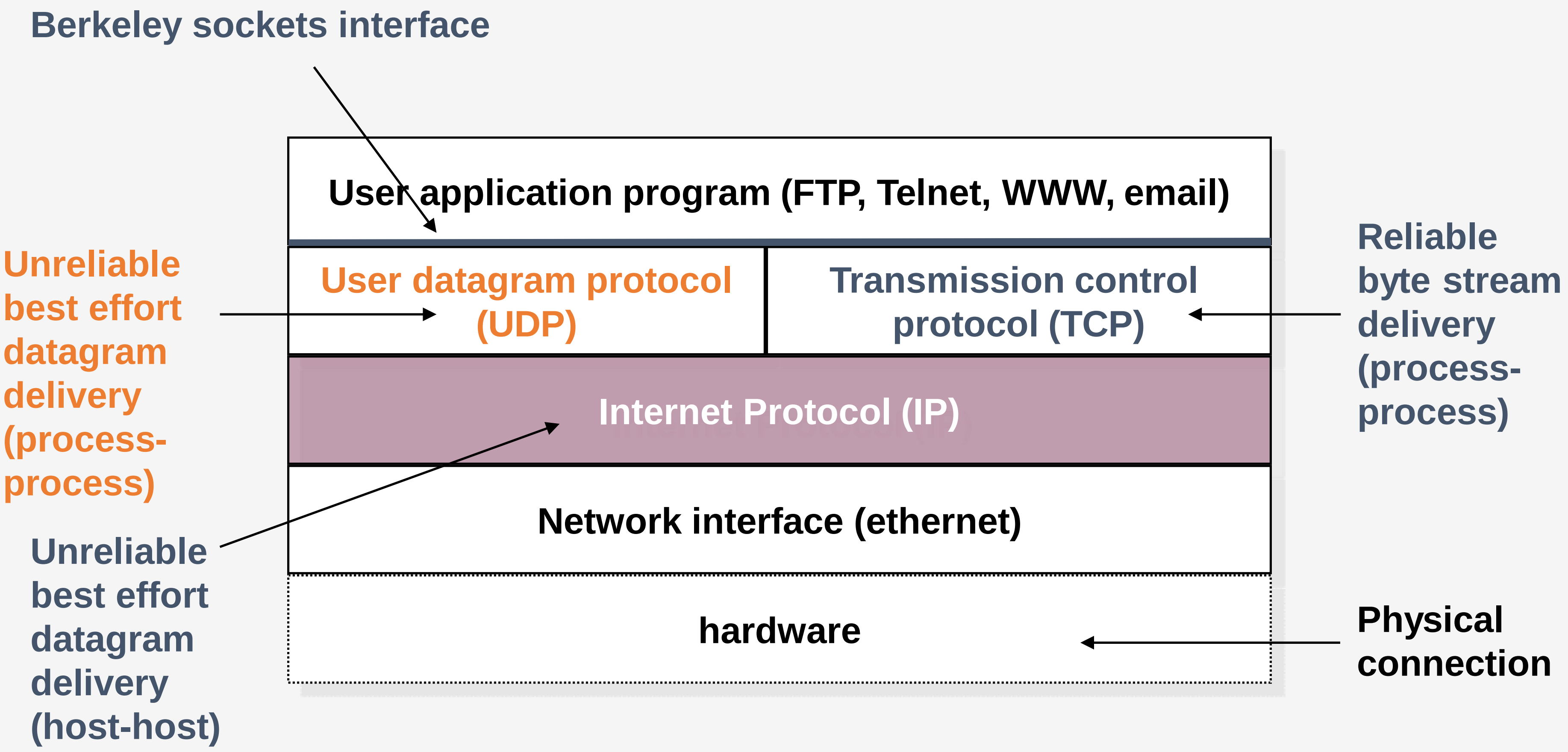
IP Protocol

Dr. Ravindra Nath UIET CSJM University Kanpur

Internet protocol stack



Berkeley sockets interface

User application program (FTP, Telnet, WWW, email)

User datagram protocol (UDP)

Transmission control protocol (TCP)

Internet Protocol (IP)

Network interface (ethernet)

hardware

Unreliable best effort datagram delivery (process-process)

Reliable byte stream delivery (process-process)

Unreliable best effort datagram delivery (host-host)

Physical connection

Functions of the Network Layer

To transport packets from the source to the destination,

possibly through some intermediate nodes.

This involves:

- Knowing the topology of the communication network.
- Choosing routes judiciously to avoid overloading some paths.
- Resolve problems that may arise if Source and Destination are not on the same network.

In other words, Network Layer performs:

- Routing
- Congestion control
- Internetworking

Network Layer Service Classes

Two possible classes:

- **Connection-oriented -- *reliable*, in-sequence delivery.**
- **Connectionless -- *unreliable*, out-of-order delivery.**

Connection -- logical concept of an entity that connects the Source and Destination at its two ends.

Supporters for both connection-oriented and connectionless service and so OSI framework supports both.

Issue of *Connection-oriented* and *Connectionless* service also comes up in other layers.

IP service model

IP service model:

- **Delivery model**: IP provides best-effort delivery of datagram (connectionless) packets between two hosts.
  - IP tries but doesn’t guarantee that packets will arrive (best effort)
  - packets can be lost or duplicated (unreliable)
  - ordering of datagrams not guaranteed (connectionless)
- **Naming scheme**: IP provides a unique address (name) for each host in the Internet.

Why would such a limited delivery model be useful?

- simple, so it runs on any kind of network
- provides a basis for building more sophisticated and user-friendly protocols like TCP and UDP

Internet Protocol

Transports a datagram from source host to destination host,possibly via several intermediate nodes (``routers'').

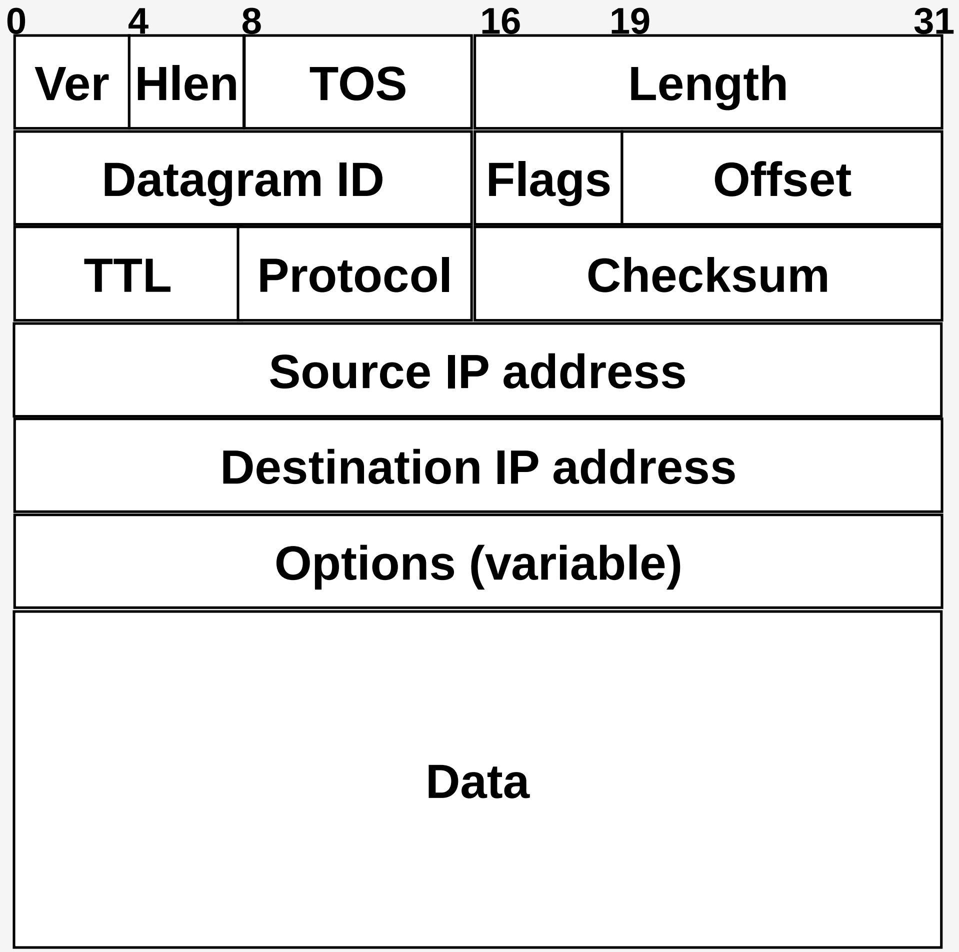
Service is:

Unreliable: Losses, duplicates, out-of-order delivery.

Best effort: Packets not discarded capriciously, delivery failure not necessarily reported.

Connectionless: Each packet is treated independently.

IP packet format



0 4 8 16 19 31

Ver | Hlen | TOS | Length

Datagram ID | Flags | Offset

TTL | Protocol | Checksum

Source IP address

Destination IP address

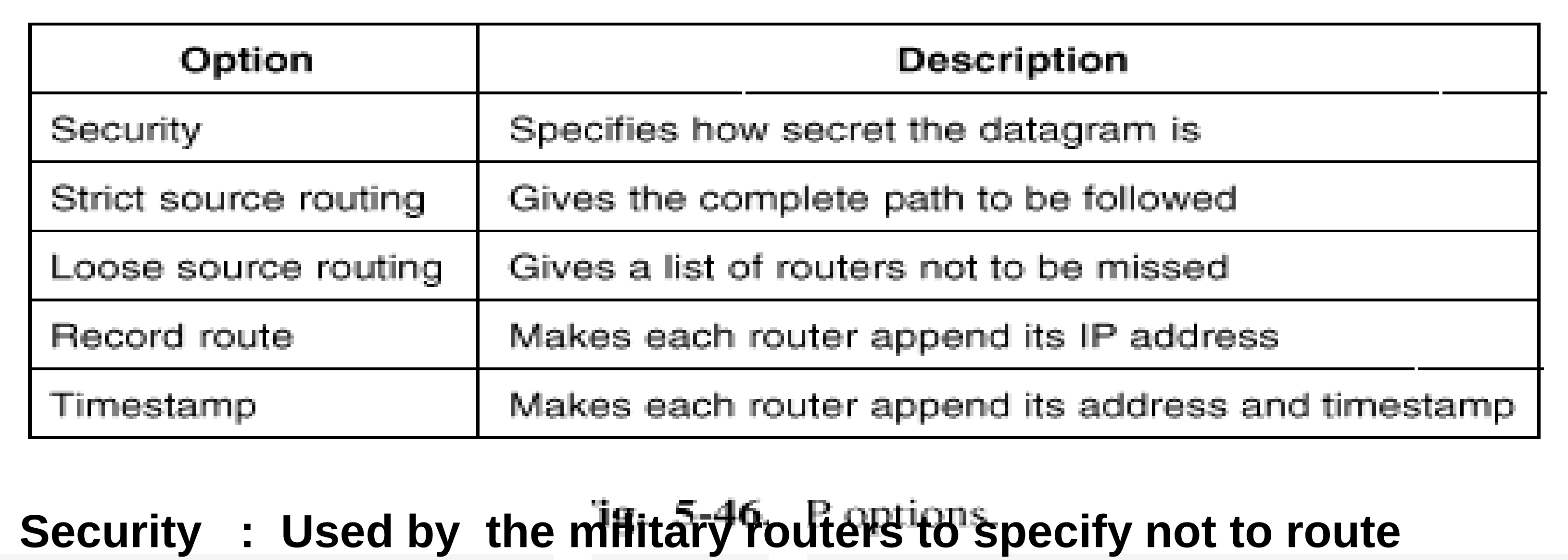
Options (variable)

Data

VER	IP version
HL	Header length (in 32-bit words)
TOS	Type of service (unused)
Length	Datagram length (max 64K B)
ID	Unique datagram identifier
Flags	xxM (more fragmented packets)
Offset	Fragment offset
TTL	Time to Live
Protocol	Higher level protocol (e.g., TCP)
Checksum	Used for detecting errors

Flags : DF = Don’t fragment
MF = More fragments

IP options



Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

ig. 5-46. P options

Security : Used by the military routers to specify not to route through certain countries routers

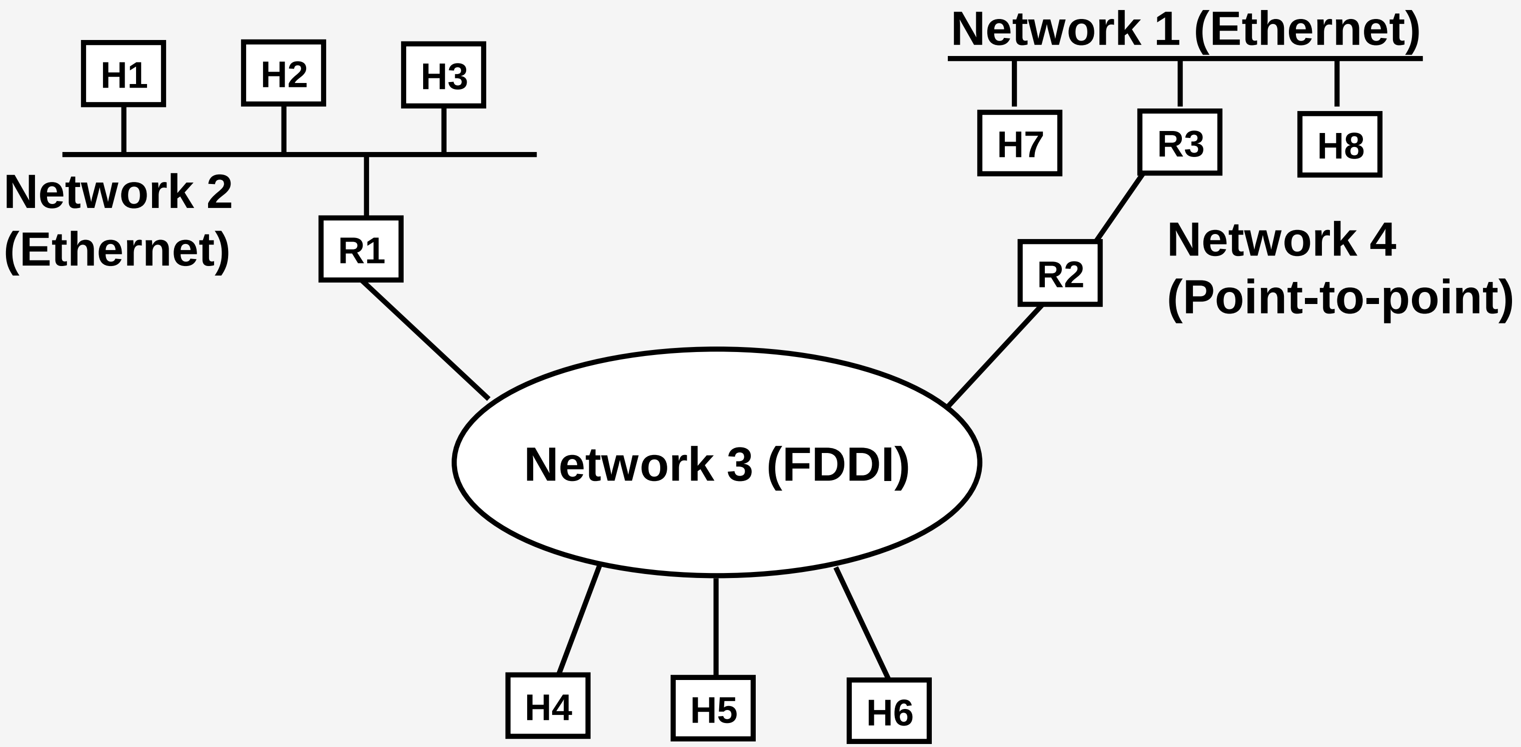
Strict source routing : Complete path to destination as sequence of IP addresses. Used by system managers to send emergency packets when routing tables are corrupted or for making timing measurements.

Loose source routing : Packets travel through a list of routers in the order specified.

Record route : Allows system managers to to track down bugs in the routing algorithms.

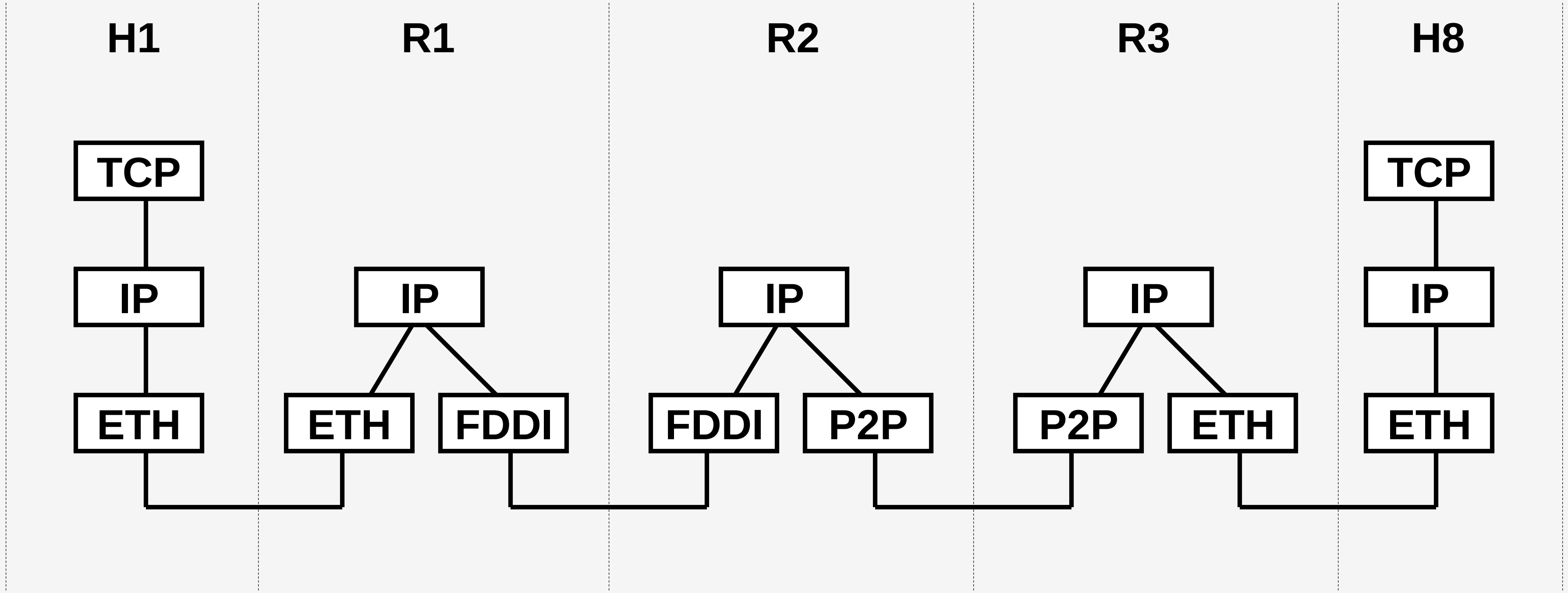
Time stamp : Each adds a 32 bit time stamp in addition to IP address.

IP datagram delivery: Example internet

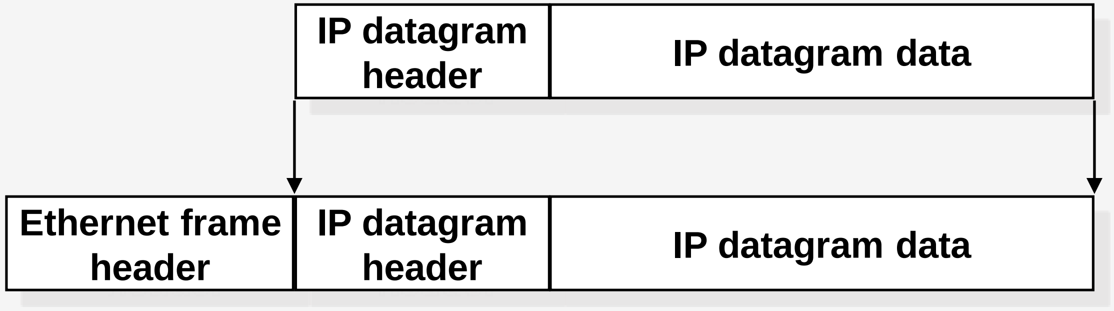


IP layering

Protocol layers used to connect host H1 to host H8 in example internet.



Encapsulating IP datagrams in Ethernet



IP datagram

Ethernet frame

The same idea is used for other types of physical networks

ICMP

The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

ICMP always reports error messages to the original source.

Internet Control Message Protocol (ICMP)

A mechanism for error reporting and communicating control information.

Implemented on top of IP.

Does not specify action.

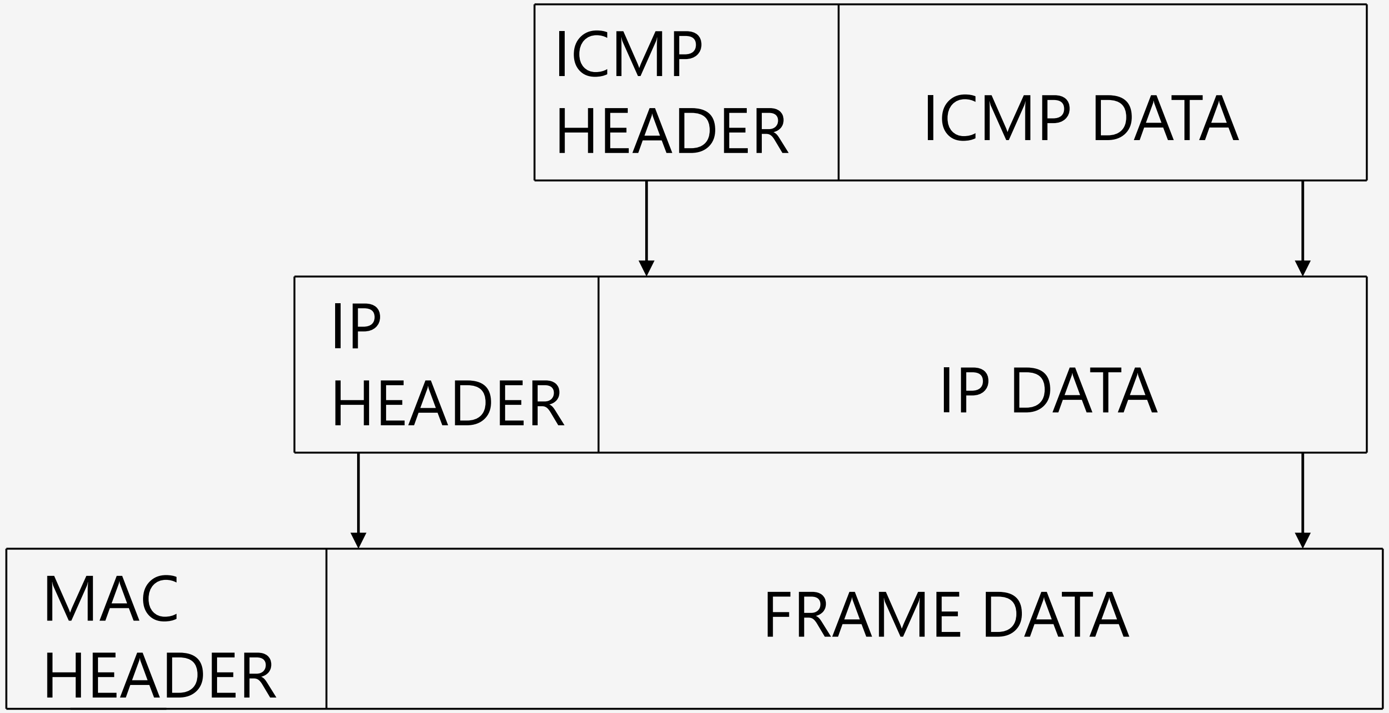
ICMP Error messages include the header and at least the first 8 octets of the IP datagram that caused the error.

No error message generation due to dropping of ICMP messages.

Used by applications like ‘ping’ and ‘traceroute’.

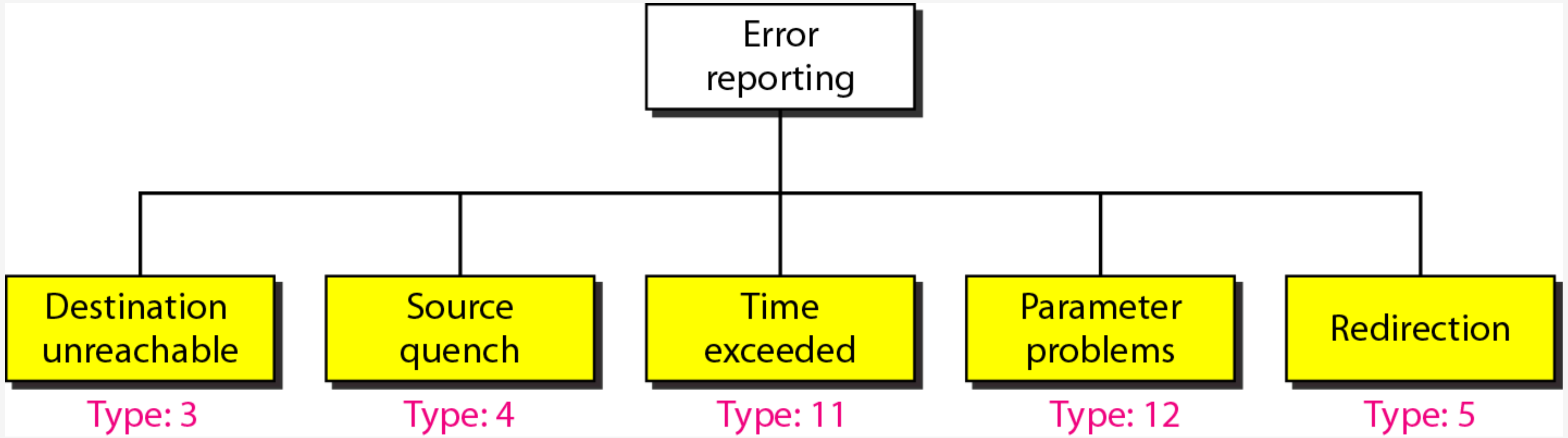
ICMP Encapsulation

ICMP messages are encapsulated in IP packets and sent.



ICMP ENCAPSULATION

Error-reporting messages



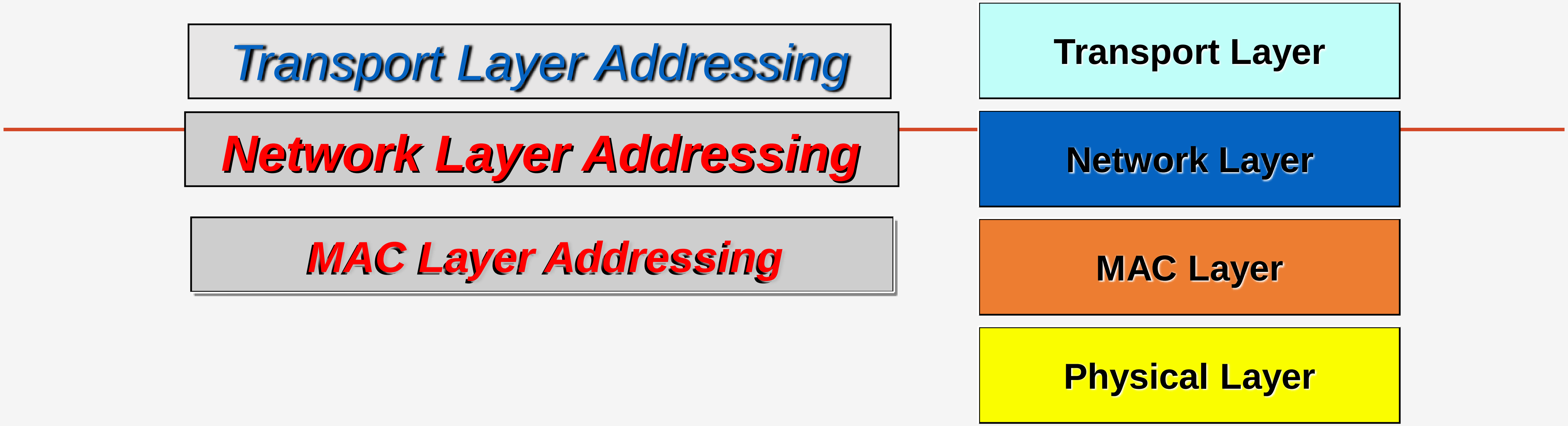
ICMP Messages

ICMP messages are sent in several situations:

- when a datagram cannot reach its destination.
- when the router does not have the buffering

  capacity to forward a datagram.
- when the router can direct the host to send traffic on a shorter route.
- when the packet has been in the network for very long time.
- when some specific information (subnet

  mask,timestamp, etc.) is needed.
- to reply to requests for information.
- to monitor whether a remote machine is up or not.



Transport Layer Addressing

Network Layer Addressing

MAC Layer Addressing

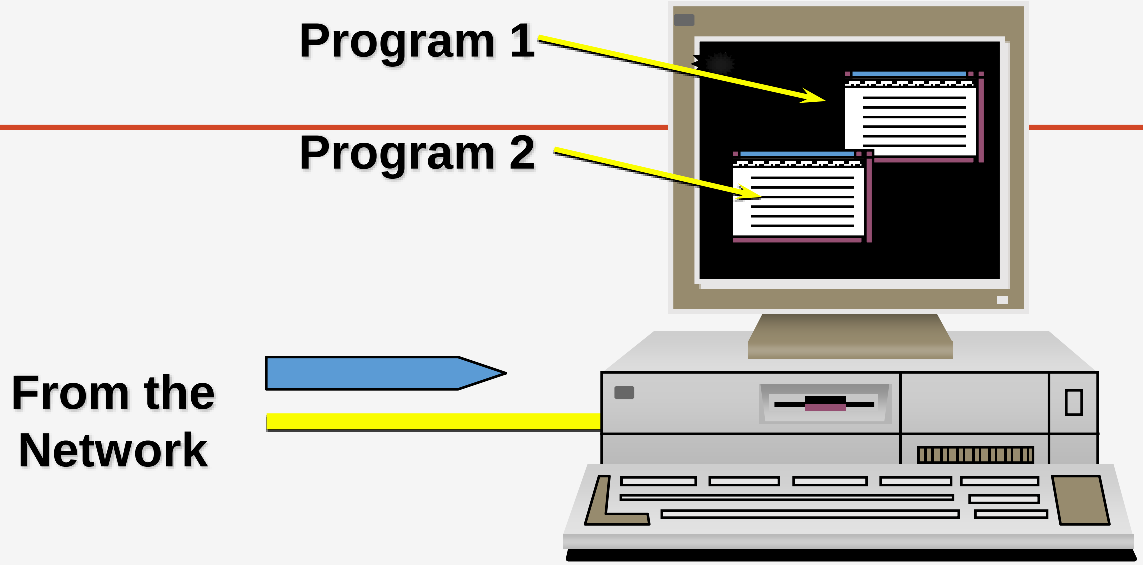
Transport Layer

Network Layer

MAC Layer

Physical Layer

- MAC Layer addressing allows us to transfer messages between two hosts on the same cable.
- Network Layer Addressing allows communication between hosts regardless of the type of network (or networks) that are used to connect the hosts.
- Transport Layer Addressing allows a specific application process running in a host computer to communicate with an equivalent process running in another host.



• Here we see a LAN frame heading towards a PC from the network. MAC and Network Layer addressing have got the frame this far, but now there's a problem.

• There are two possible communication programs running in the PC - Program 1 and Program 2.

• The MAC and IP addresses on the PC only identify the machine itself, not the program to which the packet should be sent.

* To differentiate between these programs, we use Transport Layer addressing.