CSE-3101

Computer Networking

Mala Rani Barman
Assistant Professor, Department of Computer Science and Engineering
Sheikh Hasina University

- A local area network (LAN) is a small interconnection infrastructure that typically uses a shared transmission medium. Protocols designed for LAN are normally concerned with data link layer and physical layer.

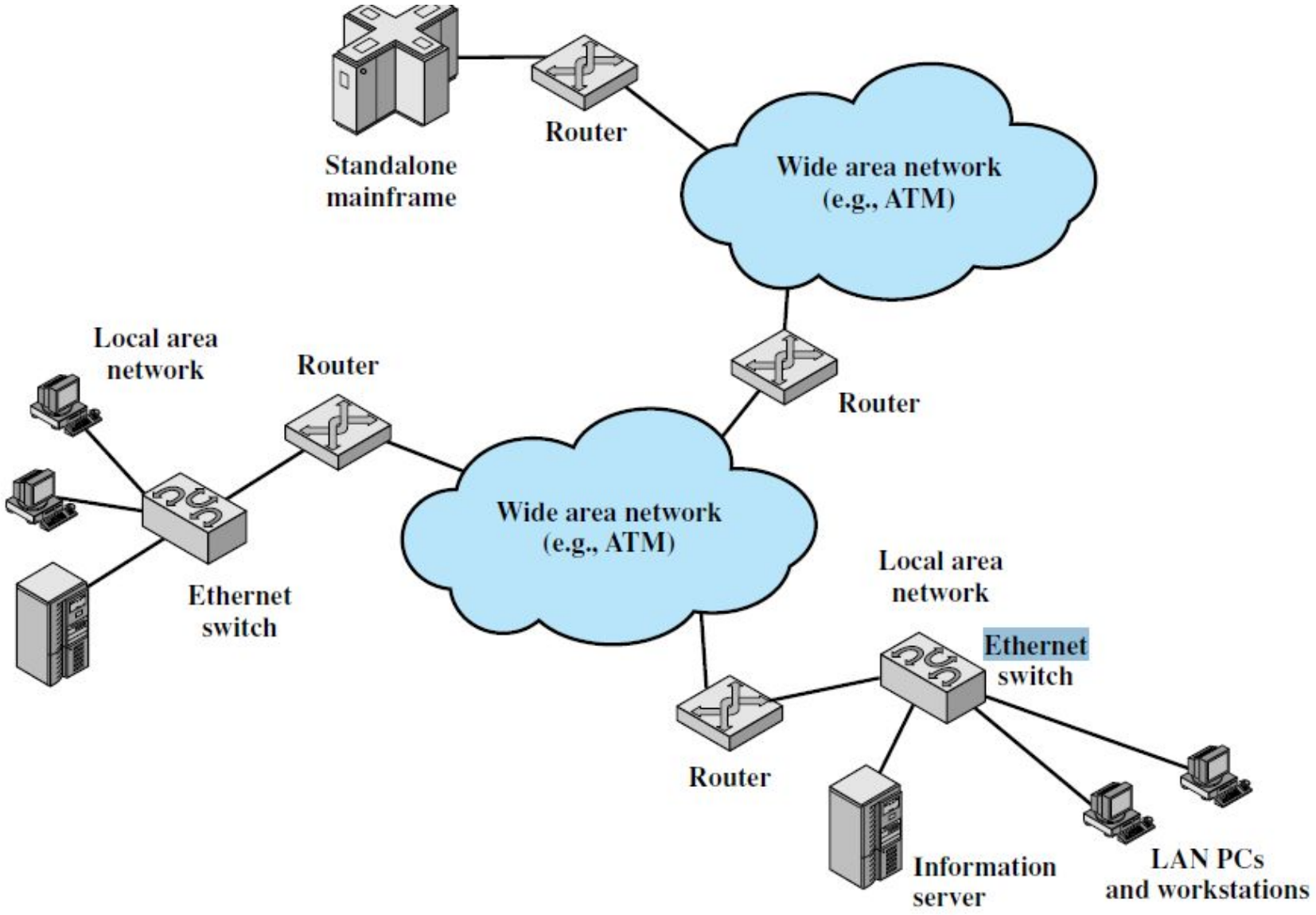
- Organizations working on LAN standards comply with the specifications of IEEE 802 reference model. IEEE 802 standard subdivides the data link layer of the protocol model into logical link control layer (LLC) which is responsible for flow and error control and medium access control (MAC) layer (controls the access to the transmission medium and is responsible for framing).

- The MAC header contains 6-bytes MAC address in hexadecimal format like: 00-50-35-76-92-BD. This MAC address is unique for each device and permanently stored in ROM of the adapter. Only MAC address can be used to communicate within the LAN.

- Both the Internet and ATM were designed for wide area networking. However, many companies, universities, and other organizations have large numbers of computers that must be connected. This need gave rise to the local area network. One of the the most popular LAN is Ethernet.

- IEEE 802.3, popularly called Ethernet, uses bus/star topology, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later (CSMA/CD).

- IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network also use IEEE 802.5 .


Standalone mainframe
Router
Wide area network (e.g., ATM)
Local area network
Router
Router
Wide area network (e.g., ATM)
Ethernet switch
Local area network
Ethernet switch
Router
Information server
LAN PCs and workstations

There are four alternative media that can be used for a bus LAN:

- ✔Twisted pair
- ✔Baseband coaxial cable
- ✔Broadband coaxial cable
- ✔Optical fiber

The switching devices of LAN are :
HUB, Bridge, Switch and Router

HUB, Bridge Switch and Router

Hub

A hub is the simplest of these devices. Any data packet coming from one port is sent to all other ports. It is then up to the receiving computer to decide if the packet is for it or not. The biggest problem with hubs is their simplicity. Since every packet is sent out to every computer on the network, there is a lot of wasted transmission. This means that the network can easily become bogged down. Hubs are typically used on small networks where the amount of data going across the network is never very high.

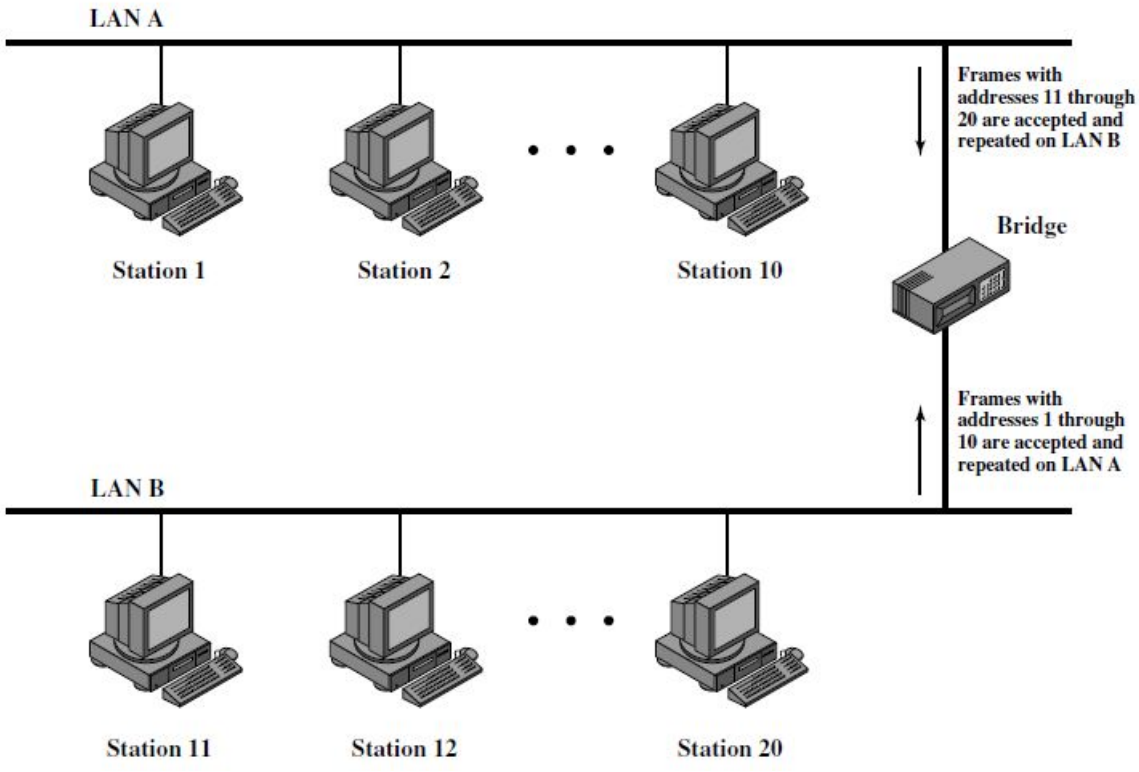
There are mainly two types of hubs:
1. Passive: The signal is forwarded as it is (so it doesn't need power supply).

2. Active: The signal is amplified, so they work as repeaters. In fact they have been called multiport repeaters (use power supply). Hubs can be connected to other hubs using an uplink port to extend the network.

OSI Model: Active Hubs work on the physical layer (lowest layer). That's the reason they can't deal with addressing or data filtering. The passive Hub is at layer 0.

Bridge

A bridge goes one step up on a hub in that it looks at the destination of the packet before sending. If the destination address is not on the other side of the bridge it will not transmit the data. It uses MAC address of 48 bits.



Switch

Instead of broadcasting the frames everywhere, a switch actually checks for the destination MAC address and forward it to the relevant port to reach that computer only. This way, switches reduce traffic and divide the collision domain into segments, this is very efficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment.

Most common switching methods are:

1. Cut-through: Directly forward what the switch gets.
2. Store and forward: receive the full frame before retransmitting it.

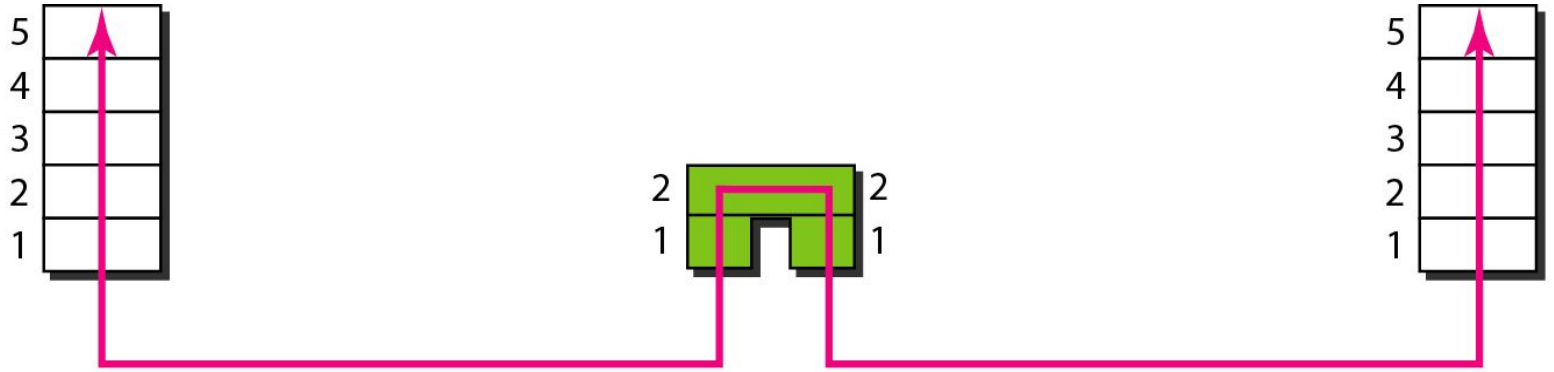
Router

A router is similar in a switch in that it forwards packets based on address. But, instead of the MAC address that a switch uses, a router can use the IP address. This allows the network to go across different protocols. The most common home use for routers is to share a broadband internet connection. The router has a public IP address and that address is shared with the network. When data comes through the router it is forwarded to the correct computer.

Gateway

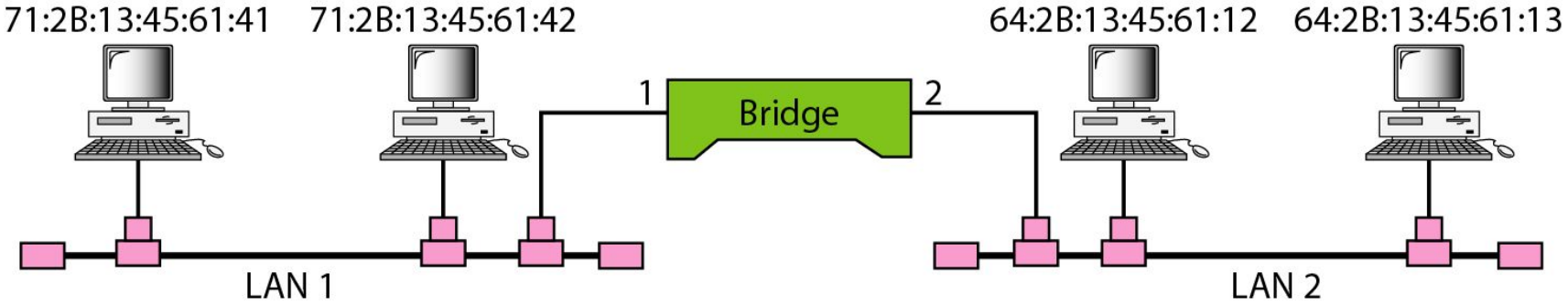
Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients and IPX/SPX or AppleTalk.

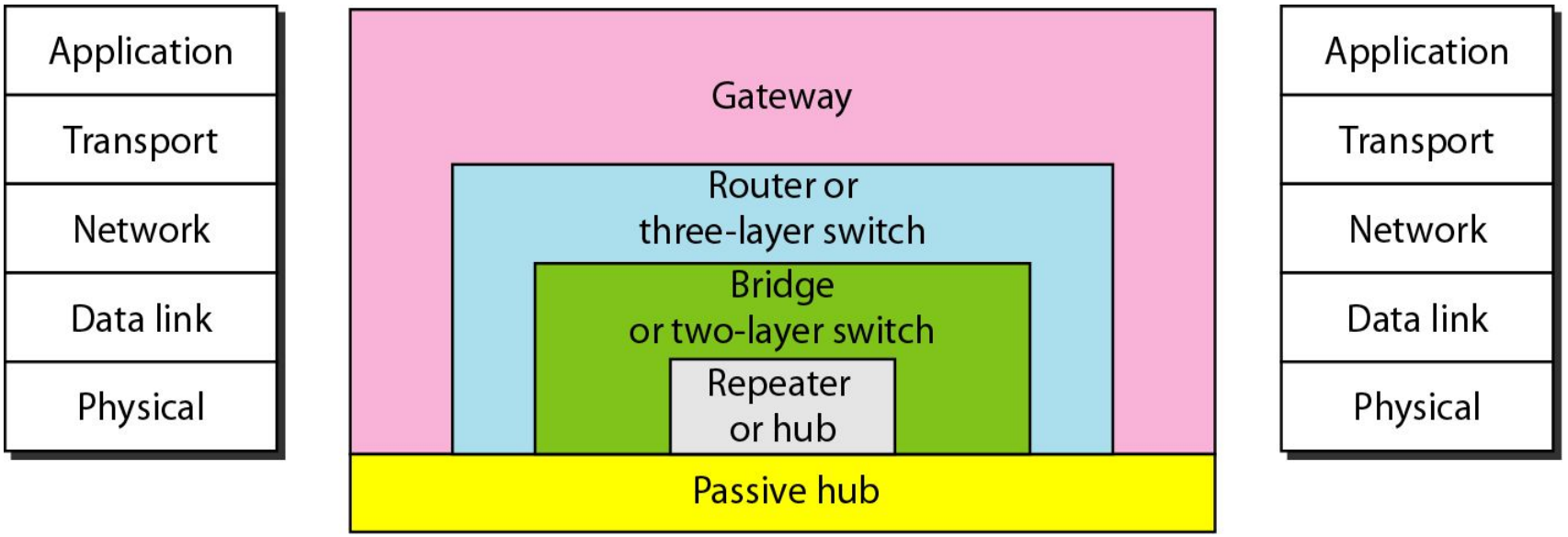
A bridge connecting two LANs



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table

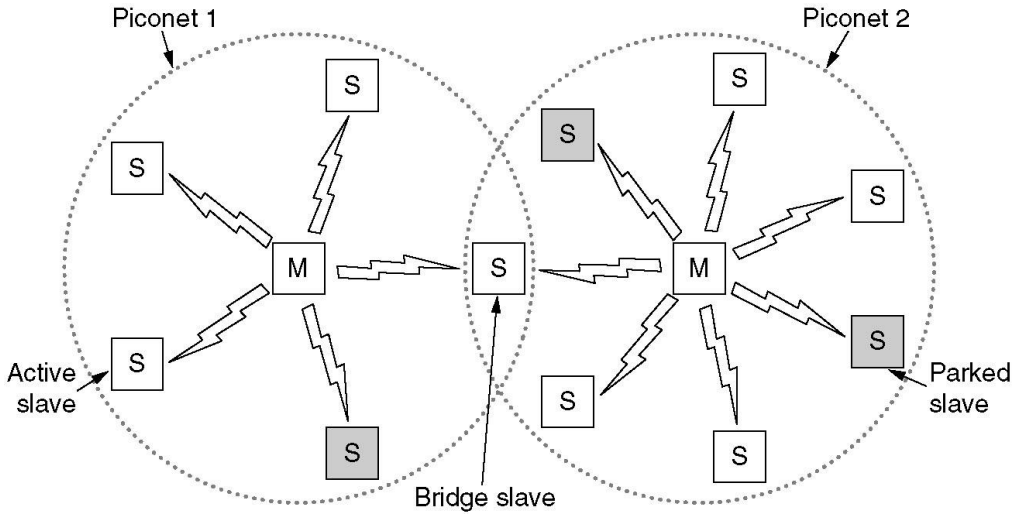




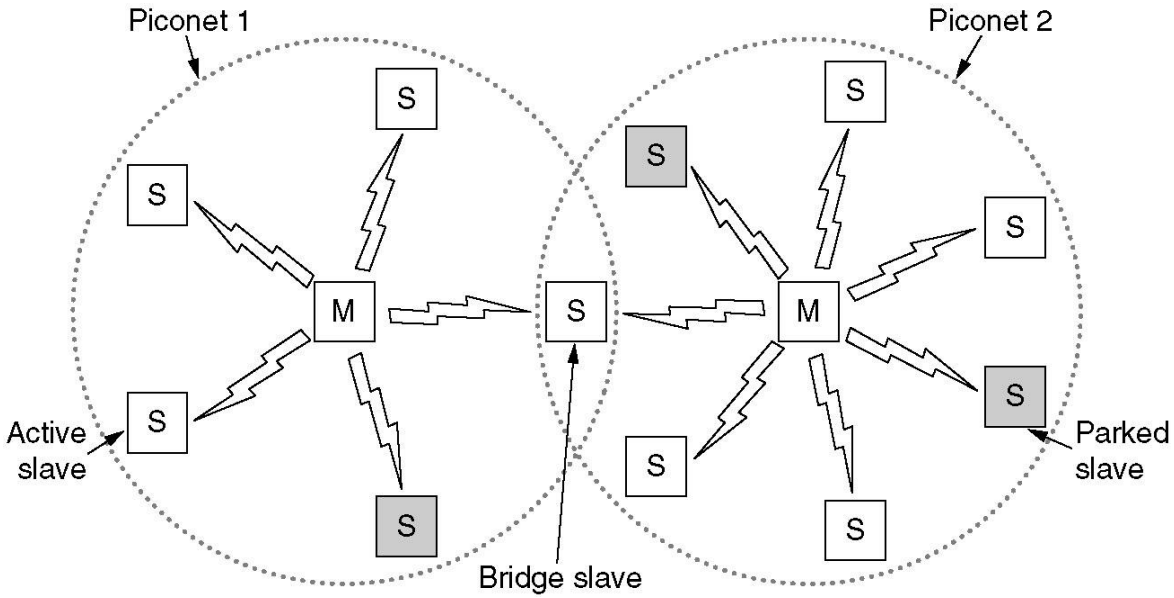
Five categories of connecting devices

Home RF and Bluetooth

Home RF is used to interconnect the various home electronic devices such as, desktops, laptops and appliances. Home RF supports data rates of about 2Mbps and has range of about 50m.



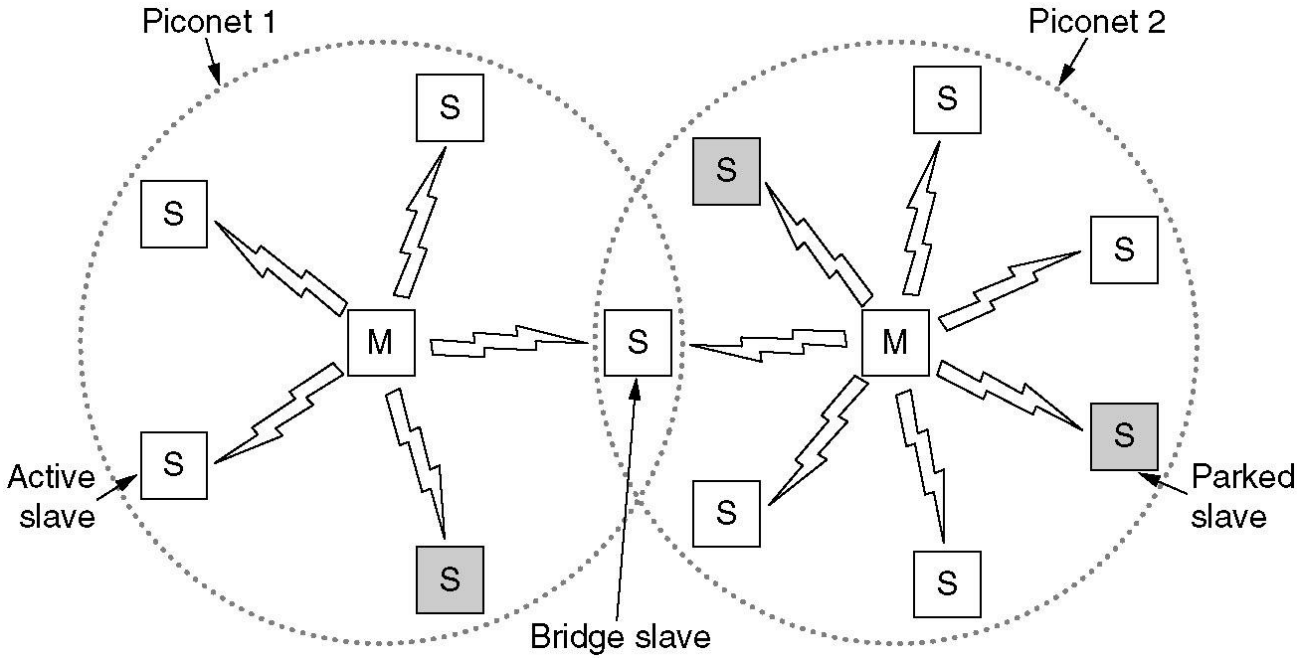
The basic Bluetooth network configuration, called a *piconet*, consists of a master device and up to seven slave devices, as in Figure above. Any communication is between the master and a slave; the slaves do not communicate directly with each other. A Bluetooth device has a built-in short range radio transmitter.



✔Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephone, notebooks, computers, cameras, printers etc.

✔Bluetooth defines two types of networks called: piconet and scatternet.

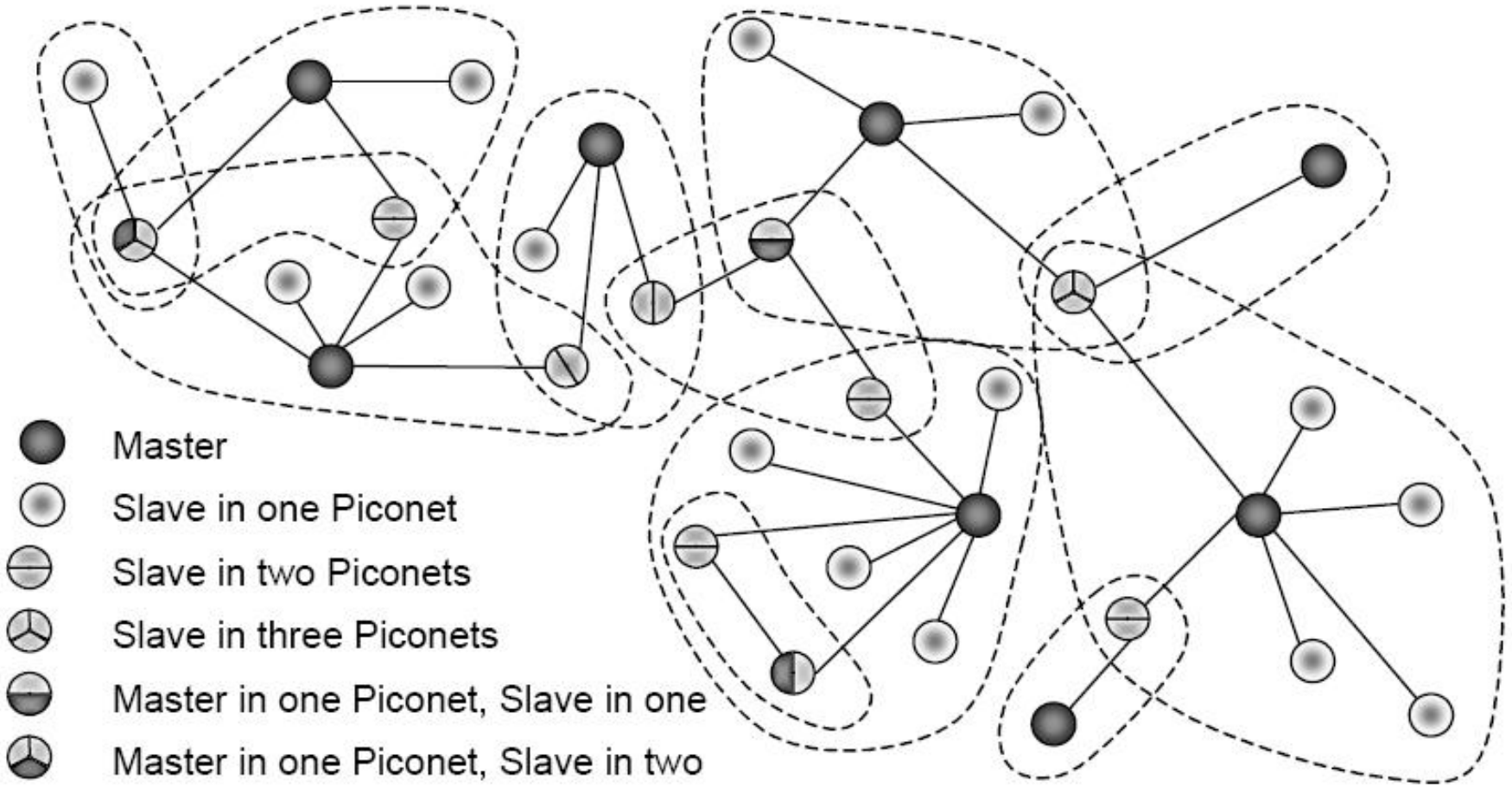
✔A piconet can have up to eight stations, one of which is called primary station, the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Bluetooth uses frequency-hopping spread spectrum (FHSS) in the physical layer to avoid interference from other devices or network.



- Piconets can be combined to form scatternet where a secondary user of one piconet acts as bridge to another piconet. The bridge secondary/slave acts as a primary in receiving packets from the original primary of first piconet then deliver the packet to secondaries of the second piconet.

- Although a piconet can have maximum 7 secondaries , additional seconarioes can be in parked state. A secondary in parked state is synchronized with the primary, but can not take part in communication until it is removed from parked state to the active state.

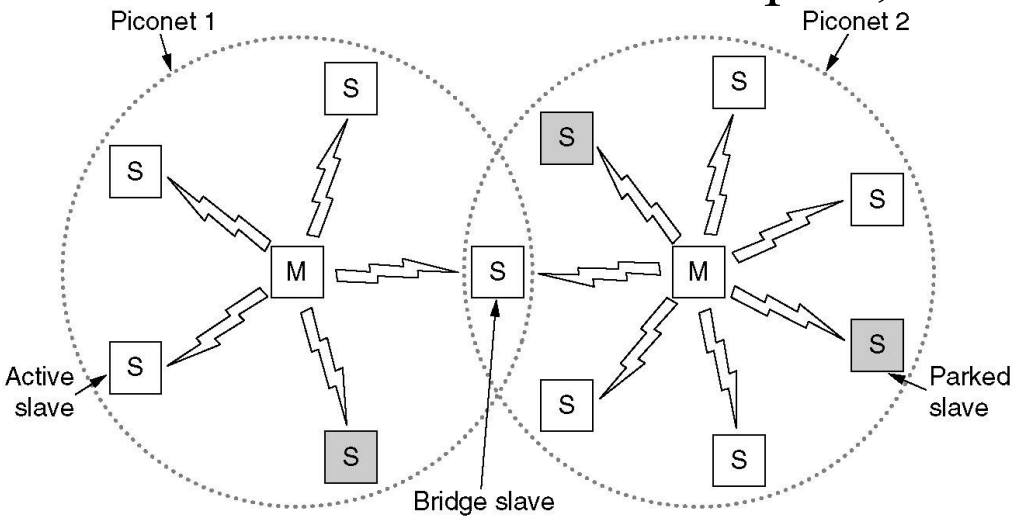
✔No central network structure: “Ad-hoc” network.



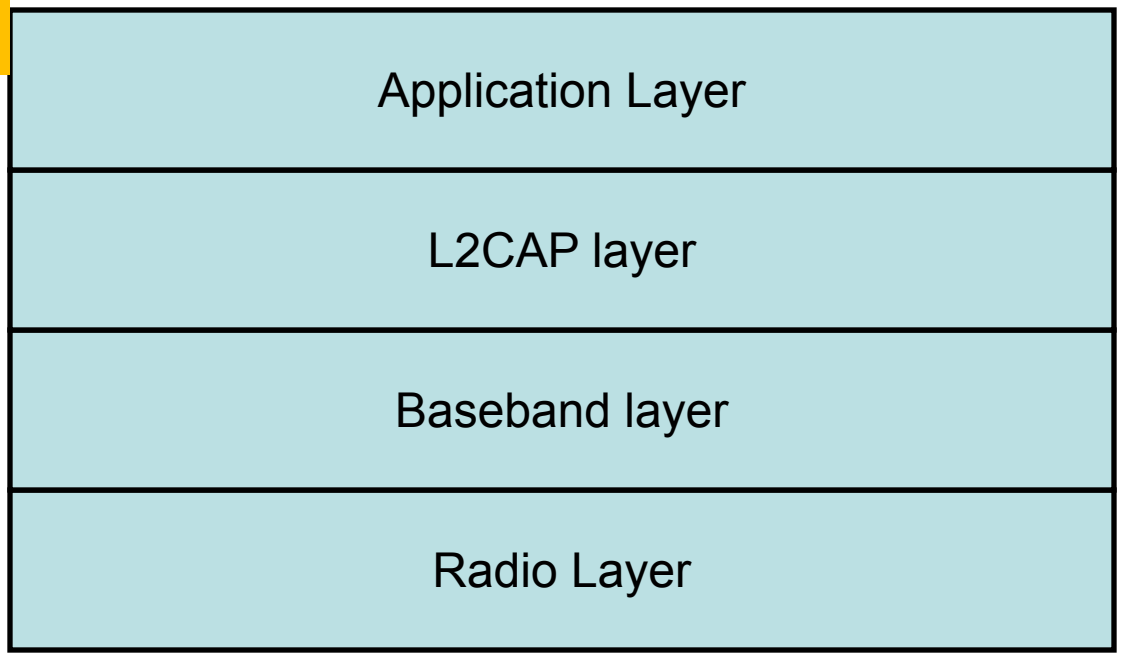
Two types of links can be created between primary and secondary:

- A **synchronous connection-oriented (SCO)** link is used when avoiding latency (delay in data delivery) is more important than integrity (error free delivery). In this case physical link is created primary and secondary by reserving specific slots at regular intervals. The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted.

- An **asynchronous connectionless link (ACL)** is used when data integrity is more important than avoiding latency. In this type link if payload encapsulated in the frame is lost/ corrupted, it is retransmitted.



Layers of Bluetooth



- Radio layer is like physical layer of Internet. Uses FHSS, GFSK modulation.
- Baseband layer is like MAC sublayer uses TDMA slot as the physical channel.
- Logical Link Control and Adaption Protocol (L2CAP) is like LLC sublayer (The function of logical link control layer (LLC) are: framing, flow control and error control). The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS) and group management.

The Network Layer

The network layer is concerned with the routing of data across the network from one end to another. To do this, the network layer converts the data into **packets** and ensures that the packets are delivered to their final destination, where they can be converted back into the original data.

Network layer protocols are concerned with the following issues:

- ✔ The interface between a host and the network.
- ✔ The interface between two hosts across the network.
- ✔ Routing of packets across the network, including the allocation of a route and handling of congestion.
- ✔ Correct ordering of packets to reflect the original order of data.
- ✔ Collection of statistical information (e.g., number of transmitted packets) for performance measurement and accounting purposes.
- ✔ Internetworking: communication between two or more networks.

Internetworking

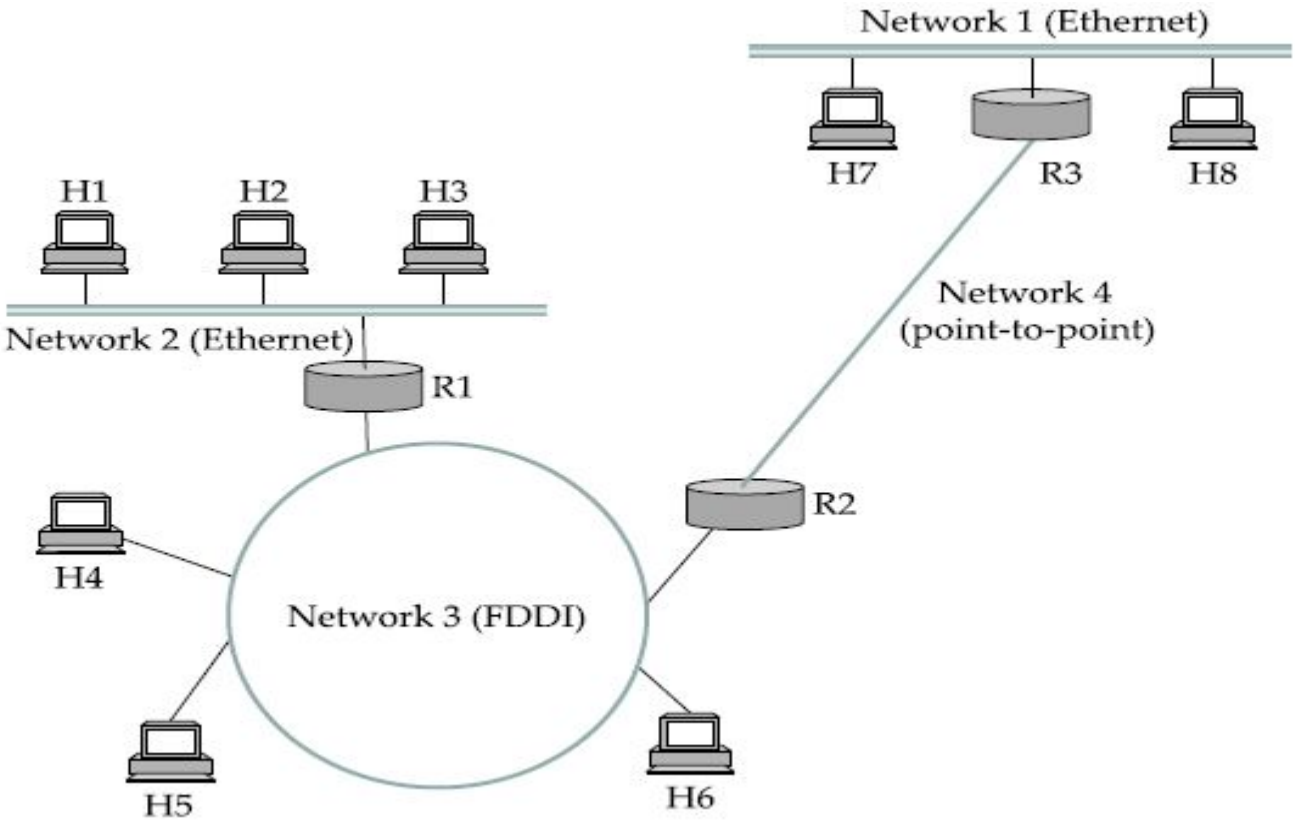
- In the previous chapter, we saw that it was possible to build reasonably large LANs using bridges and LAN switches, but that such approaches were limited in their ability to scale and to handle heterogeneity.

- In this chapter, we explore some ways to go beyond the limitations of bridged networks, enabling us to build large, highly heterogeneous networks with reasonably efficient routing. We refer to such networks as *internetworks*.

- We use the term "*internetwork*," or sometimes just "internet" with a lowercase *i,* to refer to an arbitrary collection of networks interconnected to provide some sort of host-to-host packet delivery service. For example, a corporation with many sites might construct a private *internetwork* by interconnecting the LANs at their different sites with point-to-point links leased from the phone company.

- When we are talking about the widely used, global i*nternetwork* to which a large percentage of networks are now connected, we call it the "Internet" with a capital *I* .

Figure below shows an example *internetwork*. An *internetwork* is often referred to as a network of networks because it is made up of lots of smaller networks. In this figure, we see Ethernets, an FDDI ring, and a point-to-point link. Each of these is a single technology network. The nodes that interconnect the networks are called *routers*.



A simple internetwork. H*n* = host; R*n* = router

Figure (b) shows how hosts H1 and H8 are logically connected by the internet in Figure (a), including the protocol graph running on each node.

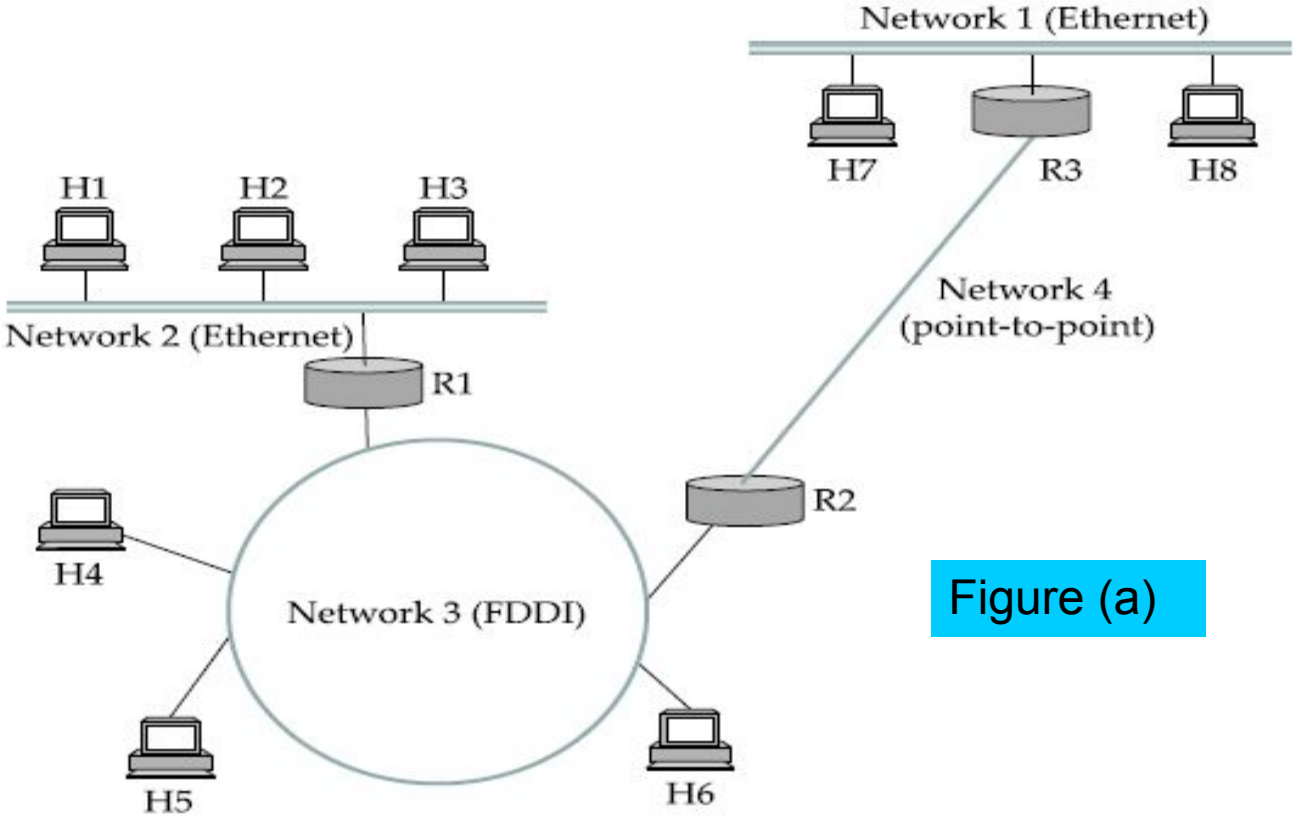


Figure (a)

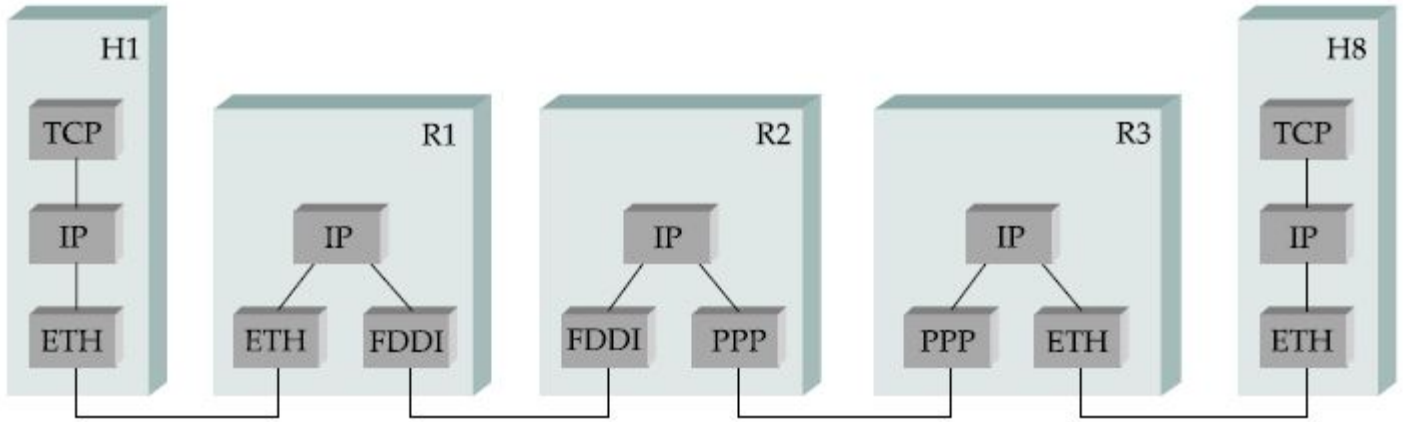
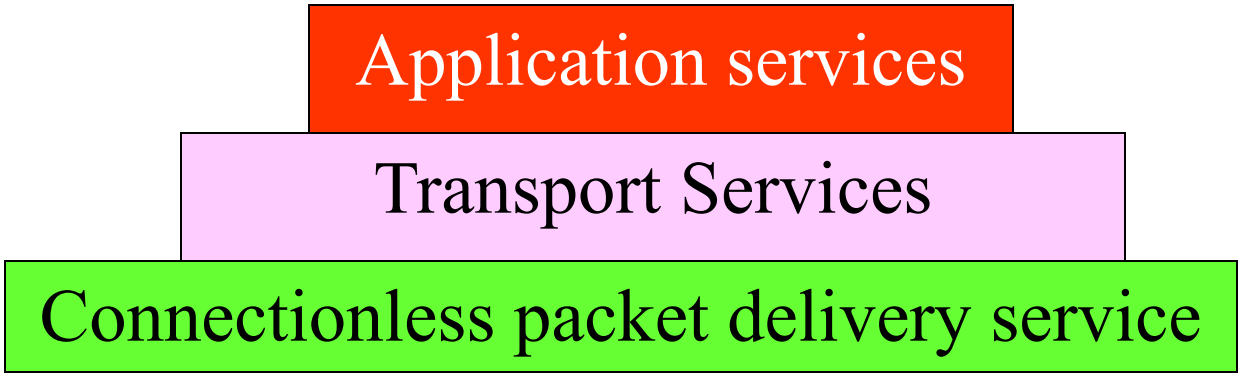


Figure (b)

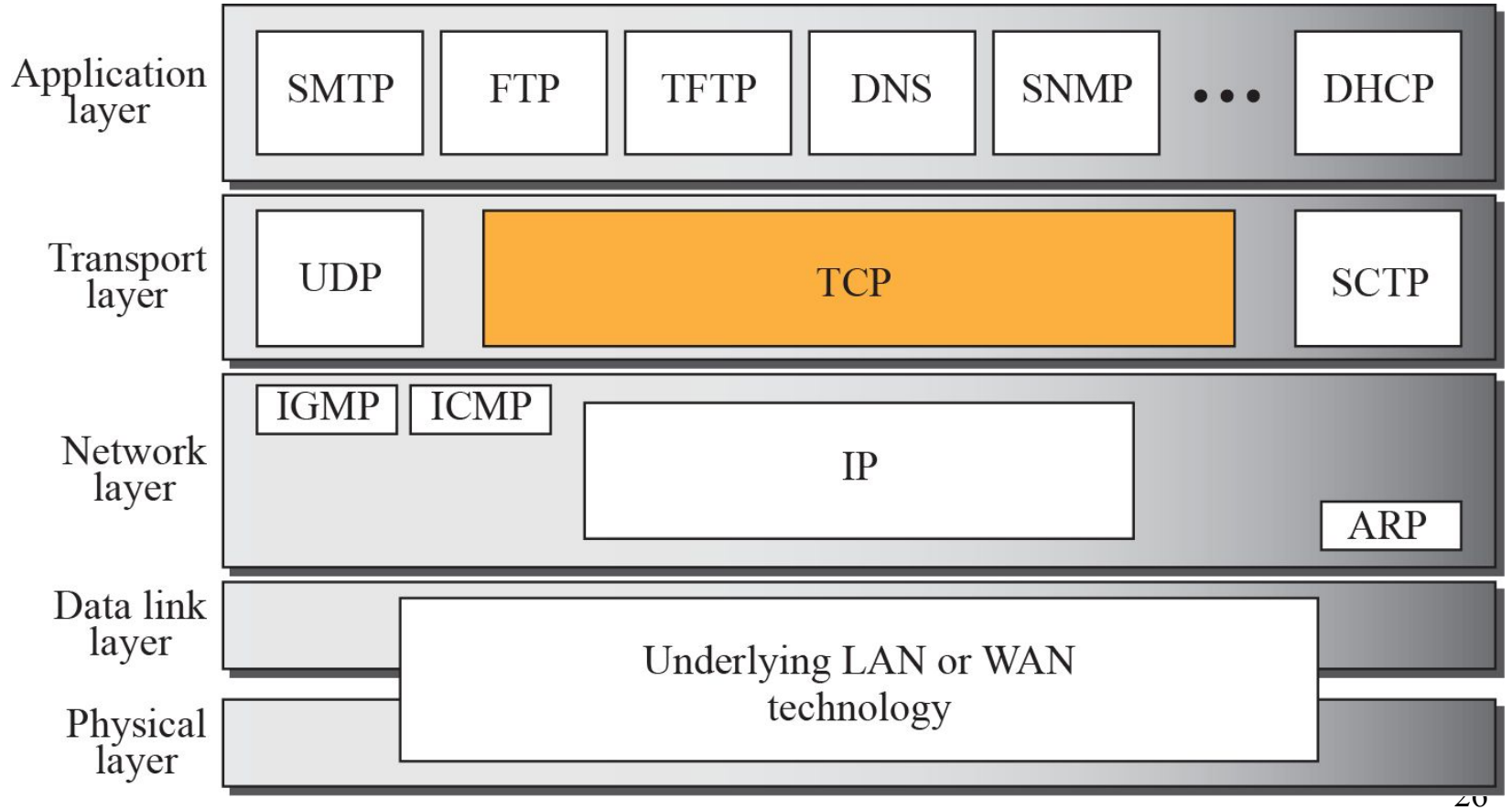
Internet Protocol

- ✔The protocol that defines the unreliable, connectionless delivery mechanism is called Internet protocol. The current version of the protocol is version 4 by the acronyms *IPv4*.
- ✔IP protocol is the basic unit of TCP/IP Internet. TCP/IP provides 3 layers of service:



Three Conceptual layers of Internet service

Figure below shows the relationship of IP and TCP to the other protocols in the TCP/IP protocol suite. TCP lies between the application layer and the network layer, and serves as the intermediary between the application programs and the network operations.



IP Header: Version, Length, ToS

Version number (4 bits)

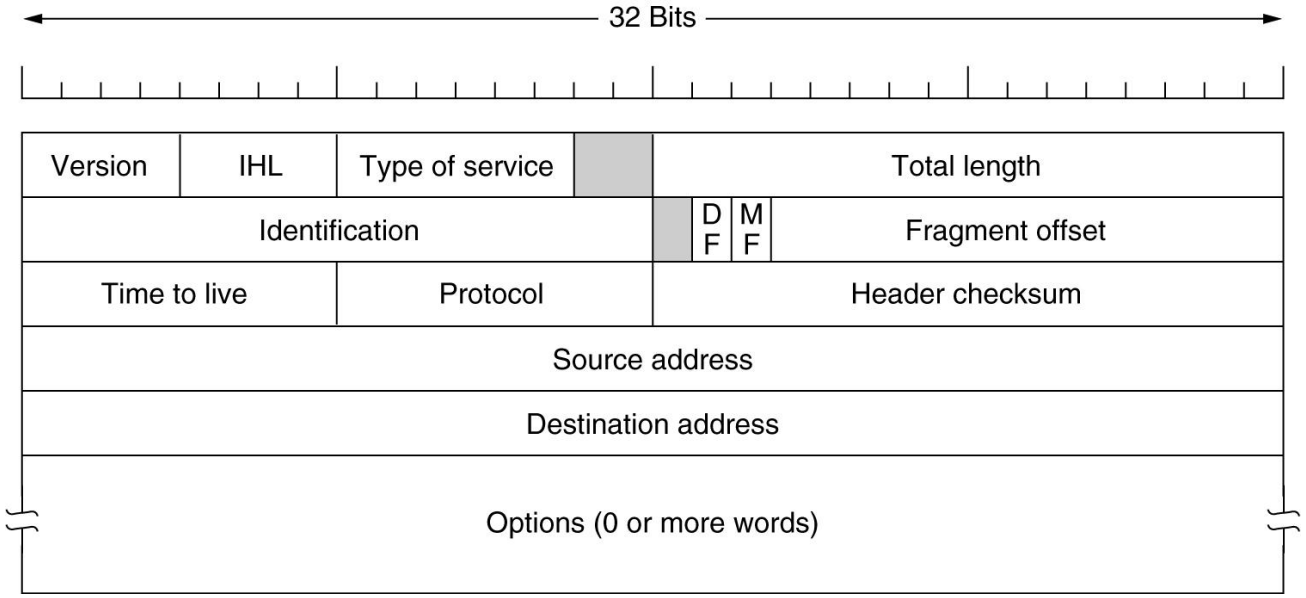
Indicates the version of the IP protocol

Typically “4” (for IPv4), and sometimes “6” (for IPv6)

Internet Header Length (IHL)

Number of 32-bit words in the header (4 bits)

Typically “5” (for a 20-byte IPv4 header)

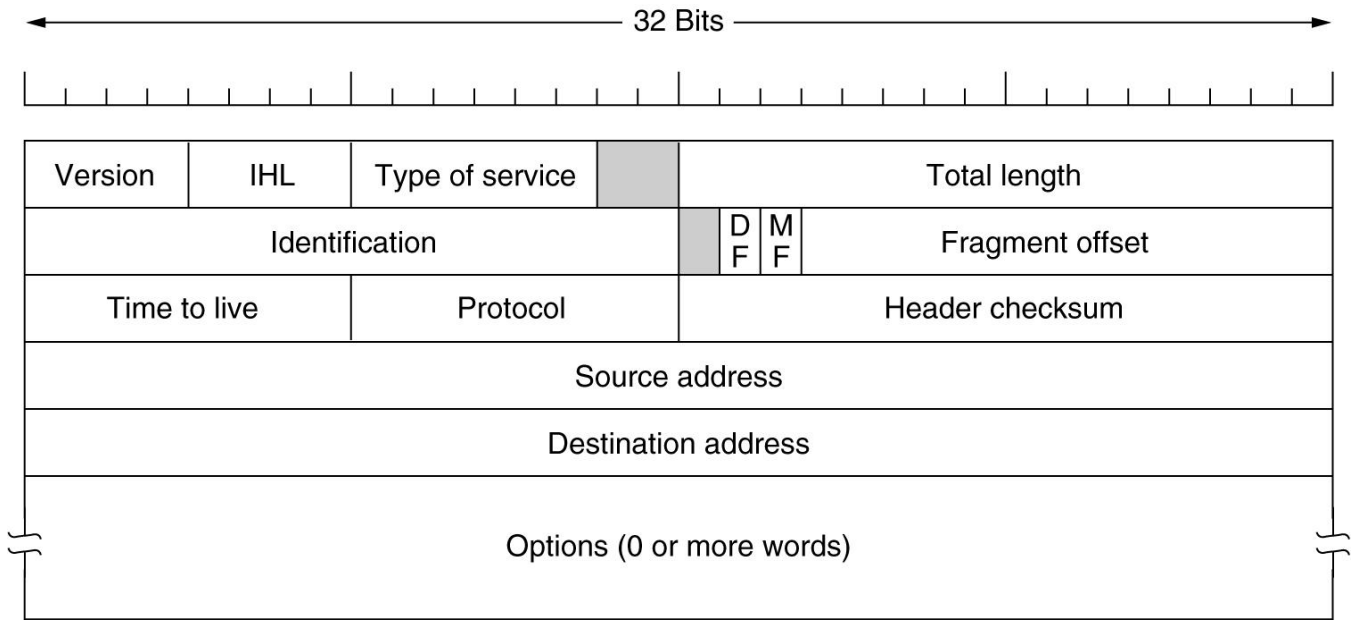


IP Packet Structure

Type-of-Service (8 bits)

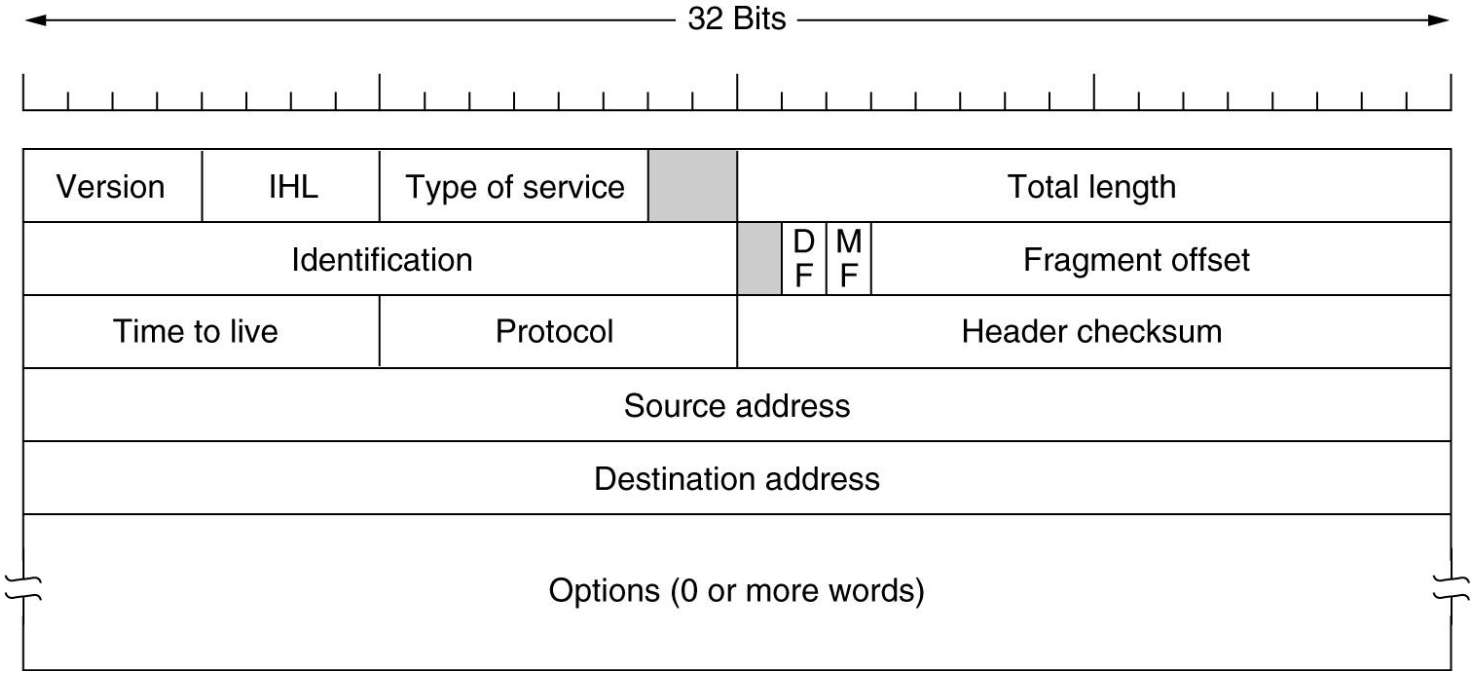
- It is intended to distinguish between different classes of service. Various combinations of reliability and speed are possible. For digitized voice, fast delivery beats accurate delivery. For file transfer, error-free transmission is more important than fast transmission.

- Originally, the 6-bit field contained (from left to right), a three-bit Precedence field and three flags, D, T, and R. The Precedence field was a priority, from 0 (normal) to 7 (network control packet). The three flag bits allowed the host to specify what it cared most about from the set {Delay, Throughput, Reliability}. In practice, current routers often ignore the Type of service field altogether.



IP Header: Length, Fragments, TTL

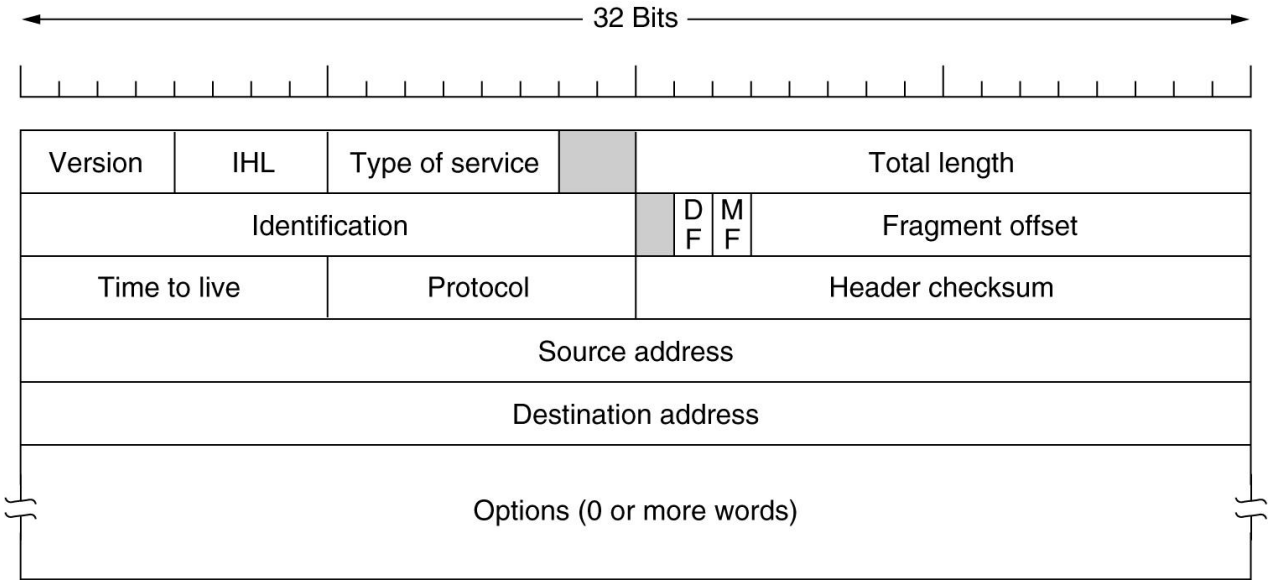
- Total length (16 bits)
  - Number of bytes in the packet
  - Maximum size is 65,535 bytes (2^{16} -1)
- Identification
- The Identification field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same Identification value.



Flags :A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):

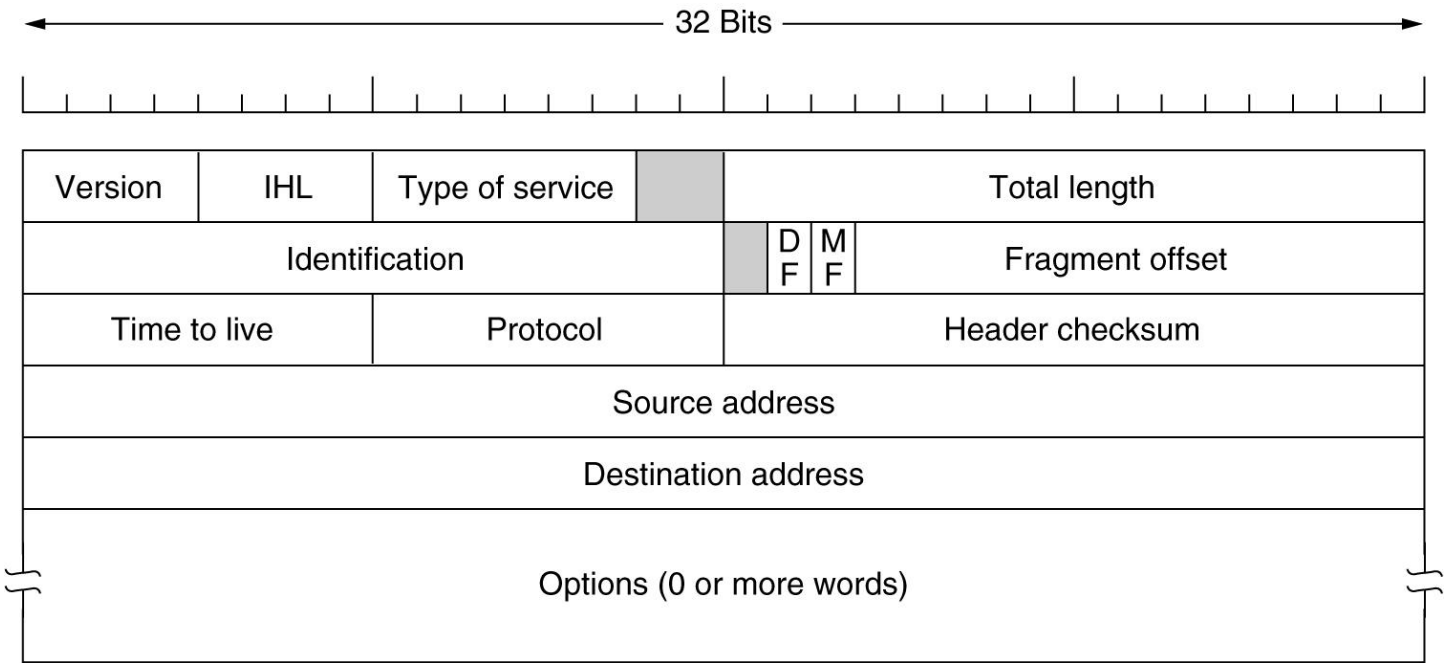
bit 0: Reserved; must be zero.
bit 1: Don't Fragment (DF)
bit 2: More Fragments (MF)

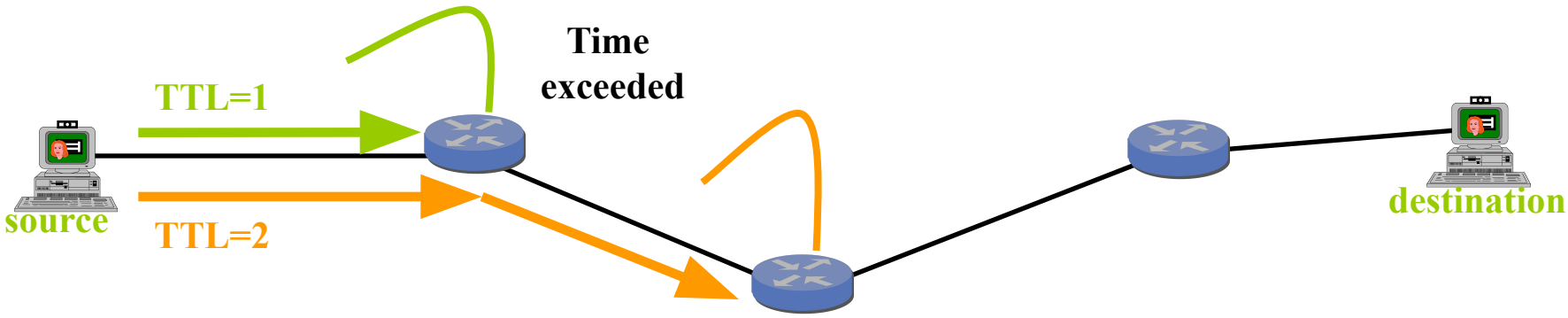
Fragment Offset The Fragment offset tells where in the current datagram this fragment belongs. All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit. Since 13 bits are provided, there is a maximum of $2^{13} = 8192$ fragments per datagram.



Time-To-Live (8 bits)

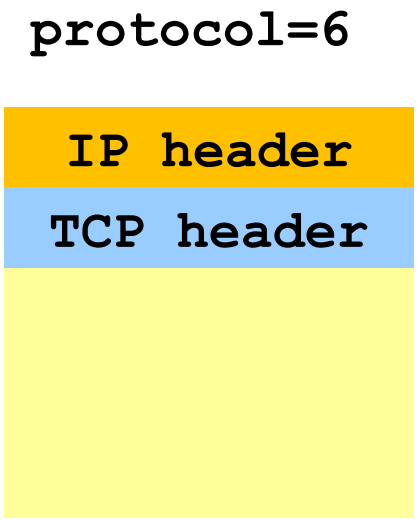
An eight-bit *time to live* field helps prevent datagrams from persisting (e.g. going in circles) on an internet. This field limits a datagram's lifetime. It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In practice, the field has become a *hop count* —when the datagram arrives at a router, the router decrements the TTL field by one. When the TTL field hits zero, the router discards the packet and typically sends an *ICMP Time Exceeded* message to the sender.

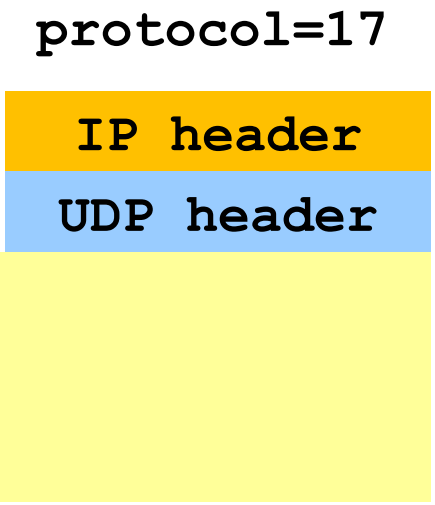


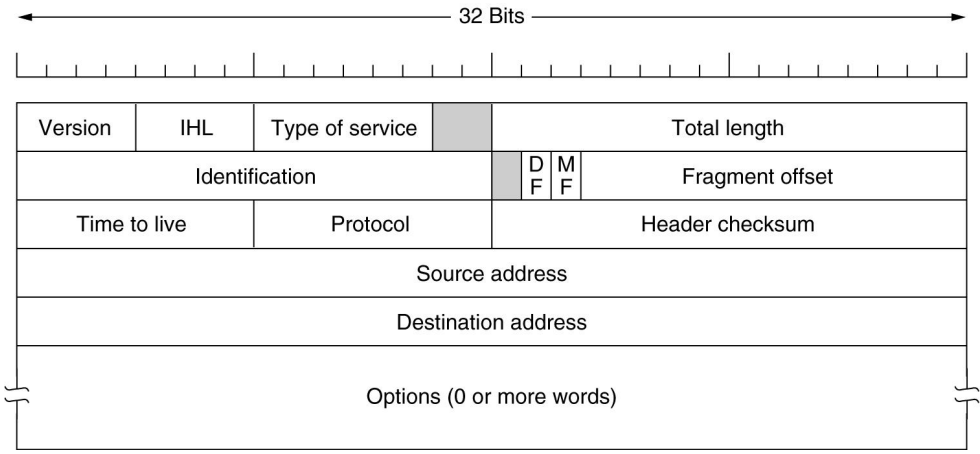


Send packets with TTL=1, 2, … and record source of "time exceeded" message

- **Protocol (8 bits)**
  - Identifies the higher-level protocol
    - "6" for the Transmission Control Protocol (TCP)
    - "17" for the User Datagram Protocol (UDP)





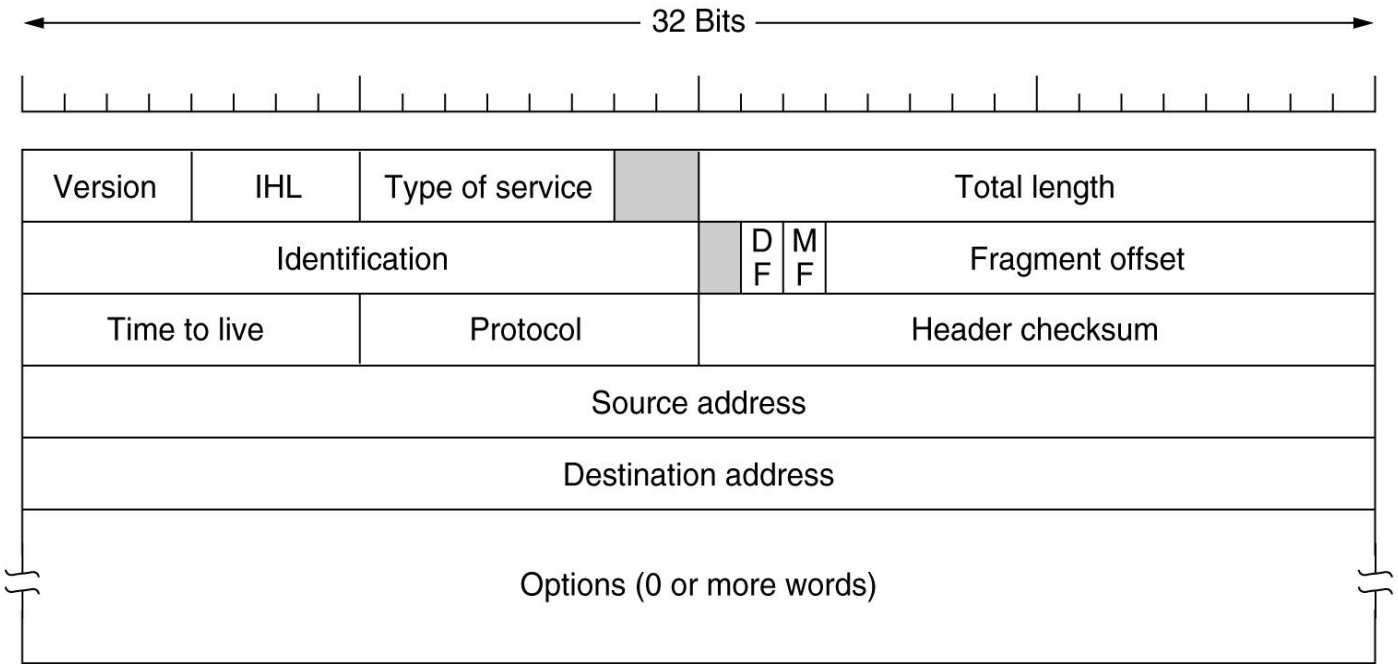


Usually a service is associated with a port under **transport layer** (e.g. http on port 80).

Well-known Ports used by TCP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20 and 21	FTP	File Transfer Protocol (Data and Control)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol

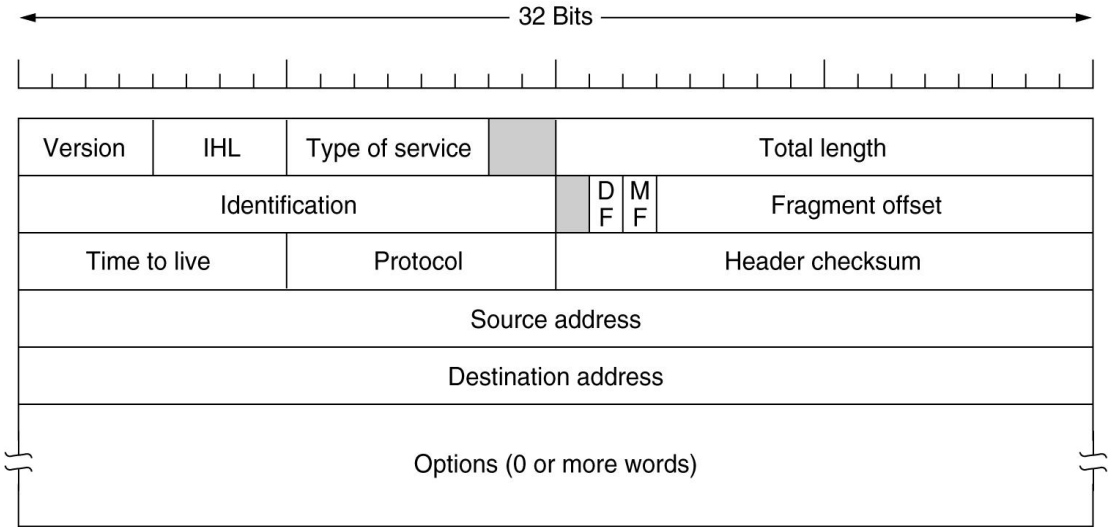
- Checksum (16 bits)
  - Sum of all 16-bit words in the IP packet header
  - If any bits of the header are corrupted in transit
    … the checksum won't match at receiving host
  - Receiving host discards corrupted packets
    - Sending host will retransmit the packet, if needed



Example: Calculating a checksum

- The header is shown in red and the checksum is underlined.
  4500 0073 0000 4000 4011 b861 c0a8 0001 c0a8 00c7 0035 e97c 005f 279f 1e4b 8180

- To calculate the checksum, we can first calculate the sum of each 16 bit value within the header, skipping only the checksum field itself. Note that the values are in hexadecimal notation.
  4500 + 0073 + 0000 + 4000 + 4011 + c0a8 + 0001 + c0a8 + 00c7
  = 2479C (equivalent to 149,404 in decimal).



- Next, we convert the value 2479C to binary:
  0010 0100 0111 1001 1100
  The first 4 bits are the carry and will be added to the rest of the value:
  0010 + 0100 0111 1001 1100 = 0100 0111 1001 1110
  Next, we flip every bit (1's complement) in that value, to obtain the checksum:
  0100 0111 1001 1110 becomes:
  1011 1000 0110 0001
  This is equal to **B861** in hexadecimal, as shown underlined in the original IP packet header.

❑ Verifying a checksum

When verifying a checksum, the same procedure is used as above, except that the original header checksum is not omitted.

4500 + 0073 + 0000 + 4000 + 4011 + **b861** + c0a8 + 0001 + c0a8 + 00c7 = 2fffd

Add the carry bits:

fffd + 2 = ffff

Taking the ones' complement (flipping every bit) yields 0000, which indicates that no error is detected. IP header checksum does not check for the correct order of 16 bit values within the header.

IP Header: To and From Addresses

- Two IP addresses
  - Source IP address (32 bits)
  - Destination IP address (32 bits)
- Destination address
  - Unique identifier for the receiving host
  - Allows each node to make forwarding decisions
- Source address
  - Unique identifier for the sending host
  - Recipient can decide whether to accept packet
  - Enables recipient to send a reply back to source