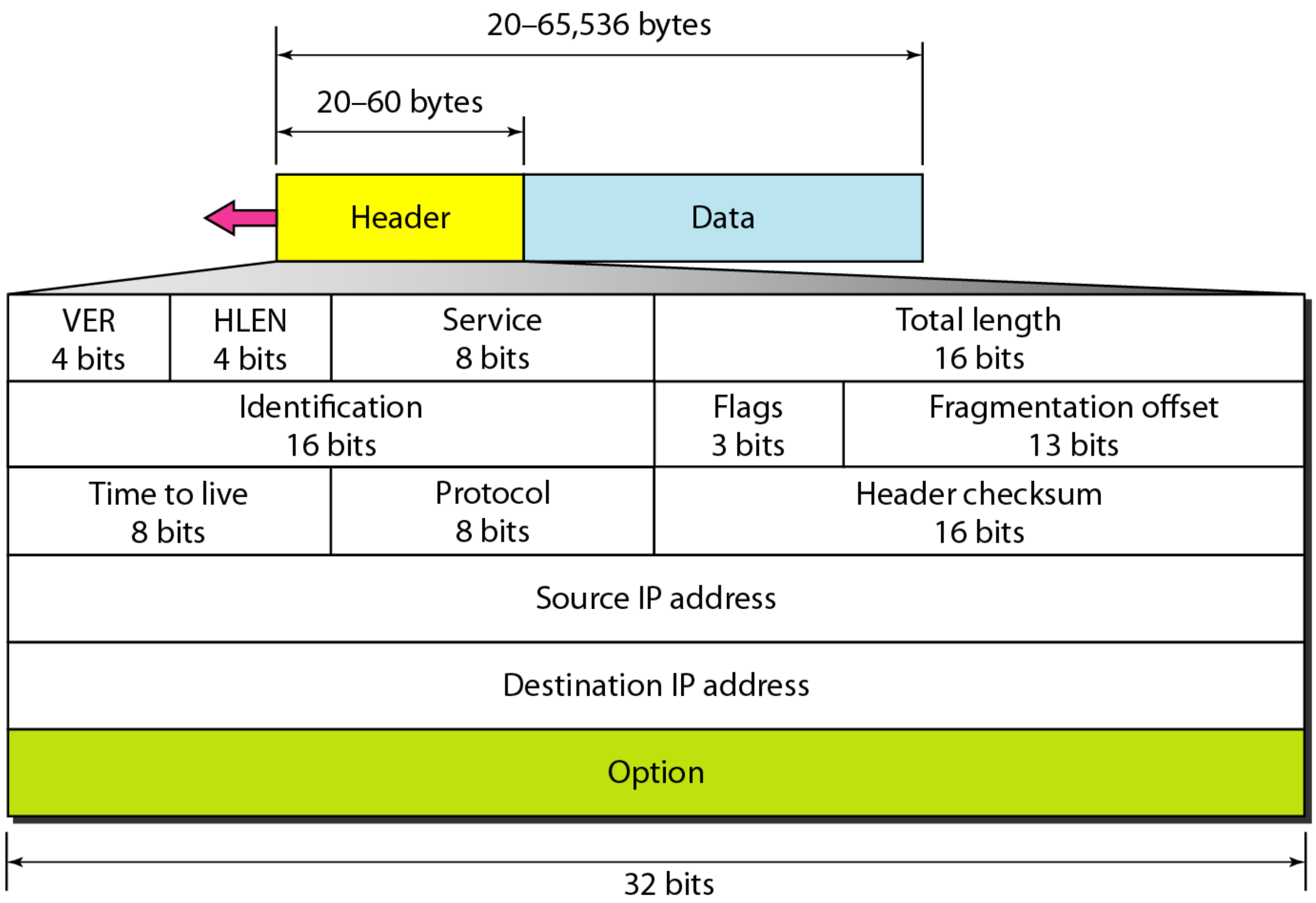
Figure 20.4 ***Position of IPv4 in TCP/IP protocol suite***

IPv4

- **Best-effort delivery**
  - **IPv4 is an unreliable and connectionless datagram protocol - a best-effort delivery service.**
  - **The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header).**
- **Connectionless protocol**
  - **Each datagram is handled independently, and diagrams sent by the source to the same destination could arrive out of order.**
  - **Also, some could be lost or corrupted during transmission.**
  - **IPv4 relies on a high-level protocol to take of all these problem.**

IPv4 Datagram

- Packets in the IPv4 layer are called Datagrams.



IPv4 Datagram (cont'd)

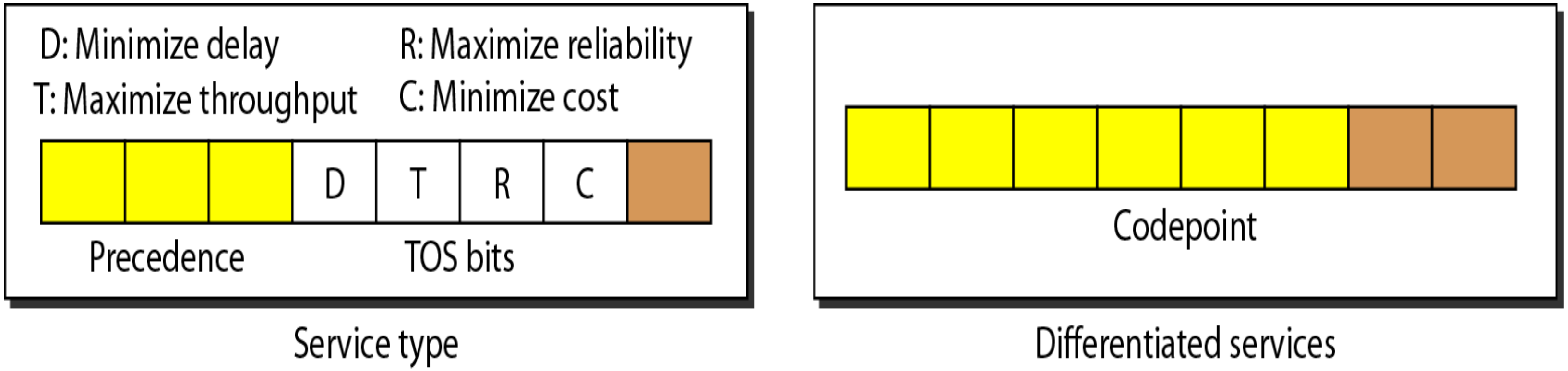
- A datagram is a variable-length packet consisting of a header and data.
- **Header**
  - length : 20 – 60 bytes
  - Contains information essential to routing and delivery.
- **Version (VER)** : It defines the Version of IPv4. it is 4.
- **Header Length (HLEN)** : Defining the total length of the datagram header in 4byte words.

IPv4 Datagram (cont'd)

Differentiated Services

- **The first 3 bits are called precedence bits. The next 4 bits are type of service (TOS) bits, and the last bit is not used.**
- **The precedence subfield was part of version 4, but never used.**

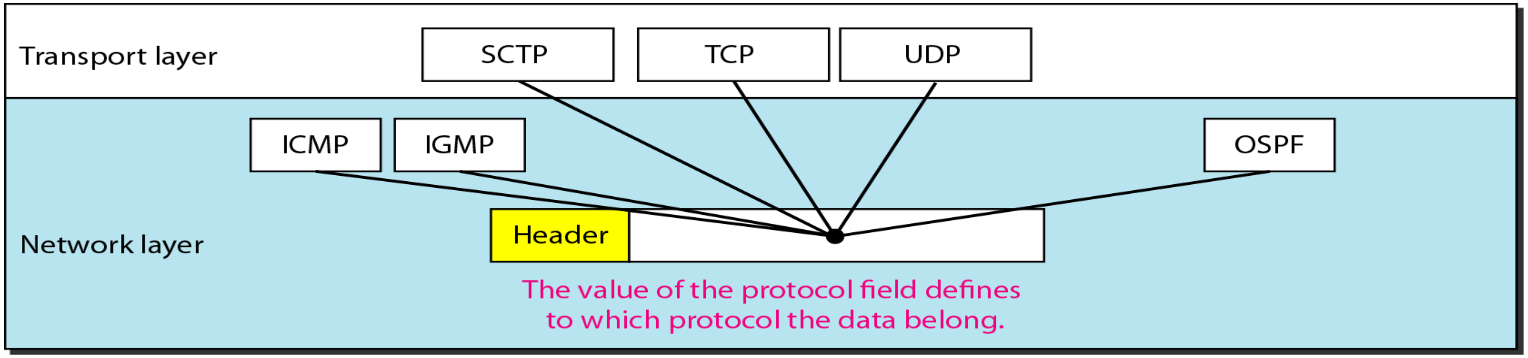
Figure 20.6 *Service type or differentiated services*



IPv4 Datagram (cont'd)

Protocol

- Defining the higher level protocol that uses the services of the IP layer
  - TCP, UDP, ICMP, and IGMP
  - Multiplexing data from different higher level protocols



Value	Protocol
1	ICMP
2	IGMP
6	TCP
8	EGP
17	UDP
89	OSPF

Summary

- IPv4 is an unreliable connectionless protocol responsible for source-to-destination delivery.
- Packets in the IPv4 layer are called datagrams. A datagram consistes of a header(20 to 60 bytes) and data. The maximum length of a datagram is 65,535 bytes.
- The MTU is the maximum number of bytes that a data link protocol an encapsulate. MTU vary from protocol to protocol.
- Fragmentation is the division of datagram into smaller units to accommodate the MTU of a datalink protocol.
- The IPv4 datagram header consists of a fixed, 20-bte section and a variable options section with a maximum of 40 bytes.
- The options section of the IPv4 header is used for network testing and debugging.

Summary (2)

- The six IPv4 options each have a specific function.
- IPv6, the latest version of the Internet Protocol, has a 128-bit address space, a revised header format, new options, an allowance for extension, support for resource allocation, and increased security measures.
- An IPv6 datagram is composed of a base header and a payload.
- Extension header add functionality to the IPv6 datagram.
- Three strategies used to handle the transition for version 4 to version 6 are dual stack, tunneling, and header translation.

Thanks !