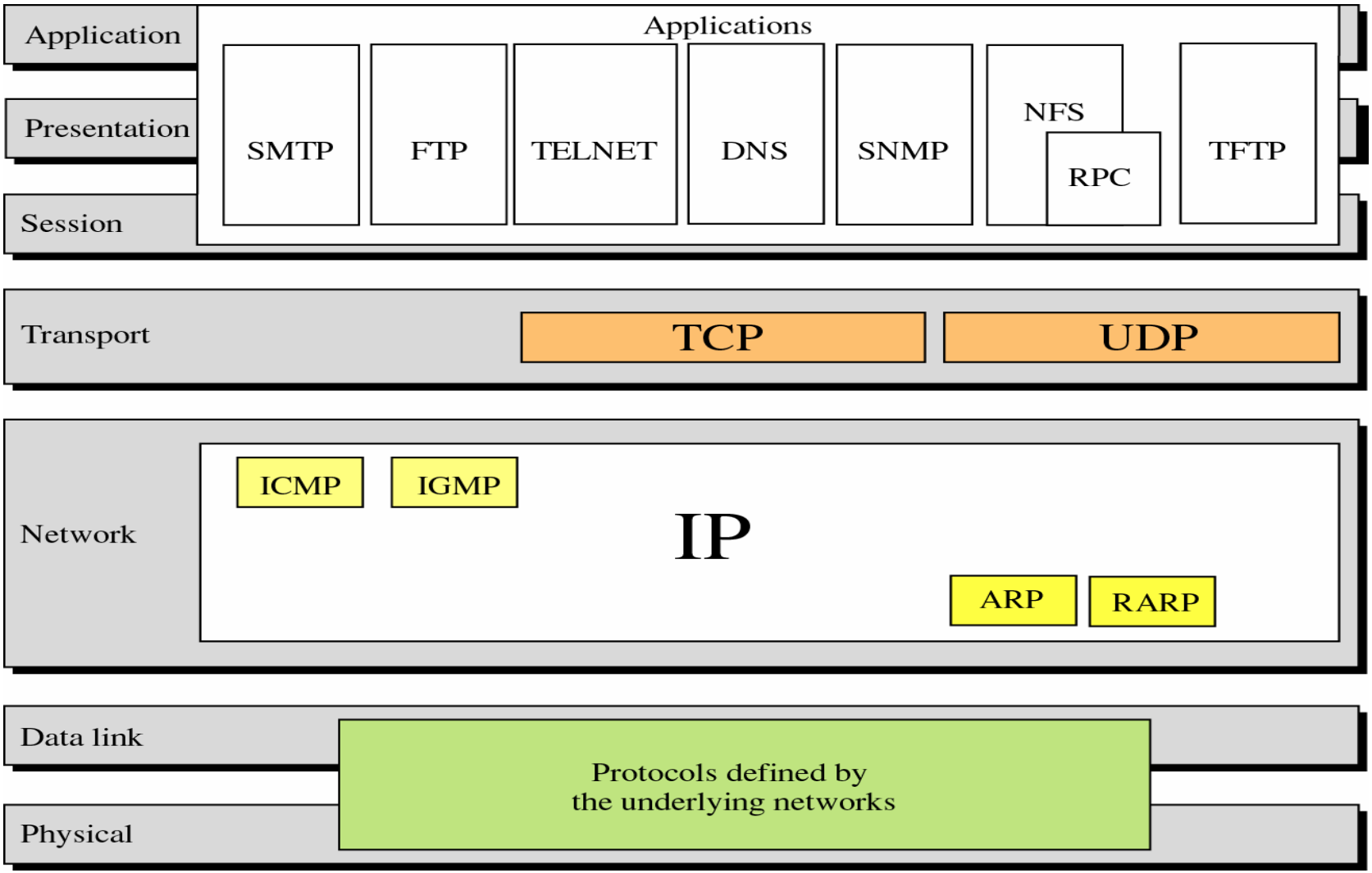
UNIT-1

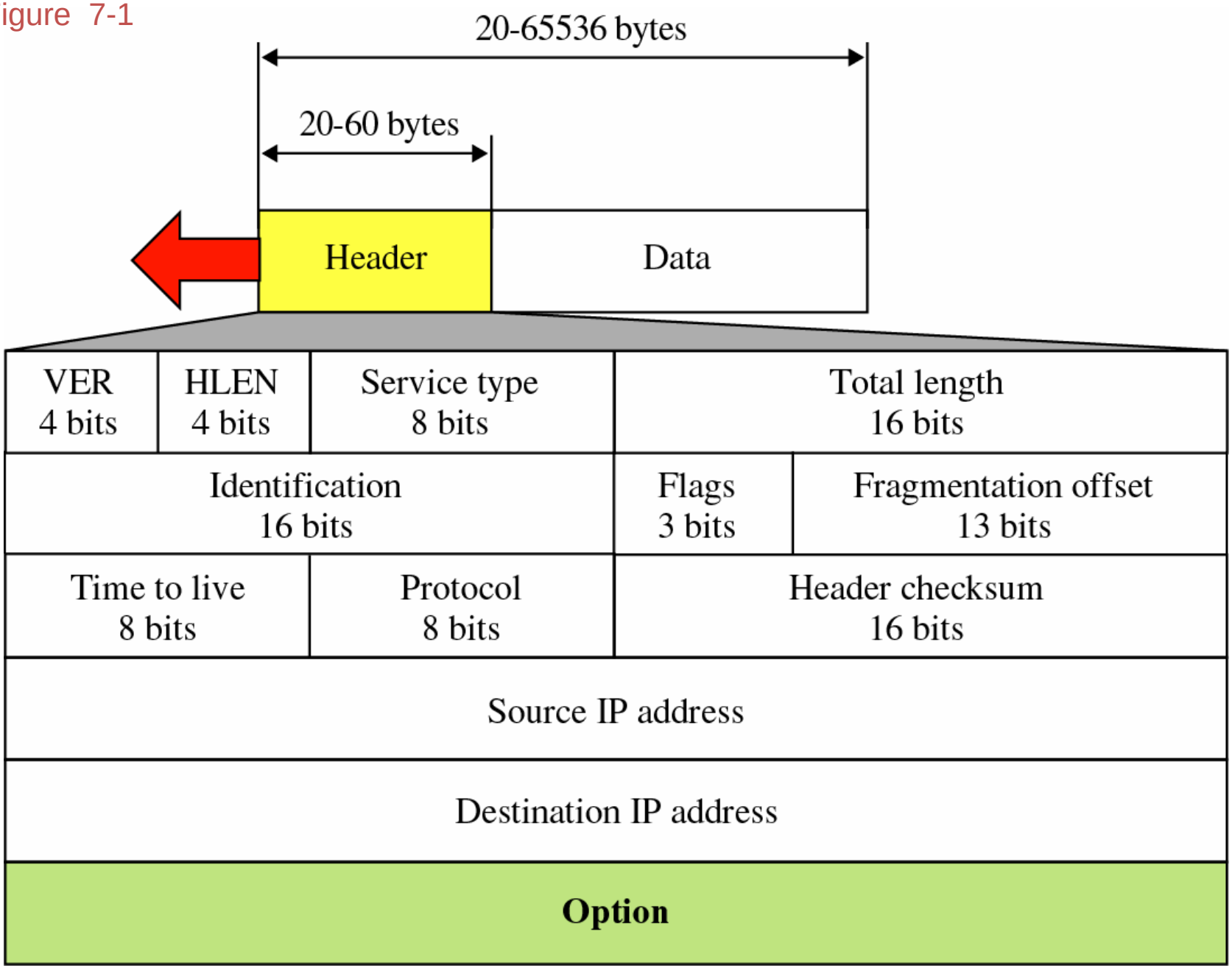
TCP/IP PROTOCOL SUITE



Internet Protocol (IP)

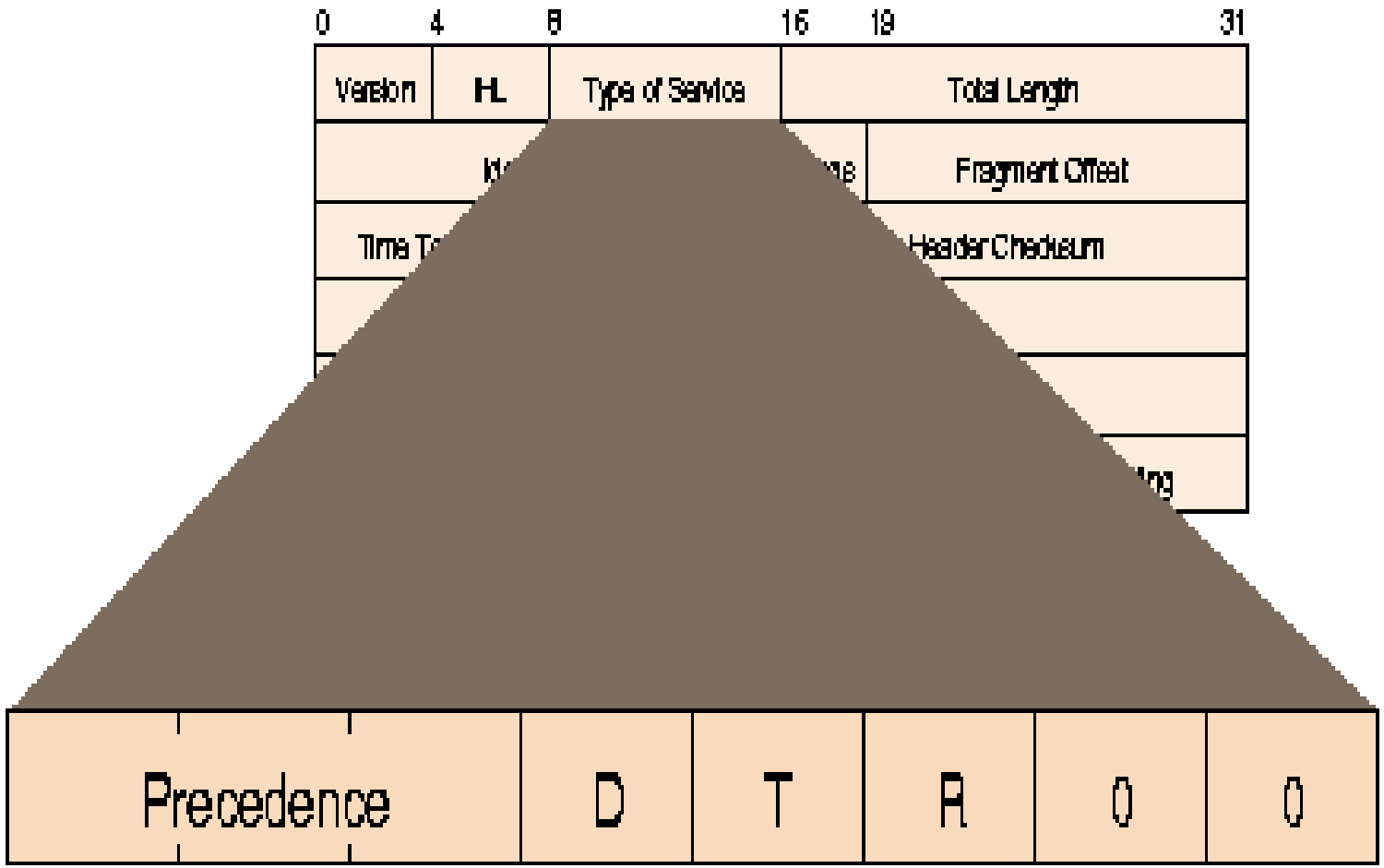
- The unit of transfer in an IP network is called an **IP datagram**. It consists of an IP header and data relevant to higher level protocols.
- It is an unreliable, best-effort, and connectionless packet delivery protocol.

Figure 7-1


20-65536 bytes
20-60 bytes
Header
Data
VER
4 bits
HLEN
4 bits
Service type
8 bits
Total length
16 bits
Identification
16 bits
Flags
3 bits
Fragmentation offset
13 bits
Time to live
8 bits
Protocol
8 bits
Header checksum
16 bits
Source IP address
Destination IP address
Option

- **VER** is the field that contains the IP protocol version. The current version is 4. 6 is the version for IPv6.

- **HLEN** is the length of the IP header in multiples of 32 bits, without the data field.


0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Fragment Offset
Header Checksum
Precedence
D
T
R
0
0

- **Service Type** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.
- *Precedence* specifies the nature/priority:
- 000: Routine
- 001: Priority
- 010: Immediate
- 011: Flash
- 100: Flash override
- 101: Critical
- 110: Internetwork control
- 111: Network control

- *TOS* specifies the type of service value:

1000: Minimize delay

0100: Maximize throughput

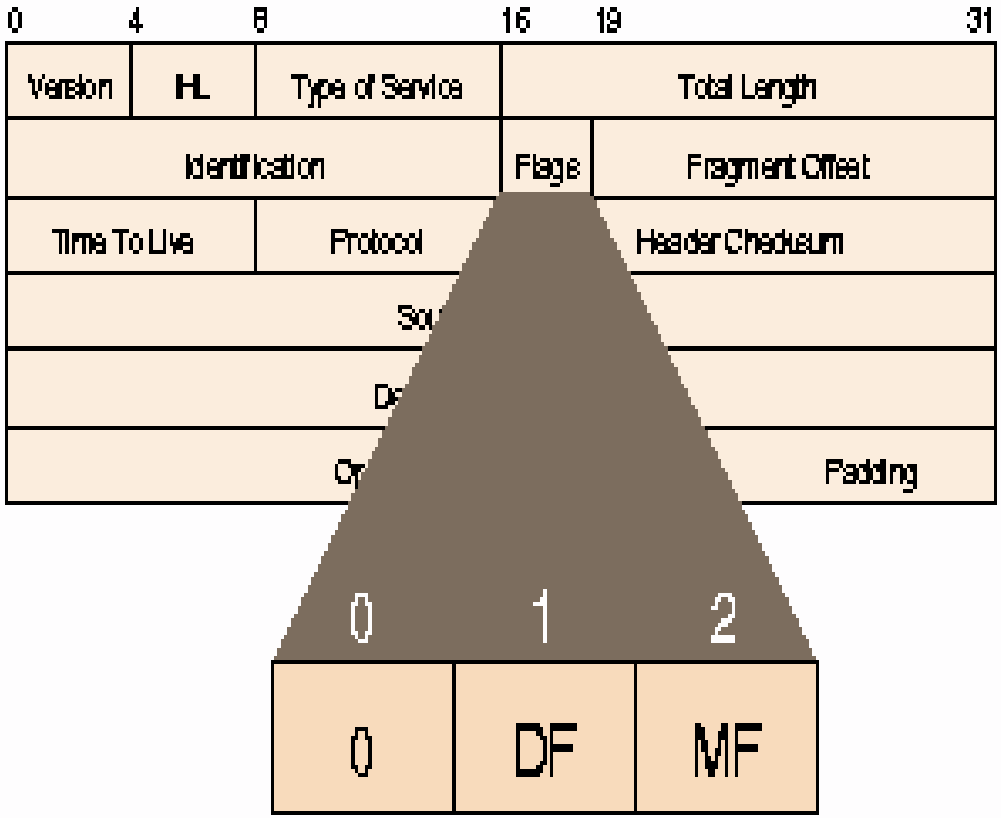
0010: Maximize reliability

0001: Minimize cost

0000: Normal service

The last bit is reserved for future use.

- **Total Length** specifies the total length of the datagram, header and data, in octets.
- **Identification** is a unique number assigned by the sender used with fragmentation.
- **Flags** contains control flags:
- – the first bit is reserved and must be zero;
- – the 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
- – the third is MF (More Fragments), 0 means that this is the last fragment.


0
4
8
16
19
31
Version
HL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Padding
0
1
2
0
DF
MF

- **Fragment Offset** is used to reassemble the full datagram. It is a pointer that shows the offset of the data. If this is the first (or only) fragment, this field contains a value of zero.
- **TTL** (Time to Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.

- **Protocol Number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
- **Header Checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.

- **Source/Destination IP Addresses** are the 32-bit source/destination IP addresses.
- **IP Options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. **Padding** is used to ensure that the IP header ends on a 32 bit boundary.

Figure 7-4

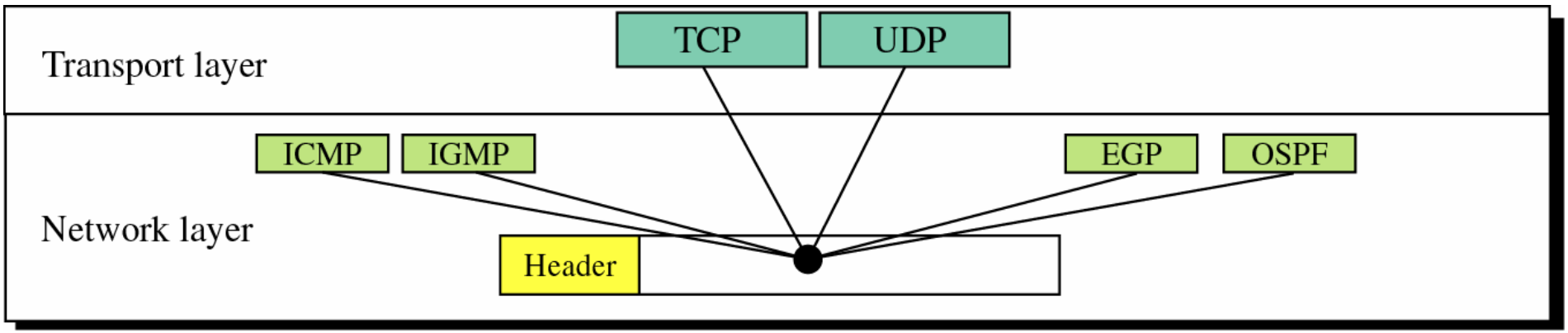
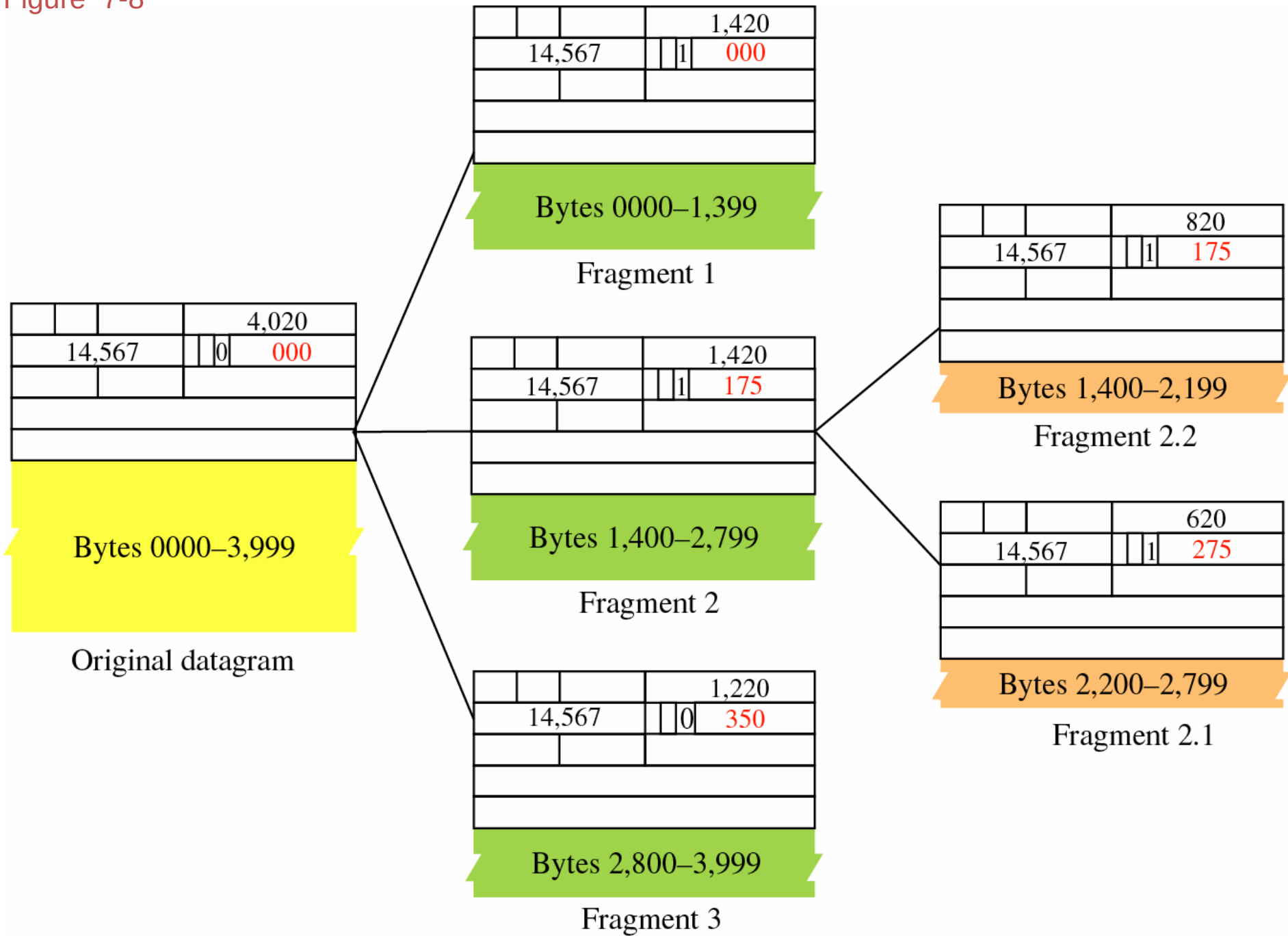

Transport layer
TCP
UDP
ICMP
IGMP
EGP
OSPF
Network layer
Header

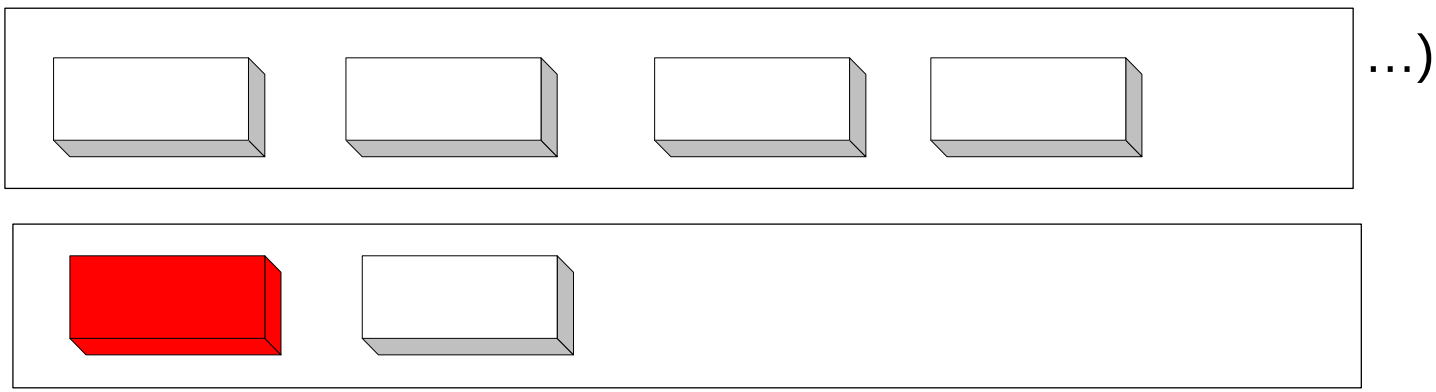
Figure 7-8


4,020
14,567
0
000
Bytes 0000–3,999
Original datagram
1,420
14,567
1
000
Bytes 0000–1,399
Fragment 1
1,420
14,567
1
175
Bytes 1,400–2,799
Fragment 2
1,220
14,567
0
350
Bytes 2,800–3,999
Fragment 3
820
14,567
1
175
Bytes 1,400–2,199
Fragment 2.2
620
14,567
1
275
Bytes 2,200–2,799
Fragment 2.1

Internet Control Message Protocol (ICMP)

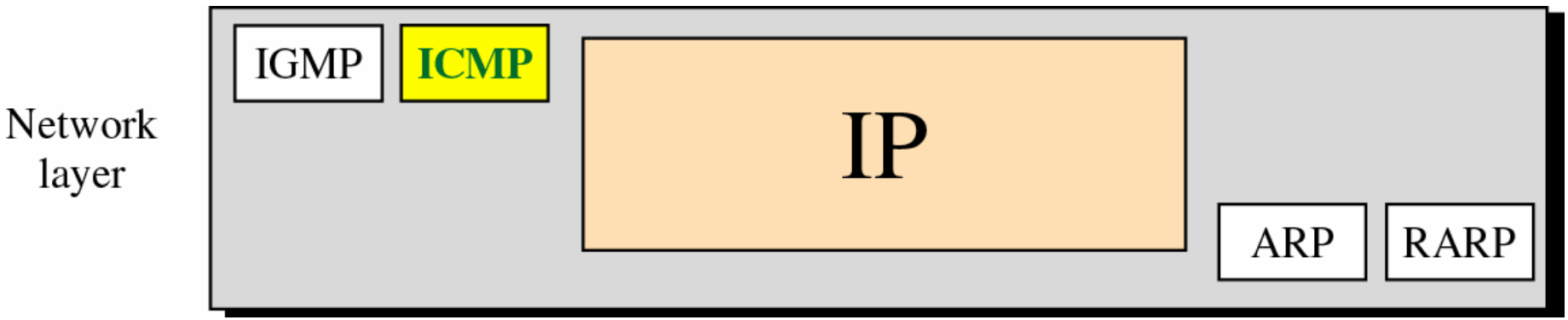
Overview

- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
  - Control functions (ICMP)
  - Multicast signaling (IGMP)



Internet Control Message Protocol (ICMP)

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
  - Error reporting
  - Simple queries
- ICMP is a mechanism used by the host and router to send notification of datagram problems back to the sender.
- If delivery of DG is not possible, ICMP allows it to inform the original source.
- ICMP reports only to the original source.


Network layer
IGMP
ICMP
IP
ARP
RARP

- ICMP Only Report problem, not correct them.
- it is an integral part of IP.
- it is typically not used to send and receive data between end systems like TCP/UDP.
- ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4.
- IPv6 has a similar protocol, ICMPv6.

- ICMP messages are constructed at the IP layer.
- IP encapsulates the appropriate ICMP message with IP header.
- For example--time to live (TTL).

ICMP HEADER FORMAT

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
ADDITIONAL INFORMATION		

Each ICMP message contains three fields

1. TYPE→ field identifies the ICMP message.

2.CODE→ field provides further information about the associated TYPE field OR subtype of message.

3. CHECKSUM→ provides a method for determining the integrity of the message. similar to IP header checksum.

If there is no additional data, 4 bytes set to zero.

The TYPES defined are:

TYPE	Description
0	Echo Reply
1 & 2	IS RESERVED.
3	Destination Unreachable
4	Source Quench
5	Redirect Message
6	
7	RESERVED.
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request

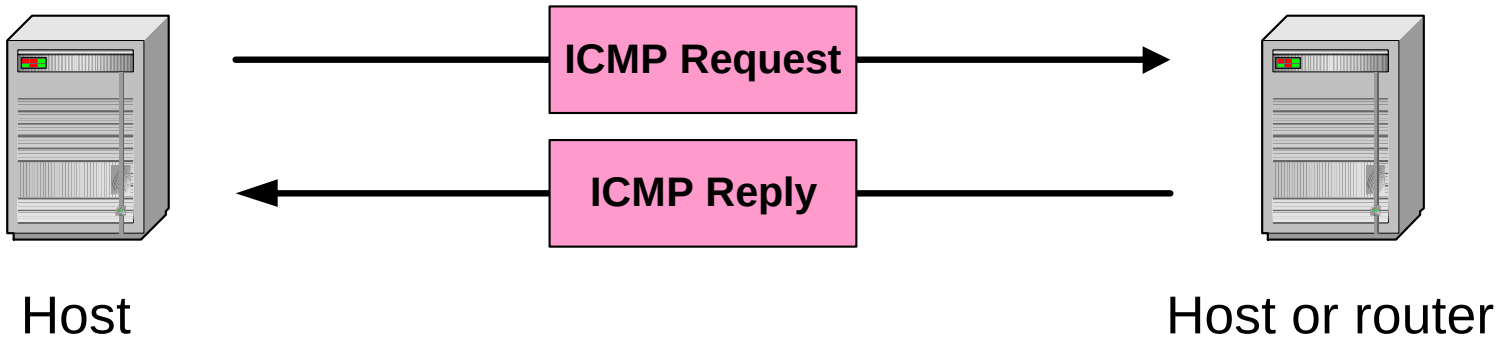
Frequent ICMP Error message

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

Example of ICMP Queries

Type/Code:	Description	
8/0	Echo Request	The ping command uses Echo Request/ Echo Reply
0/0	Echo Reply	
13/0	Timestamp Request	
14/0	Timestamp Reply	
10/0	Router Solicitation	
9/0	Router Advertisement	

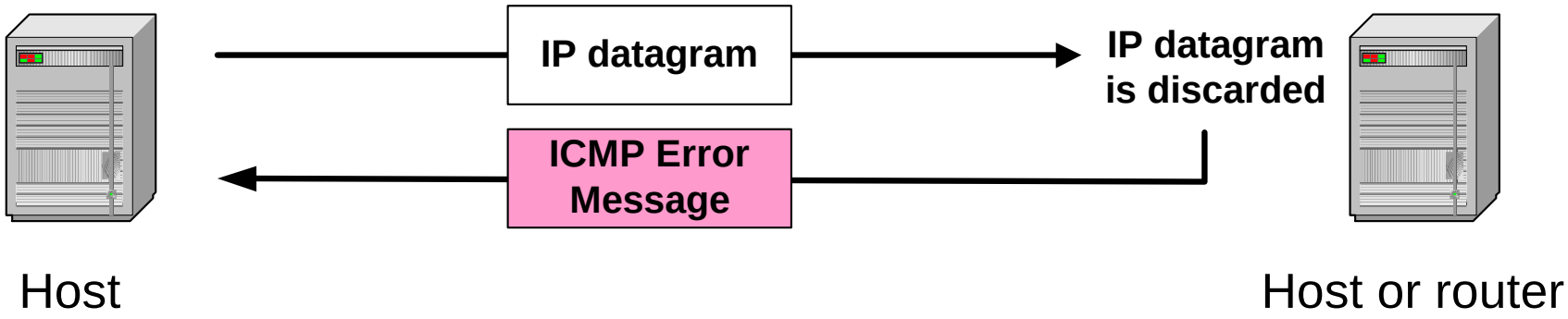
ICMP Query message



ICMP query:

- Request sent by host to a router or host
- Reply sent back to querying host

ICMP Error message



- **ICMP error messages report error conditions**
- **Typically sent when a datagram is discarded**
- **Error message is often passed from ICMP to the application program**

- **Destination Unreachable→** When a packet is undeliverable, a Destination Unreachable, Type 3, ICMP is generated. Type 3 ICMPs can have a Code value of 0 to 15:

Type 3

Code Value Description

0 Network Unreachable

1 Host Unreachable

2 Protocol Unreachable

3 Port Unreachable

4 Fragmentation needed and DF (Don't Fragment) set

5 ---

6 ---

7 ----

8 -----

15 Source route failed

Some subtypes of the “Destination Unreachable”

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

- **Echo Request & Echo Reply→** This is the ICMP most used to test IP connectivity commonly known as PING.
- The Echo Request ICMP will have a Type field of 8 and a Code field of 0.
- Echo Replies have a Type field of 0 and a Code field of 0.
- Ask a machine if it is alive.

- **Source Quench→** An ICMP Source Quench message has a Type field of 4 and Code 0.
- Source Quench messages are sent when the destination is unable to process traffic as fast as the source is sending it.
- The Source Quench ICMP tells the source to cut back the rate at which it is sending data.
- continue generate Source Quench ICMPs speed.

- **Redirect Message→** An intermediary device will generate an ICMP Redirect Message when it determines that a route being requested can be reached either locally or through a better path.
- Redirect Message ICMPs are Type 5 and are further defined by the following Code field values.
- Teach a router about geography.

Type 5

Code Value	Description
0	Redirect datagrams for the Network
1	Redirect datagrams for the Host
2	Redirect datagrams for the Type of Service and Network
3	Redirect datagrams for the Type of Service and Host.

- **Time Exceeded→** If a router or host discards a packet due to a time-out, it will generate a Time Exceeded Type 11 ICMP.
- The Time Exceeded ICMP will have a Code value of either 0 or 1.
- A Code 0 is generated when the hop count of a datagram is exceeded and the packet is discarded.
- A Code 1 is generated when the reassemble of a fragmented packet exceeds the time-out value.

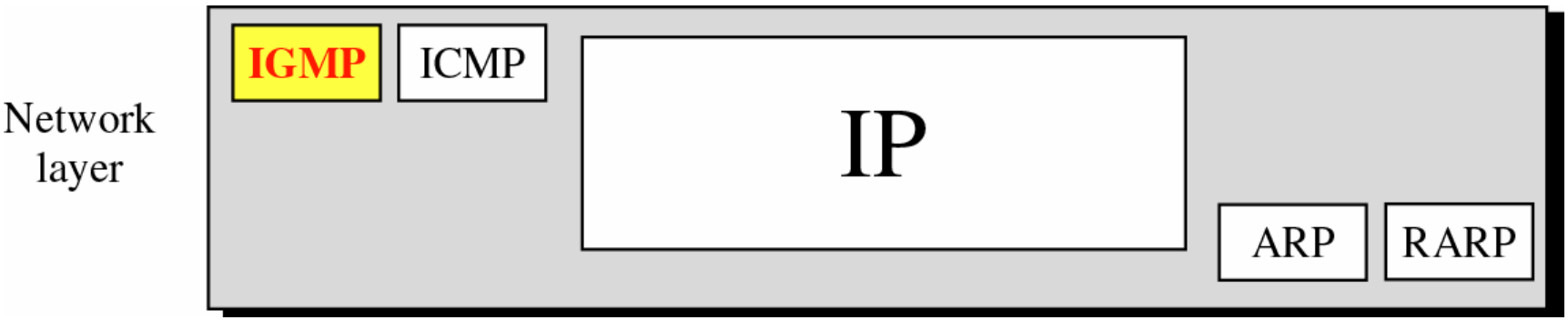
- **Parameter Problem**
- Invalid header field, an ICMP 12 is generated.
- For missing option, the ICMP will have a Code value 1.
- For invalid field, code value is 0.

Timestamp Request & Timestamp Reply

- Like as Echo request and reply, but with timestamp.
- synchronizing the time maintained on different devices.
- Network performance.
- The Request has a Type field of 13 and the Reply is Type 14.
- This method for time synchronization is crude and unreliable. Therefore, it is not heavily used.

Internet Group Management Protocol (IGMP)

Position of IGMP in the network layer

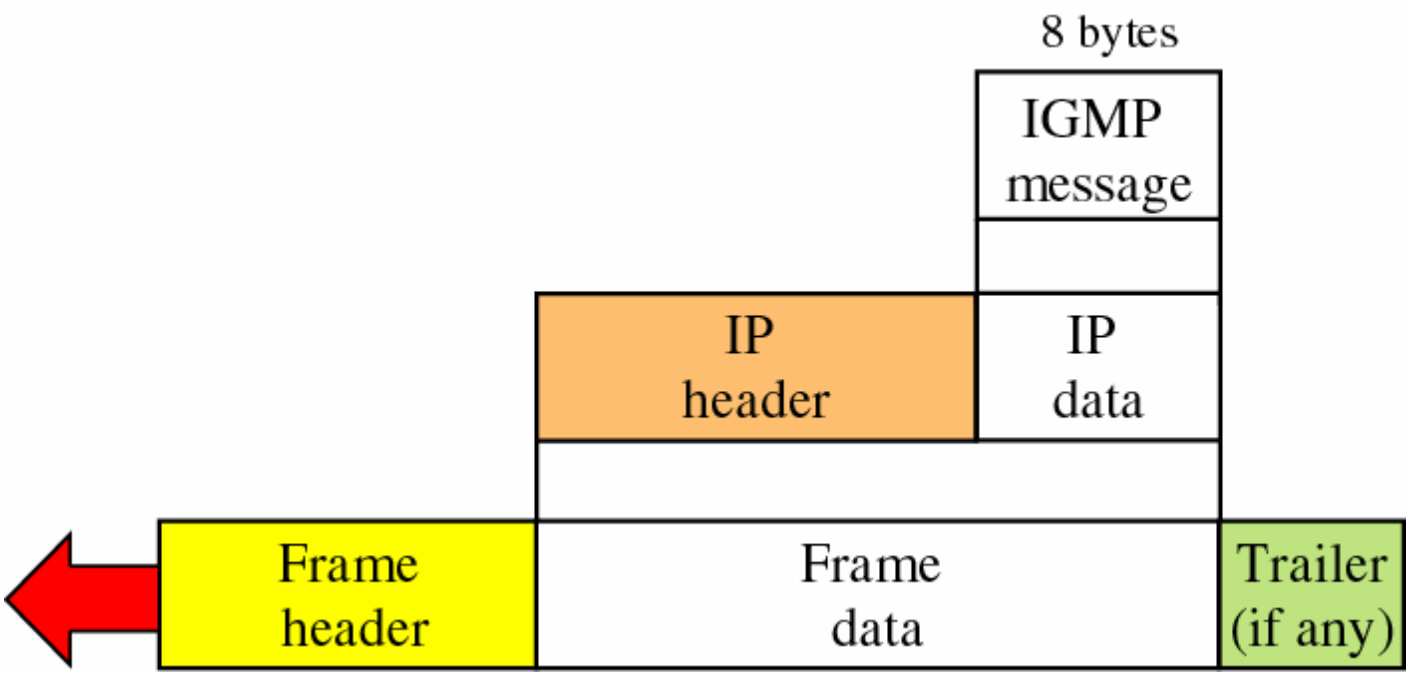


- The Internet Group Management Protocol (IGMP) is a communication protocol used to manage the membership of Internet Protocol multicast groups.
- Multicasting allows a host to transmit an IP datagram to a set of hosts that form a multicast group.
- Used in mapping of class D network.

- IGMP is used by IP host and adjacent multicast routers .
- It is an integral part of the IP_multicast specification, operating above the network layer.
- Not_like_TCP/UDP.
- only needed for IPv4 networks.

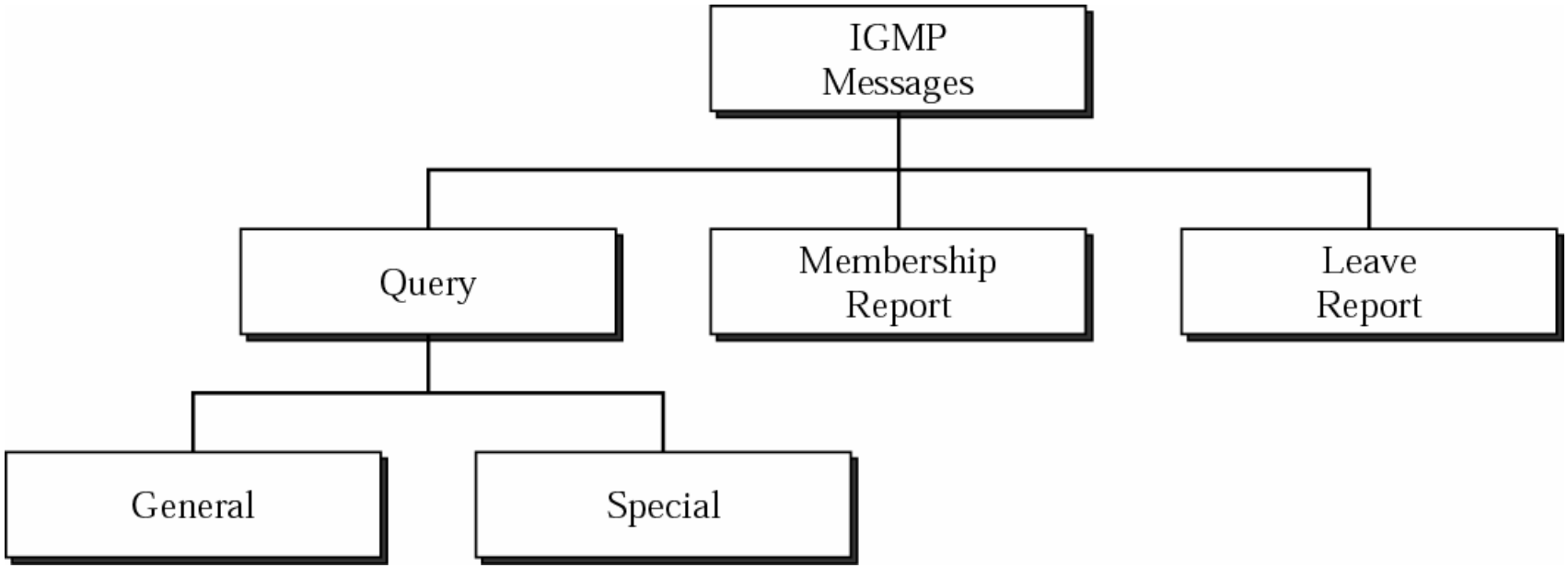
- The IGMP message is encapsulated in an IP datagram, which is itself encapsulated in a frame.
- The IP packet that carries an IGMP packet has a value of 2 in its protocol field.

Encapsulation of IGMP packet

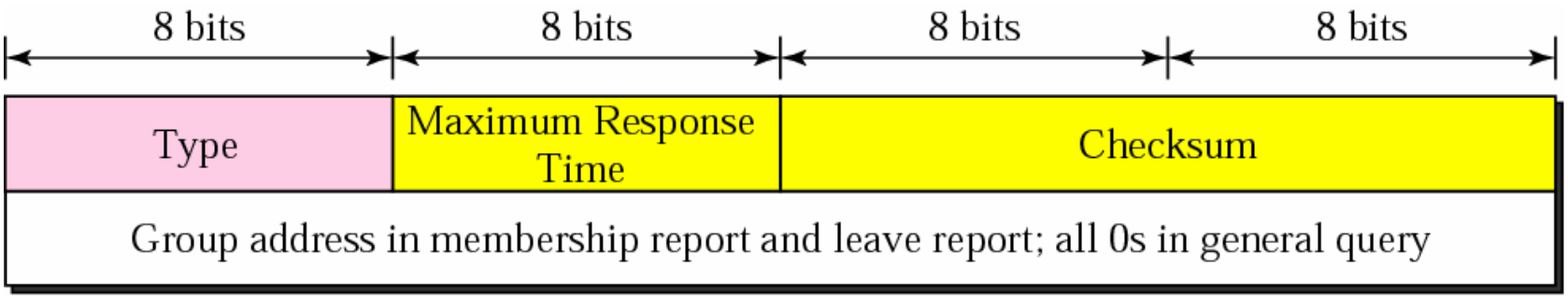


- Membership in a multicast group is dynamic.
- IGMP can be used for online streaming video and gaming, and allows more efficient use of resources.
- IGMP does allow some attacks, and firewalls.

IGMP message types



IGMP message format



- Max Resp Time → specifies the time limit for the corresponding report.
- Used only in query messages.
- In all other messages, it is set to 0 by the sender and ignored by the receiver.
- Checksum →This is the 16-bit one's complement of the sum of the entire IGMP message.
- Group Address → The field is zeroed when sending a General Query.

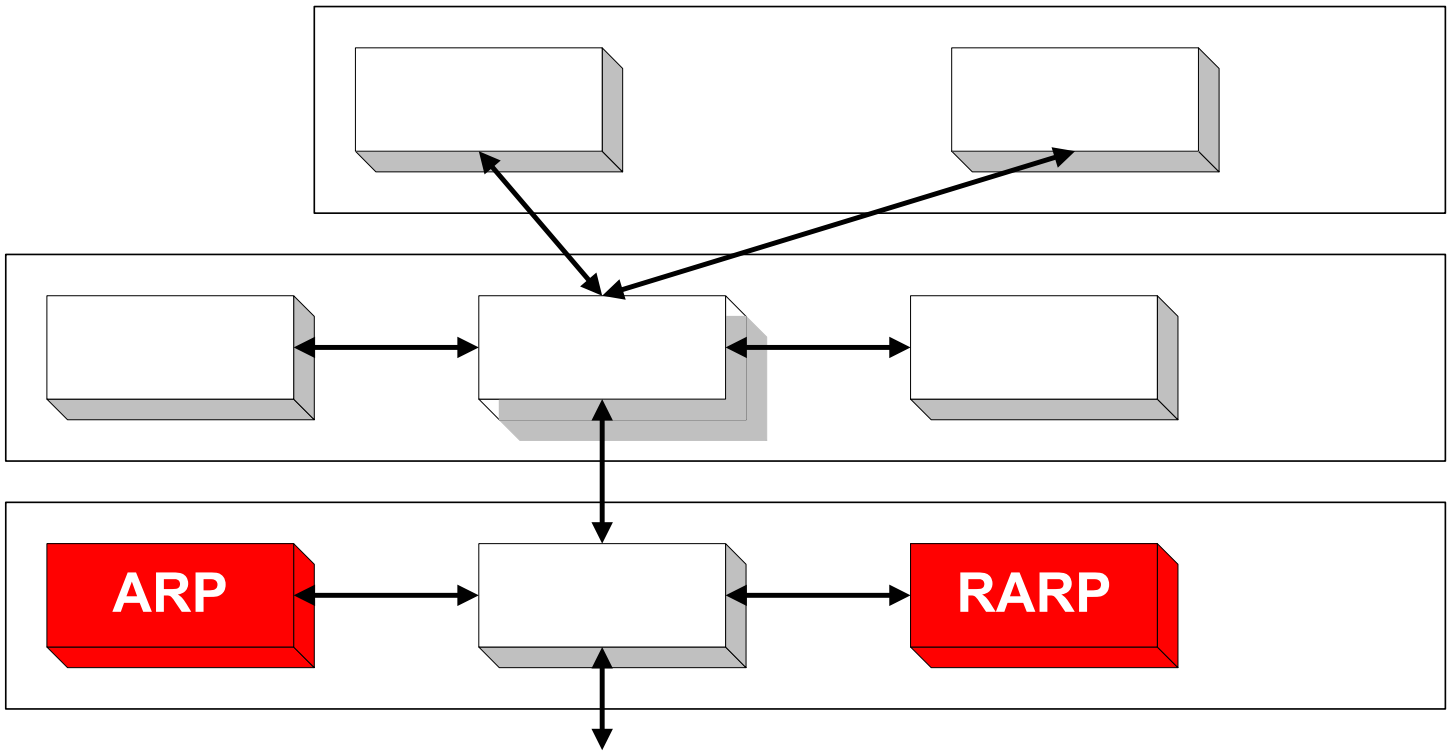
IGMP type field

Type	**value**
General Or Special	11 OR 00010001
Membership Report	16 OR 00010110
Leave Report	17 OR 00010111

ARP and RARP

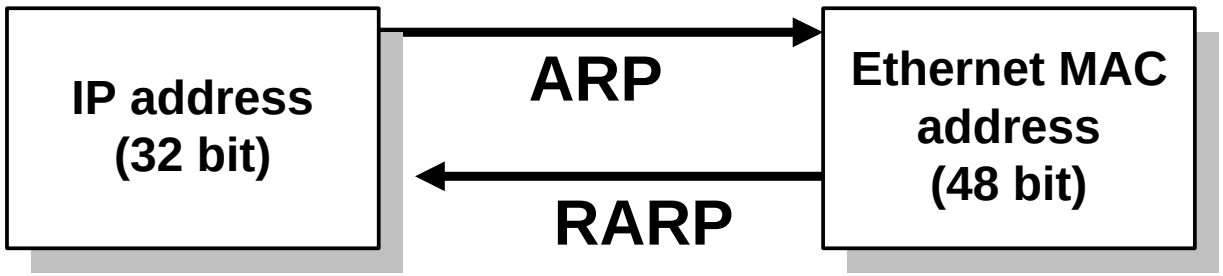
Address Resolution Protocol (ARP)

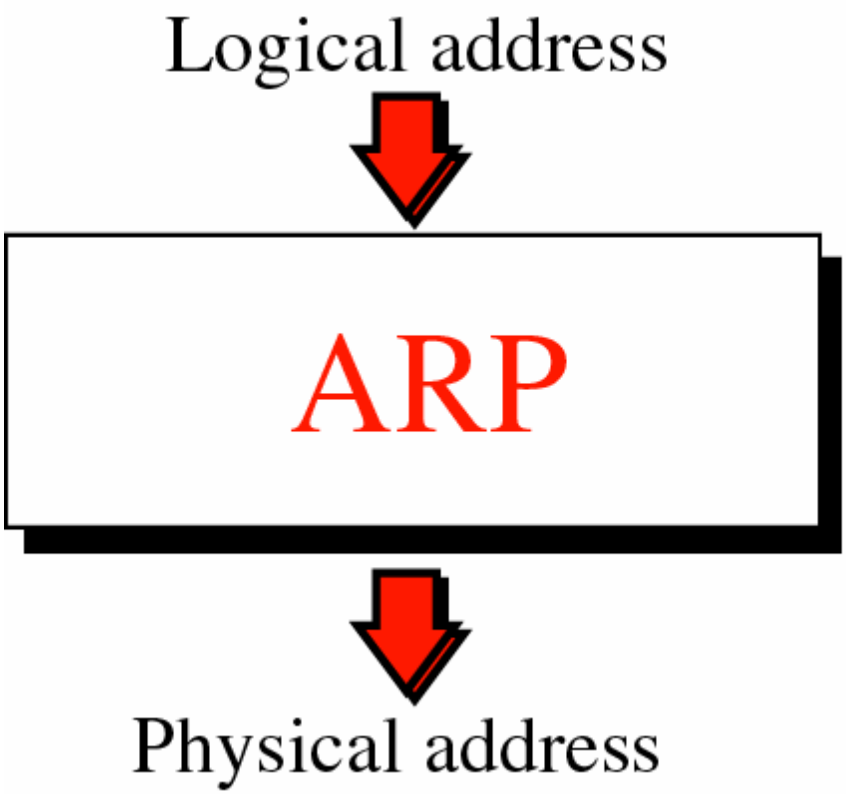
Overview

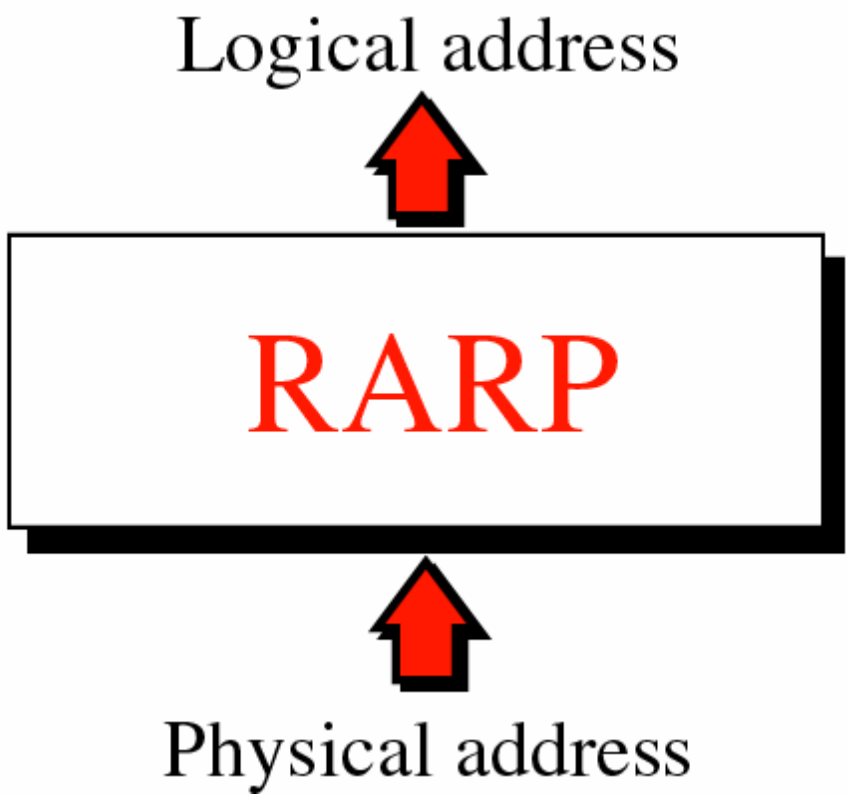


- Note:
  - The Internet is based on IP addresses
  - Data link protocols (Ethernet, FDDI, ATM) may have different (MAC) addresses
- The ARP and RARP protocols perform the translation between IP addresses and MAC(medium access control) layer addresses.

- MAC→ The address of a device used at the DLL.(MAC)
- Ethernet → a LAN using CSMA/CD access method.

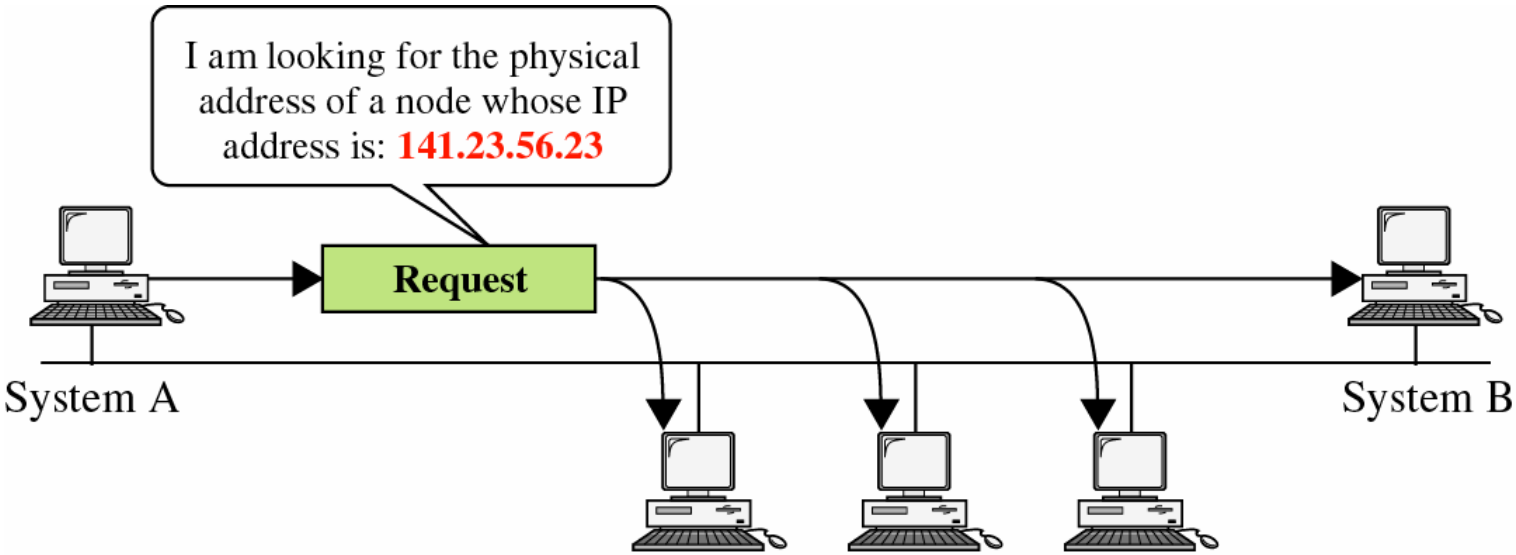

IP address
(32 bit)
ARP
RARP
Ethernet MAC
address
(48 bit)


Logical address
ARP
Physical address

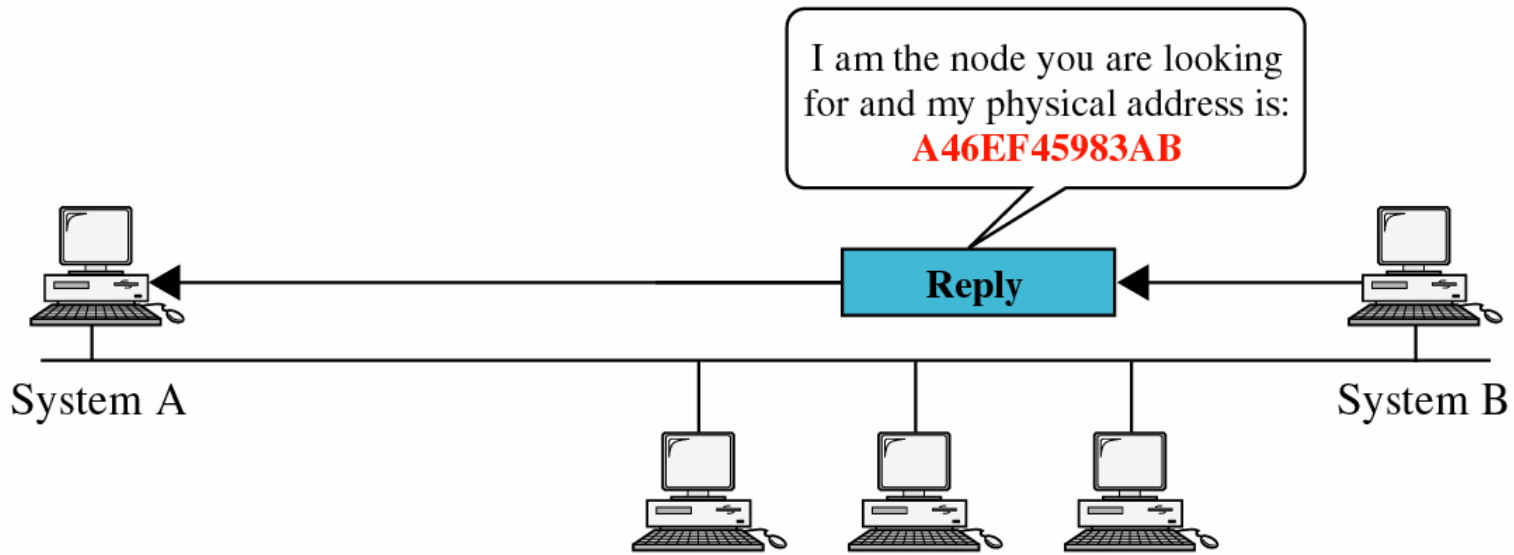

Logical address
RARP
Physical address

ARP Protocol

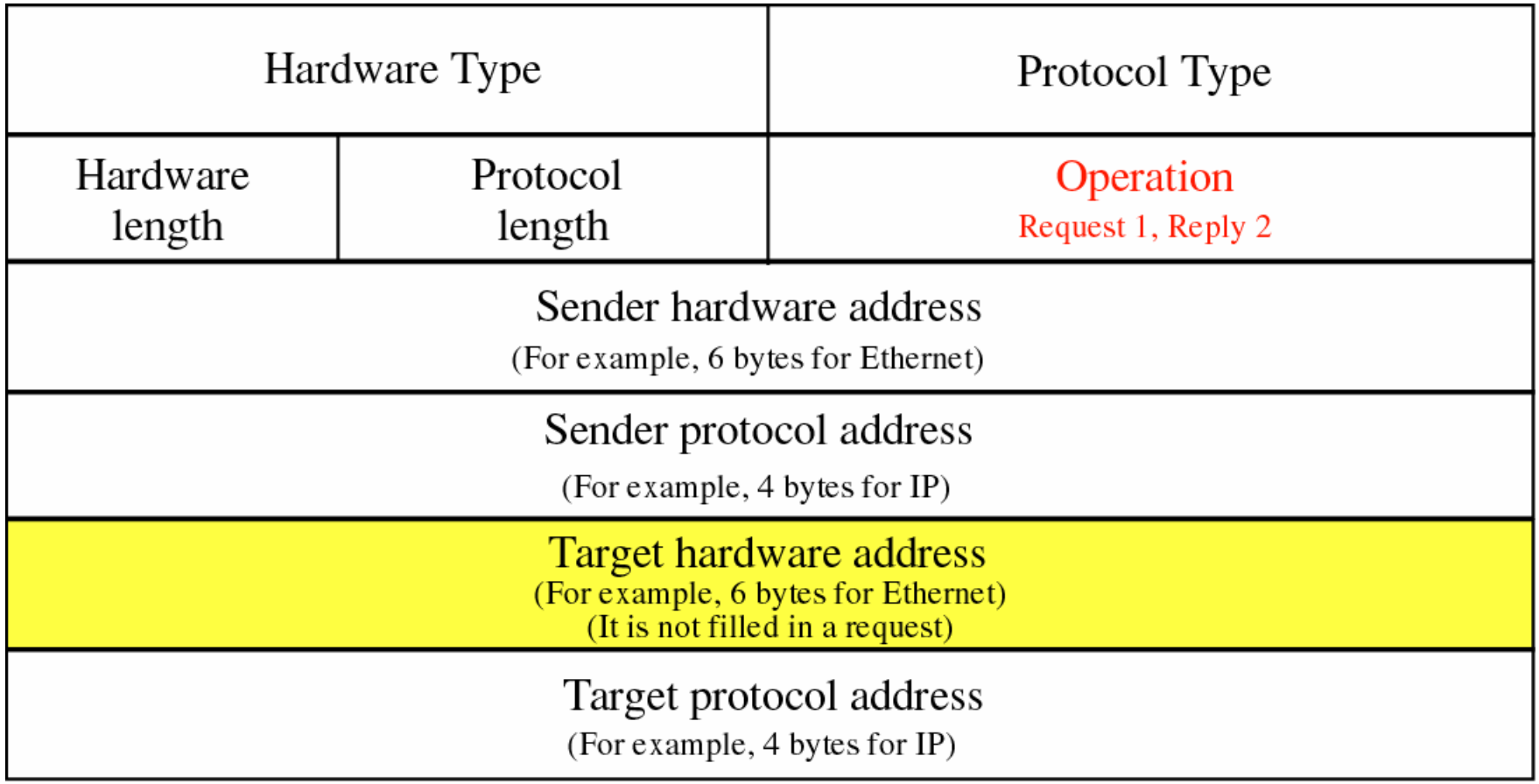
- Machine A wants to send a packet to B, but A only knows B's IP address
- Machine A broadcasts ARP request with B's IP address
- All machines on the local network receive the broadcast
- Machine B replies with its physical address
- Machine A adds B's address information to its table
- Machine A delivers packet directly to B



a. ARP request is broadcast



b. ARP reply is unicast


Hardware Type
Protocol Type
Hardware length
Protocol length
Operation
Request 1, Reply 2
Sender hardware address
(For example, 6 bytes for Ethernet)
Sender protocol address
(For example, 4 bytes for IP)
Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)
Target protocol address
(For example, 4 bytes for IP)

- Hardware type (HTYPE) →Each data link layer protocol is assigned a number used in this field. For example, Ethernet is 1.
- Protocol type (PTYPE) →Each protocol is assigned a number used in this field. For example, IPv4.
- Hardware length (HLEN) →Length in bytes of a hardware address. Ethernet addresses are 6 bytes long.

- Protocol length (PLEN) →Length in bytes of a logical address. IPv4 address are 4 bytes long.
- Operation →Specifies the operation the sender is performing: 1 for request, 2 for reply, 3 for RARP request, and 4 for RARP reply.

- Sender hardware address (SHA) →Hardware address of the sender. (first 32 bit)
- Sender protocol address (SPA) →Protocol address of the sender.
- Target hardware address (THA) →Hardware address of the intended receiver. This field is ignored in requests. (last 32 bit)
- Target protocol address (TPA) → Protocol address of the intended receiver.

ARP Caching

- To reduce communication cost, computers that use ARP maintain a cache of recently acquired IP-to-physical address bindings.
- Each entry has a timer (usual timeout period is 20 minutes)
- The sender's IP-to-address binding is included in every ARP broadcast; receivers update the IP-to-physical address binding information in their cache before processing an ARP packet.

Introduction to LAN with its cables, connectors, Switches, Hubs and topologies

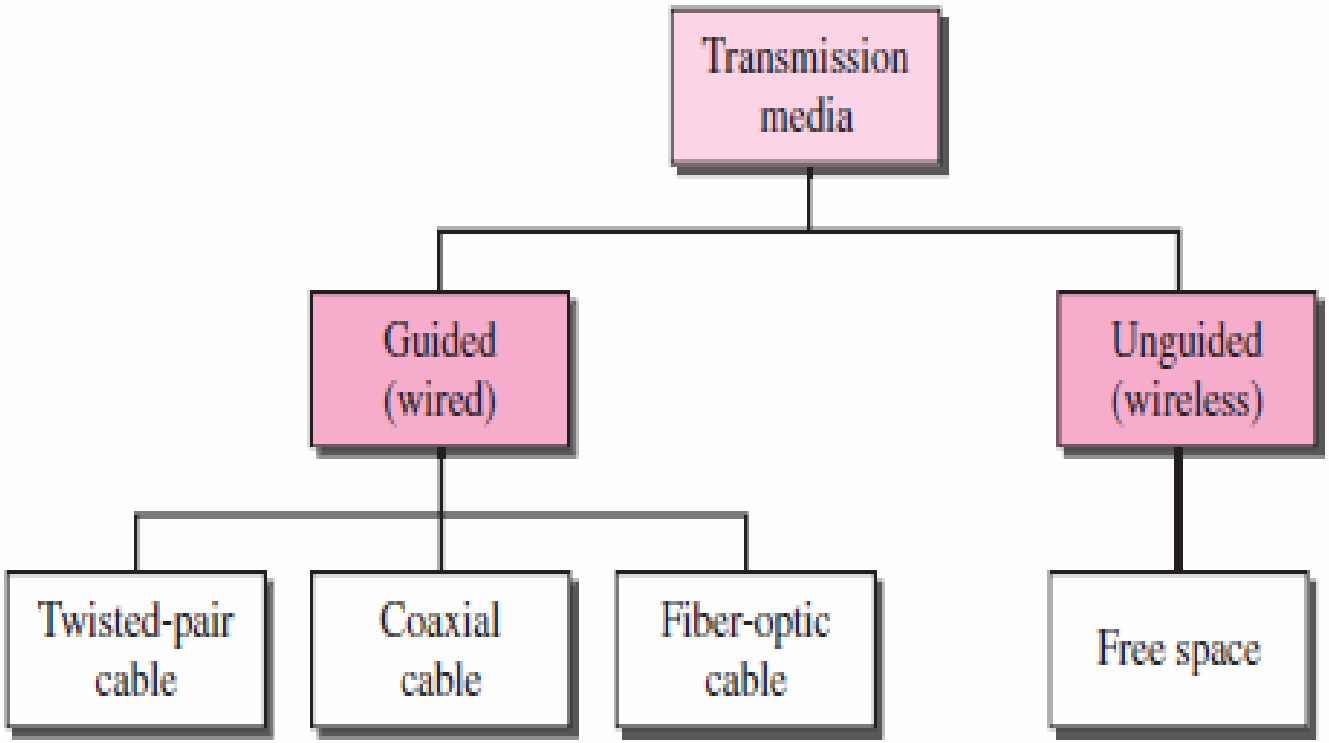
LAN

- Small interconnected computers or workstations within a building or small area up to 10 Kms.
- Small group of workers that share common application programs and communication needs.
- LANs are capable of very high transmission rates (100s Mb/s to G b/s).
- LAN is interconnected with other networks via switches and router/gateways.
- In general, a given LAN will use only one type of transmission medium.

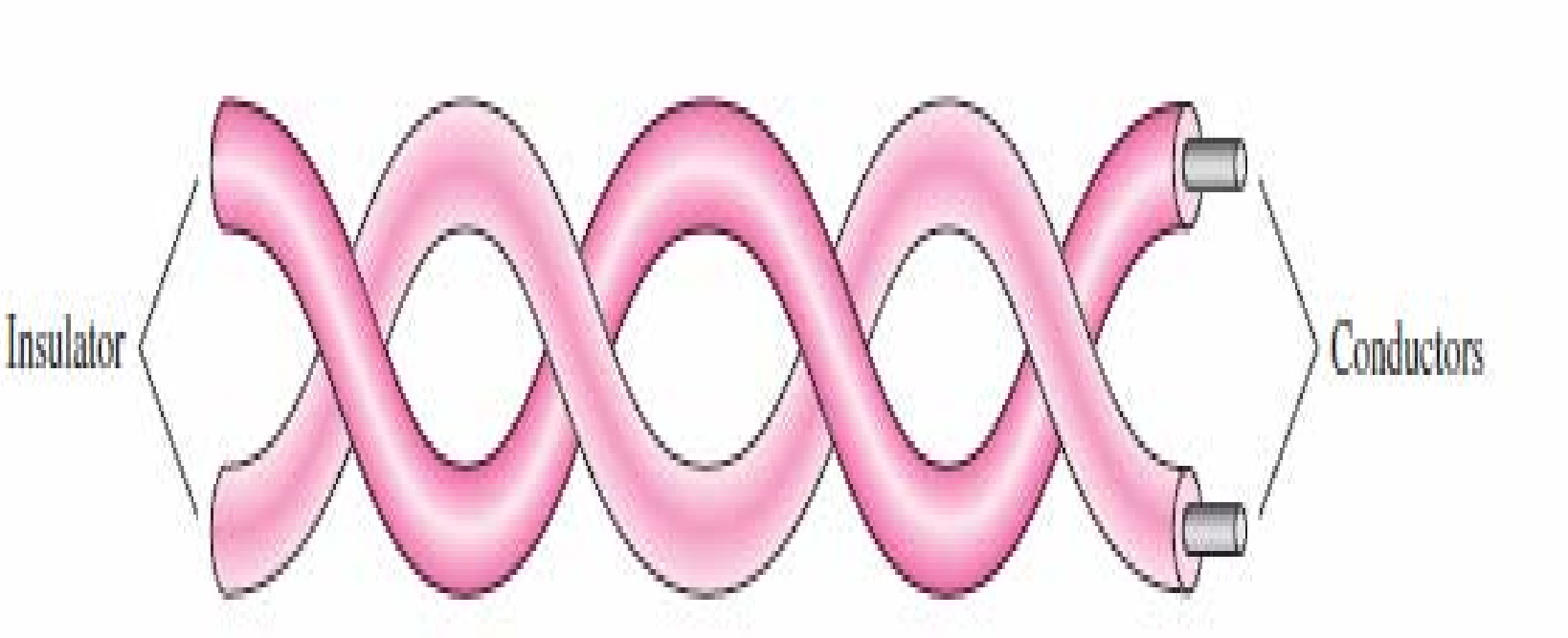
Basic transmission medium concepts

- Medium is the physical path between transmitter and receiver in a data transmission system.
- Guided Medium: waves are guided along a solid medium path.
- Unguided medium: waves are propagated through the atmosphere and inner/outer space.

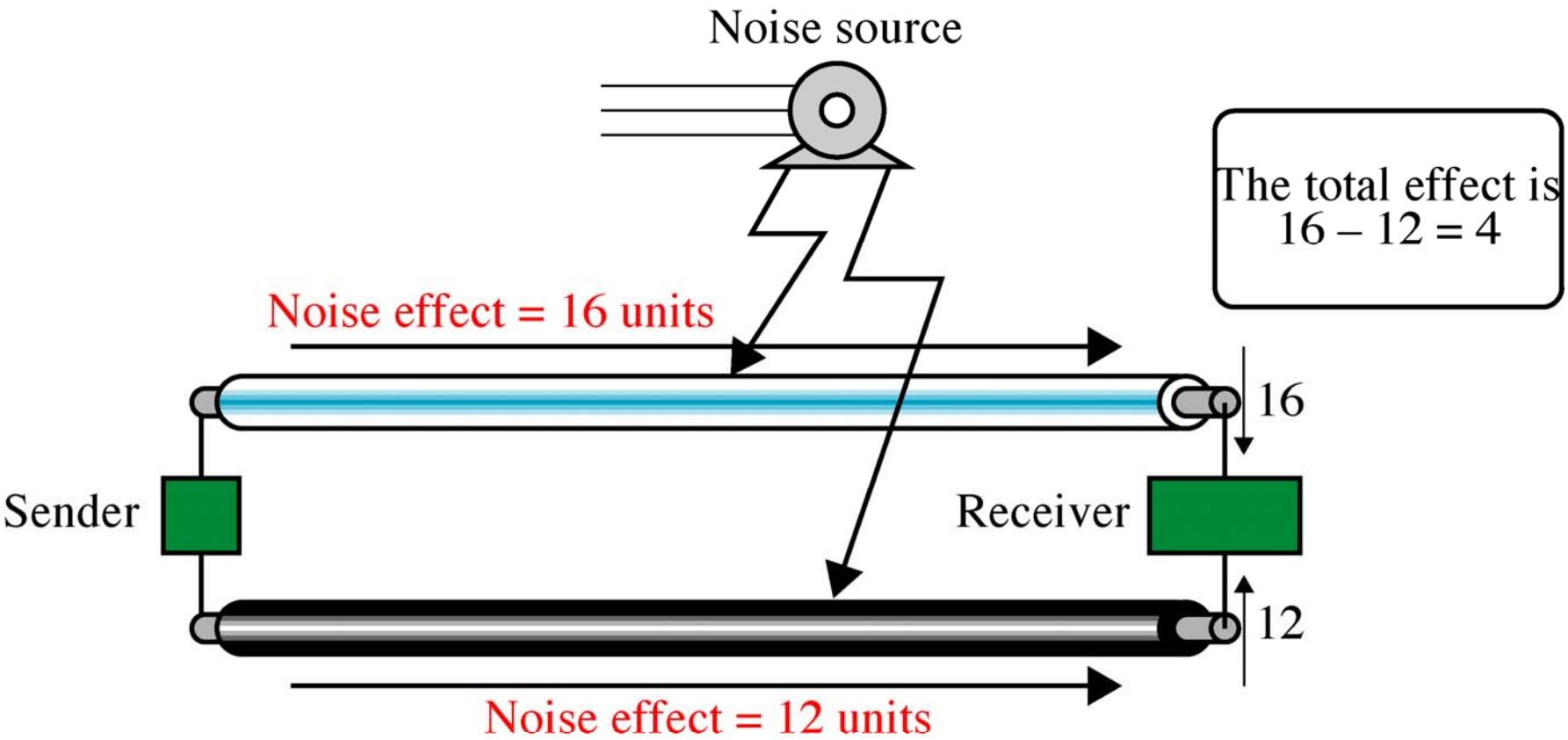
Transmission medium



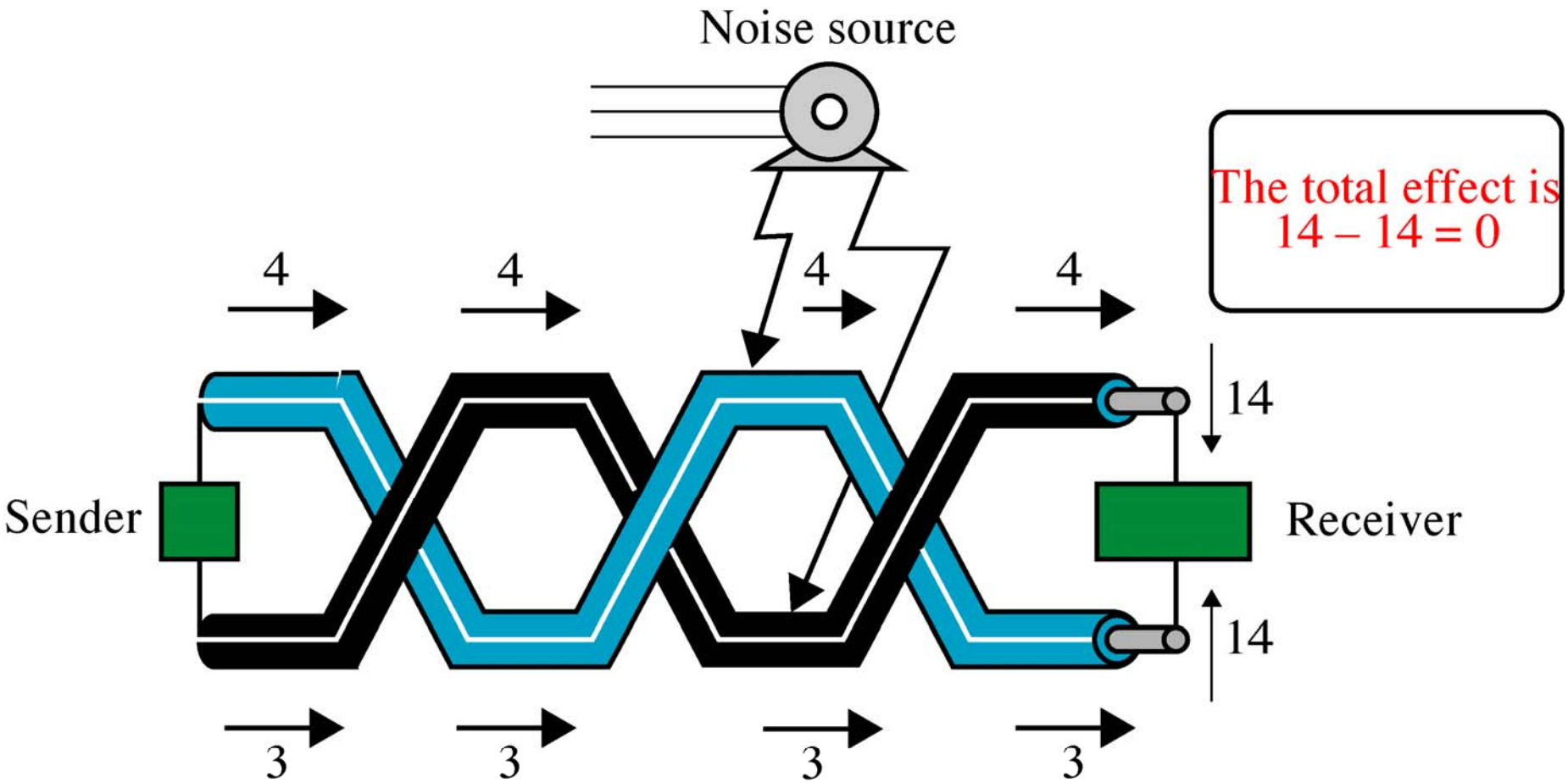
Twisted-pair cable



Effect of Noise on Parallel Lines



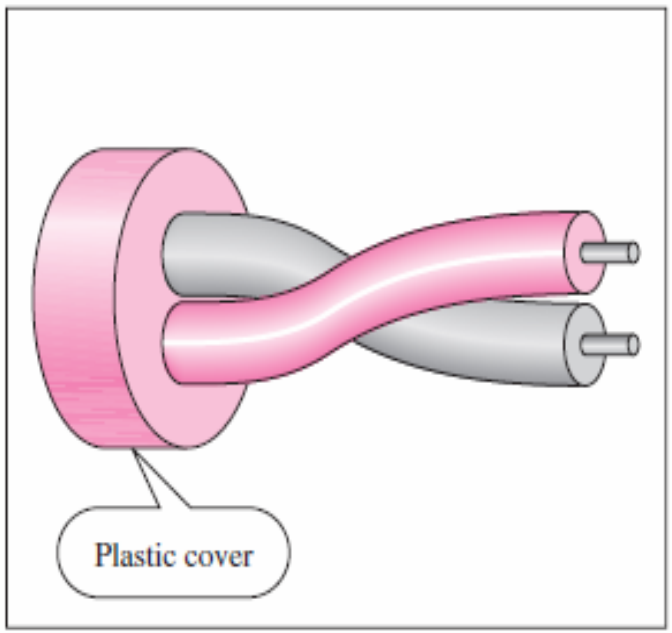
Noise on Twisted-Pair Lines



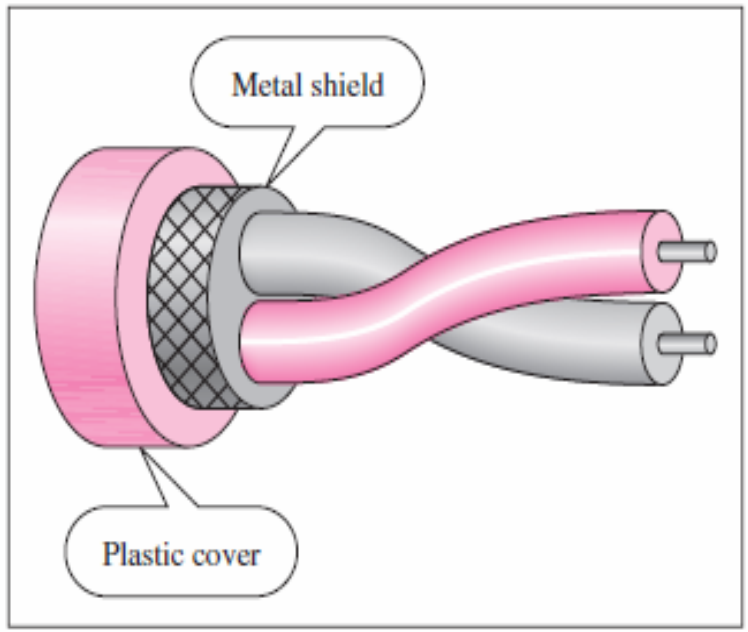
Twisted-pair cable

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther).
- By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk).
- This means that the receiver, which calculates the difference between the two, receives no unwanted signals.

Types of *Twisted-pair cable*



a. UTP



b. STP

Frequency range

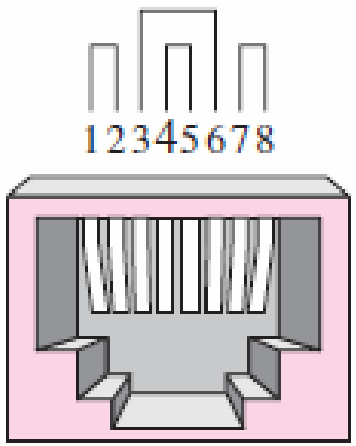
- 100Hz-5MHz

Applications

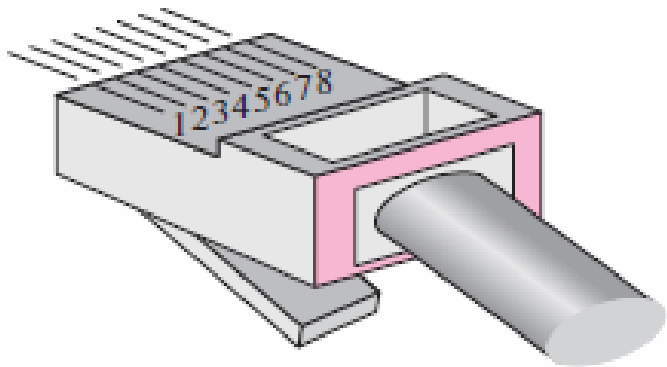
- Common in building for digital signaling used at speed of 10's Mb/s (CAT3) and 100Mb/s (CAT5) over 100s meters.
- Common for telephone interconnection at home and office buildings
- Less expensive medium; limited in distance, bandwidth, and data rate.

Connector

- The most common UTP connector is **RJ45** (RJ stands for registered jack)
- It is a keyed connector, meaning the connector can be inserted in only one way.
- It has 8 wires.



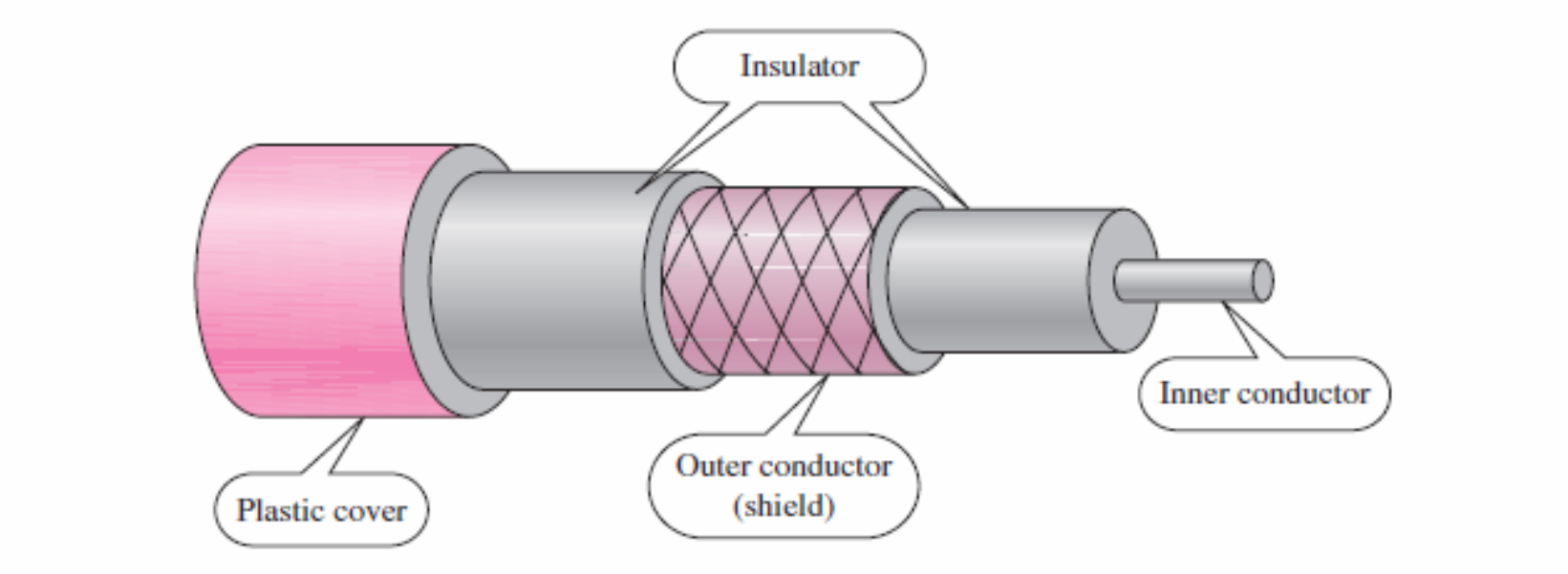
RJ-45 Female



RJ-45 Male

Coaxial Cable

- Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twisted pair cable.



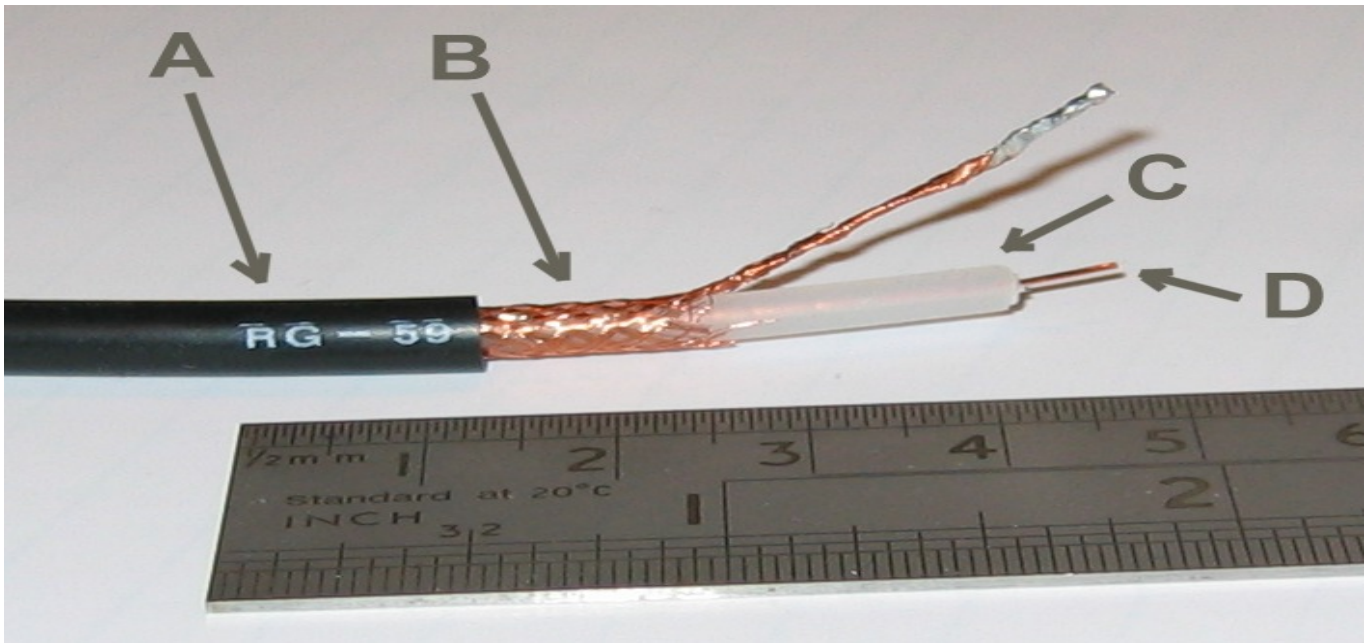
Frequency range

- 100 KHz-500MHz

Categories of coaxial cables

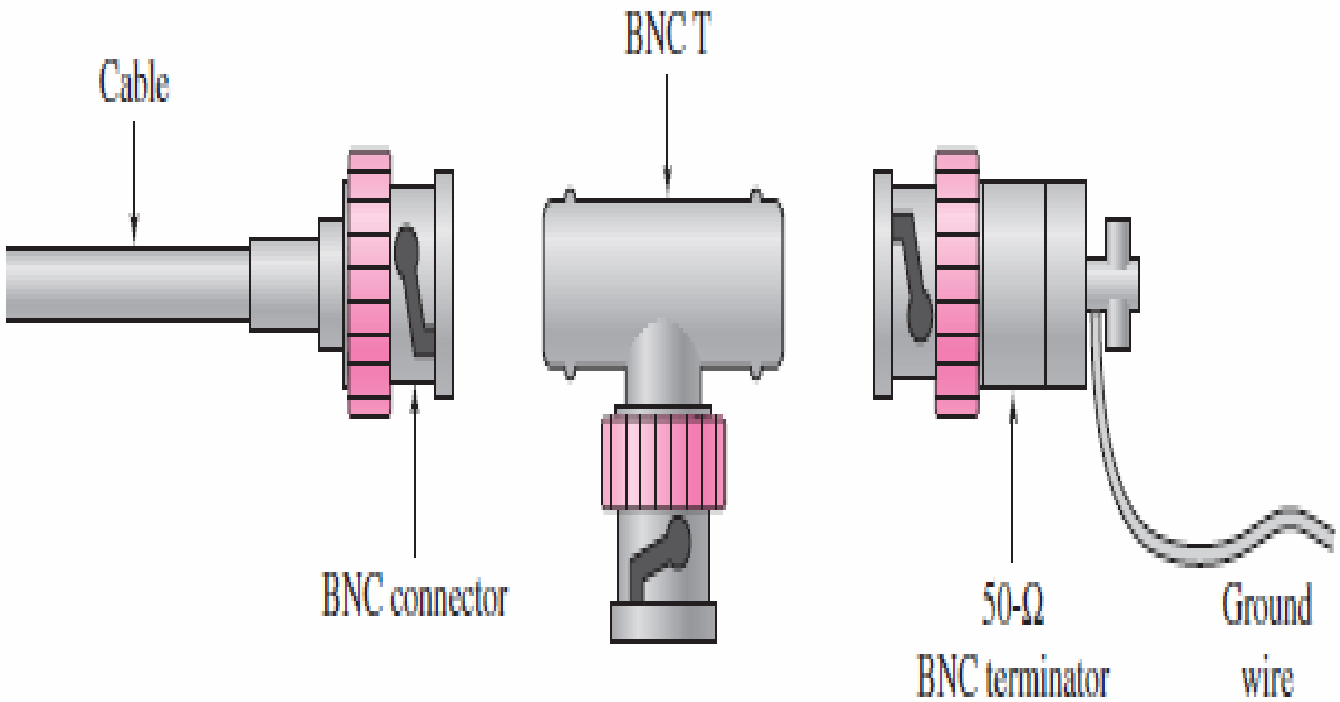
Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

A section of RG-59 cable with its end stripped.
A: outer plastic sheath
B: copper braid shield
C: inner dielectric insulator
D: copper core



Coaxial Cable Connectors

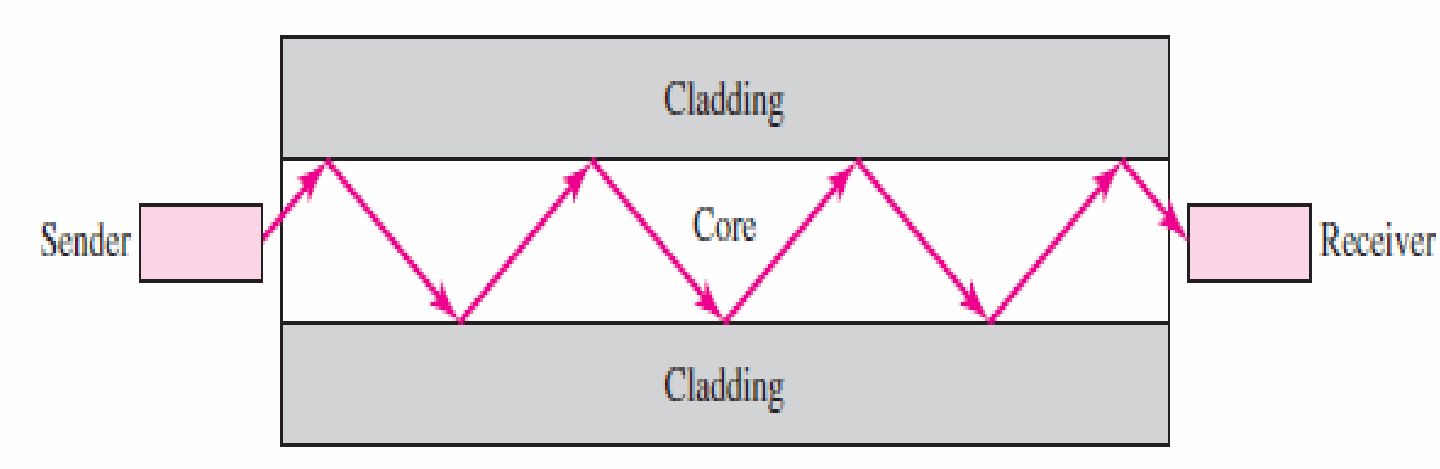
- **Bayone-Neill-Concelman (BNC)**
- BNC T connector,
- BNC terminator


Cable
BNC T
BNC connector
50-Ω
BNC terminator
Ground
wire

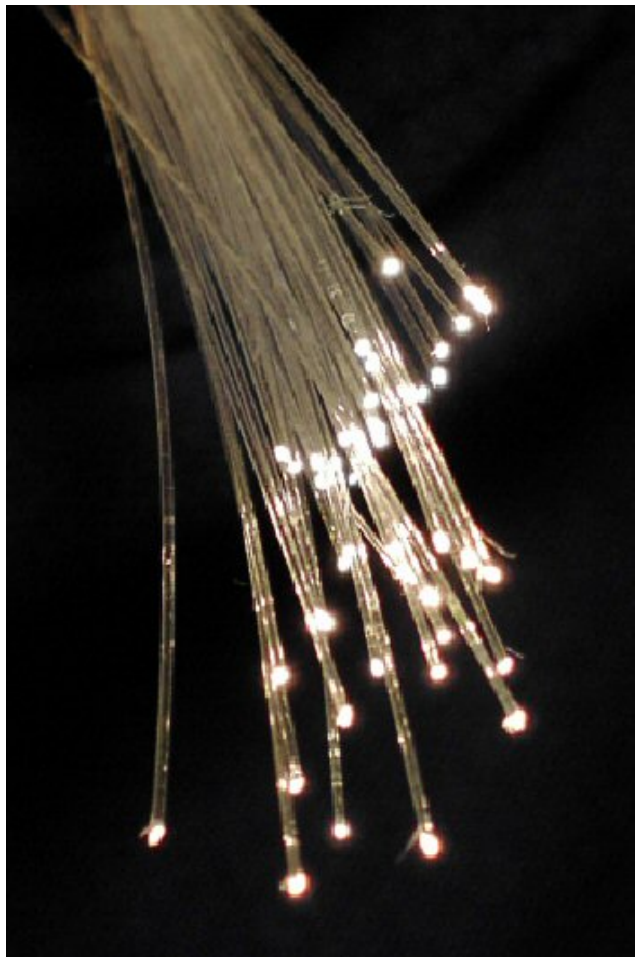
BNC(British Naval Connector)

Fiber-optics

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light



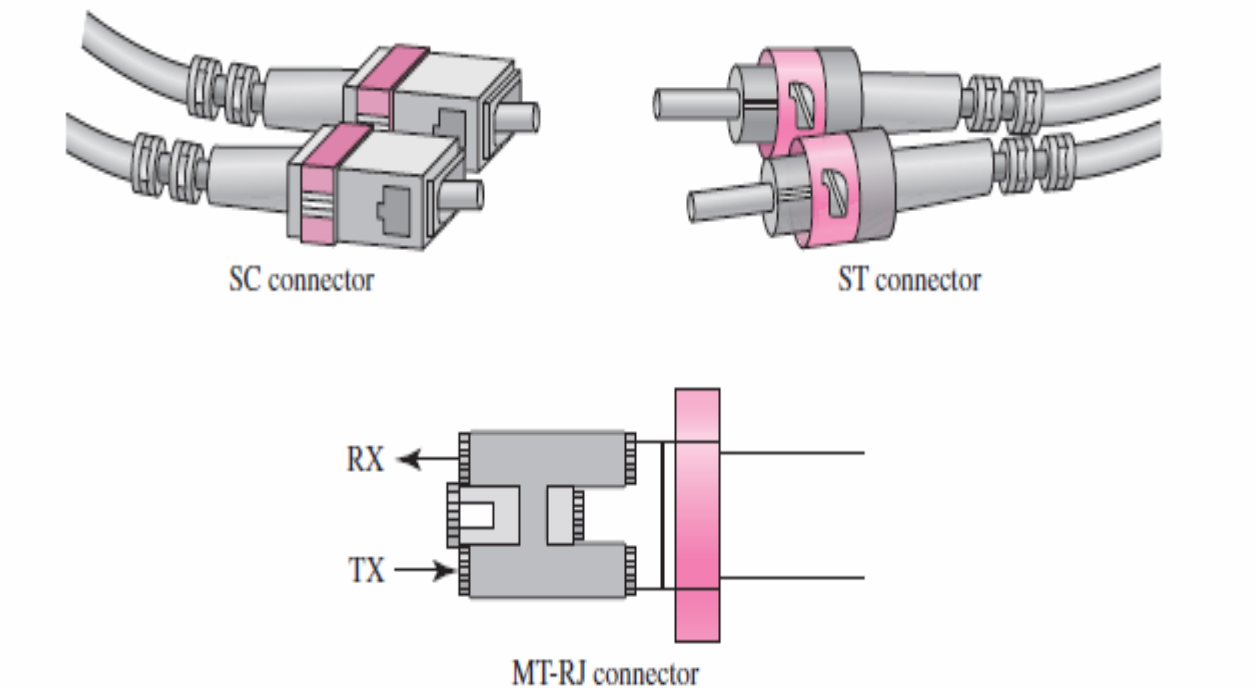
Fiber-optics



Fiber-optics

- Optical fibers use reflection to guide light through a channel. A glass or plastic **Core** is surrounded by a **cladding** of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Fiber optics cable connector



Connectors

- The **subscriber channel (SC) connector** is used for cable TV. It uses a push/pull locking system.
- The **straight-tip (ST) connector** is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.
- **MT-RJ** is a connector that is the same size as RJ45.

Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.

Advantages

- **SPEED:** Fiber optic networks operate at high speeds - up into the gigabits.
- **BANDWIDTH:** large carrying capacity.
- **DISTANCE:** Signals can be transmitted further without needing to be "refreshed" or strengthened.
- **RESISTANCE:** Greater resistance to electromagnetic noise such as radios, motors or other nearby cables.
- **MAINTENANCE:** Fiber optic cables costs much less to maintain.

Disadvantages

Installation and maintenance.

- Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

Unidirectional light propagation.

- Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

Cost.

- The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

connectivity

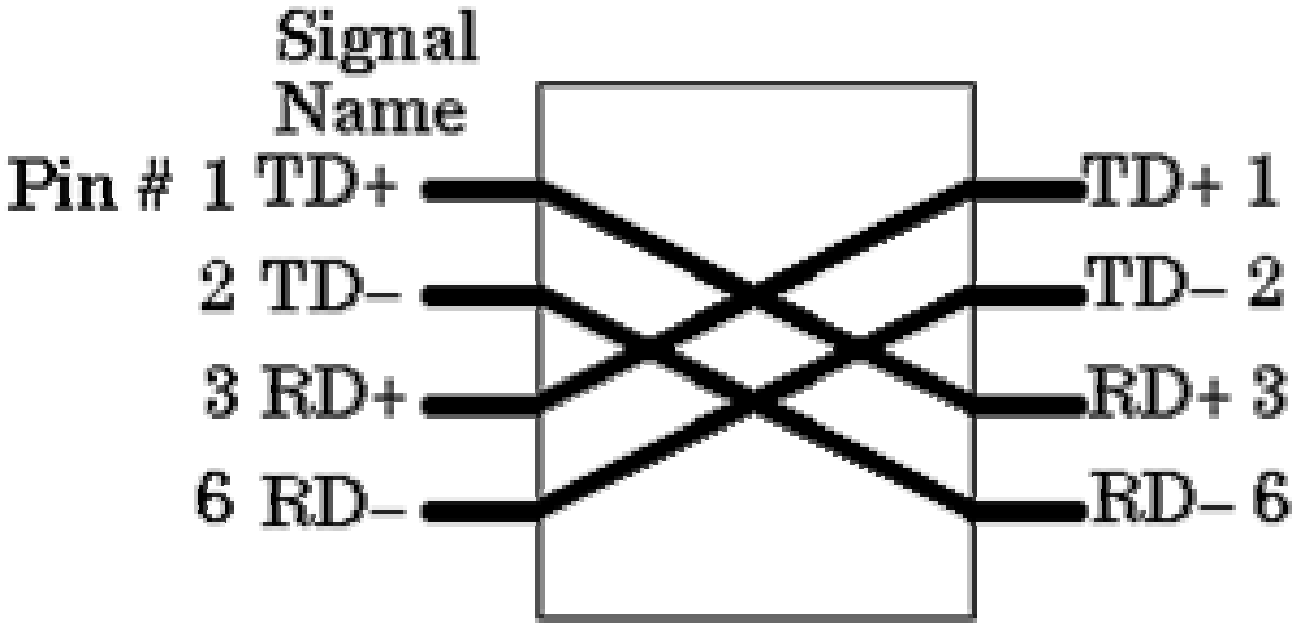
Connection can be made between

- Computer-computer
- Computer-hub
- Hub-hub
- Hub-switch
- Switch-switch

Straight-through cable

- *Straight-through cable* is a type of twisted pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same *pinout* (i.e., arrangement of conductors).
- Straight-through cable is also commonly referred to as *patch cable.*
- Straight-through cable is used to connect computers and other end-user devices (e.g., printers) to networking devices such as hubs and switches

Cross over cable



Cross over cable

- It is generally used to connect similar devices.
- Such as hub-hub, switch-switch.

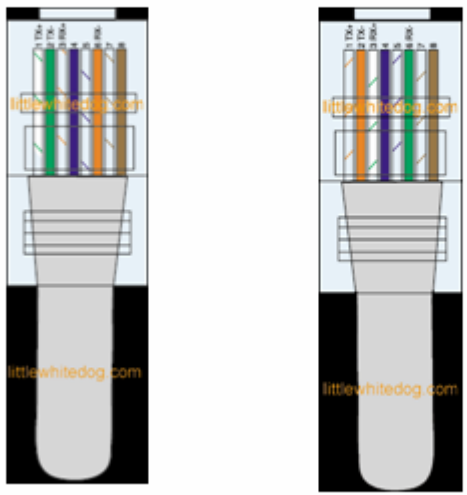
Roll over cable

- You can identify a roll-over cable by comparing the two modular ends of the cable.
- Holding the cables side-by-side, with the tab at the back, the wire connected to the pin on the outside of the left plug should be the same color as the wire connected to the pin on the outside of the right plug.

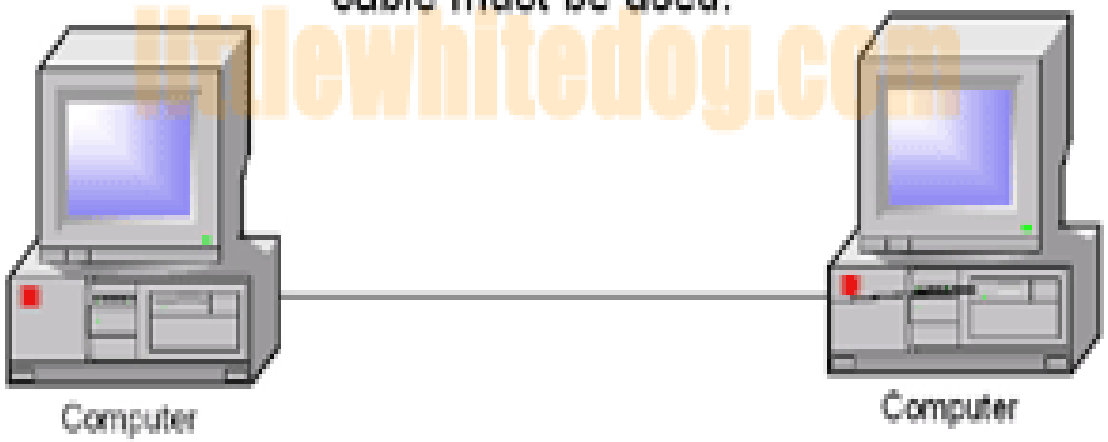
Roll over cable

Conn 1	conn2
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

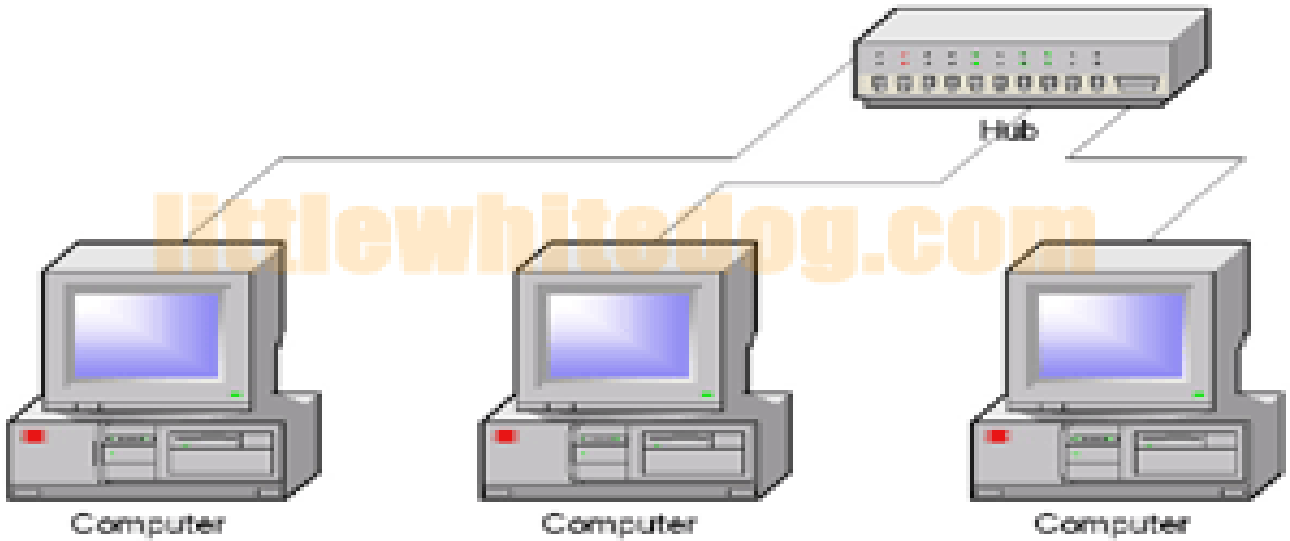
Cross cable



When connecting two computers together without the use of a hub or switch, a "Crossover Cable" cable must be used.



When connecting computers together with a hub or switch, "Straight Through" cables are used.



Switches

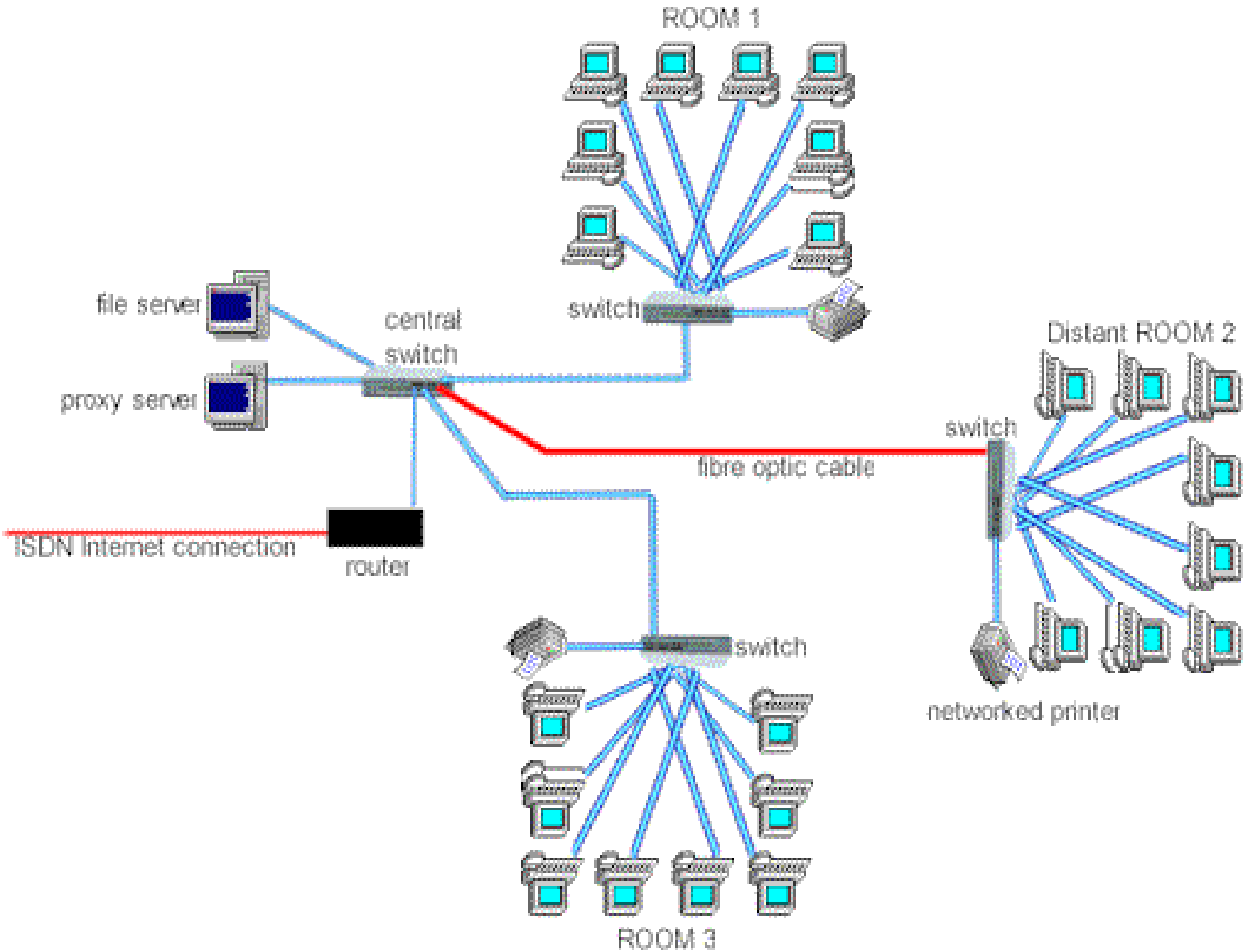
- A **network switch** is a computer networking device that connects network segments.
- The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model.

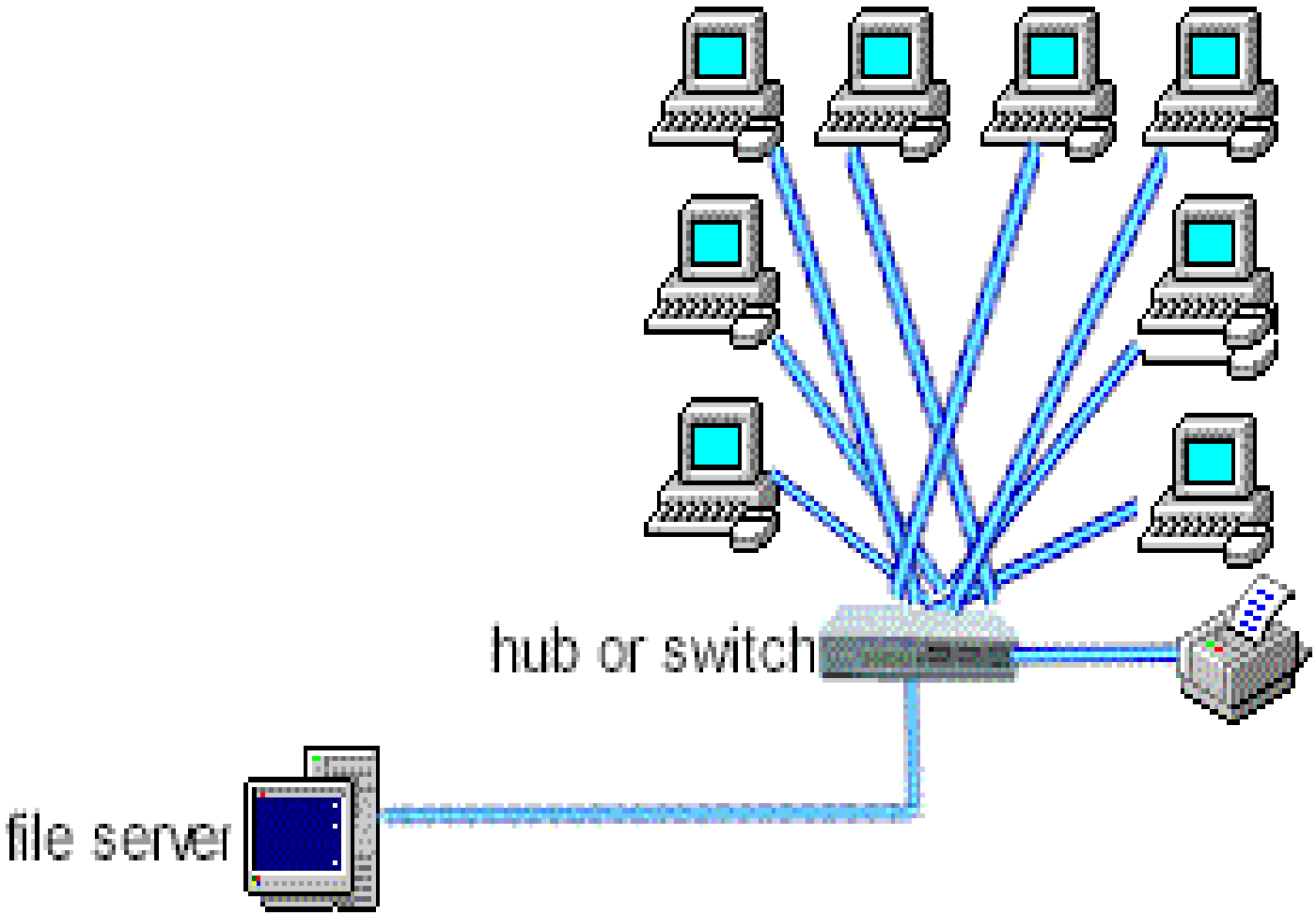
Rack mounted 24 port switches

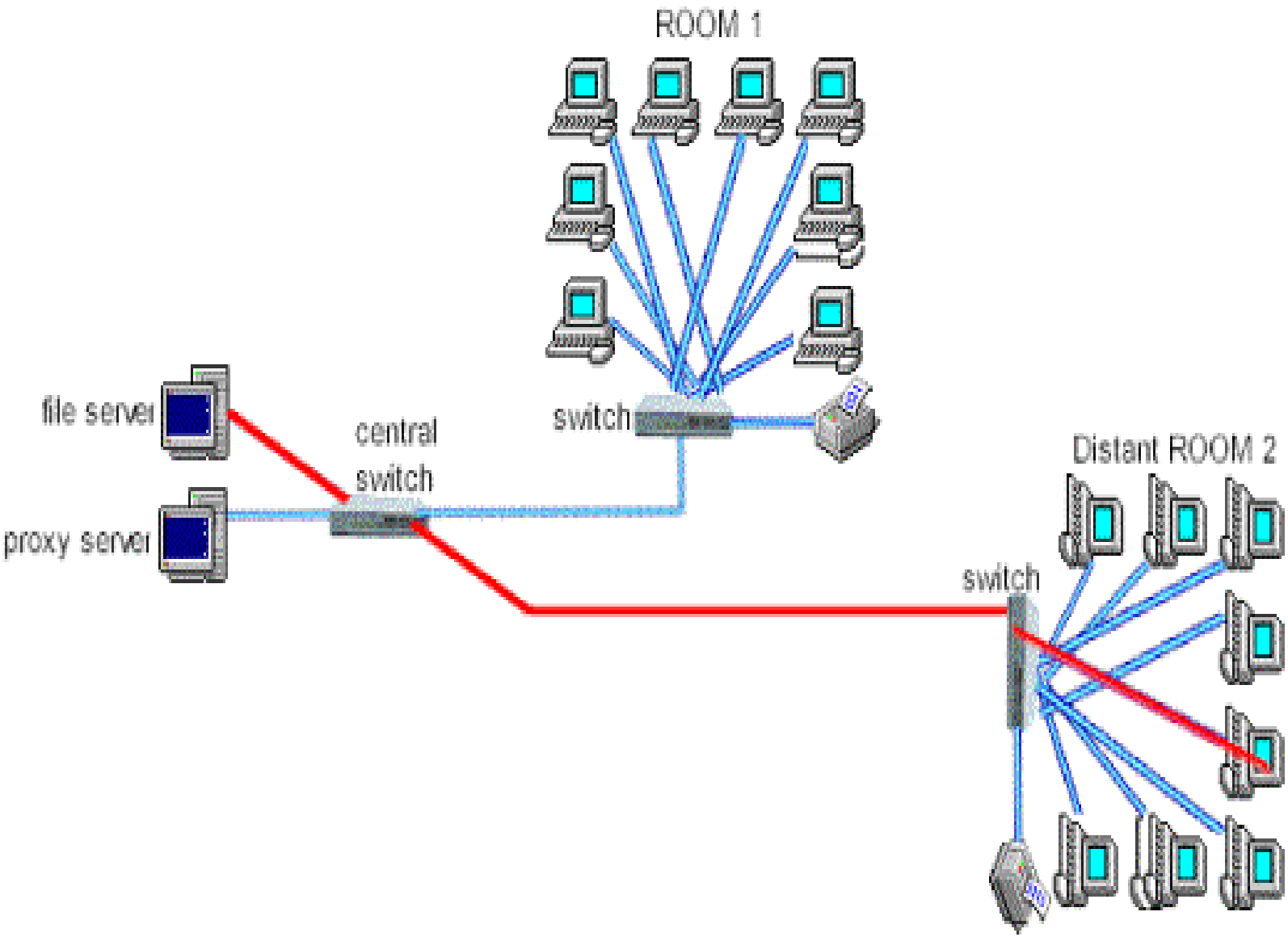
HUB

- A hub is a device that lets a single network cable to split into multiple cables leading to **nodes.**

4-port Ethernet hub


ROOM 1
file server
central
switch
switch
proxy server
Distant ROOM 2
switch
fibre optic cable
ISDN Internet connection
router
switch
networked printer
ROOM 3


hub or switch
file server


ROOM 1
file server
central
switch
switch
proxy server
Distant ROOM 2
switch