CS540 - Network II - Chapter 01

1. Definitions

- **Protocol Architecture**: each layer performs a subset of functions, change in one layer should not require changes in other laywers. Key features: syntax, semantics, timing.
- The services between adjecent layers are expressed in terms of **primitives** (functions to be performed) and **parameters** (input/output, and control info).
  - Service Primitives

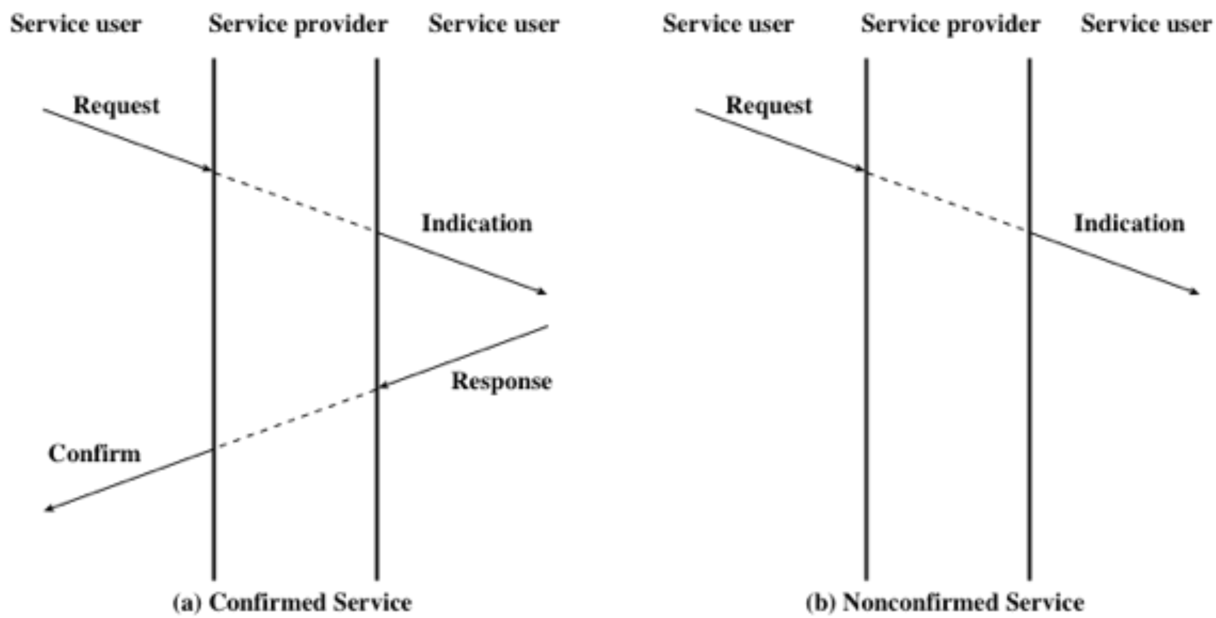


Figure 2.10 Time Sequence Diagrams for Service Primitives

- Socket is the **concatenation of a port value and an IP address**, and is **unique** through out the Internet. Categorized into stream sockets, datagram sockets and raw sockets.
- Elements of routing techniques for **Packet Switching Networks**

Performance Criteria Number of hops Cost Delay Throughput **Decision Time** Packet (datagram) Session (virtual circuit) **Decision Place** Each node (distributed) Central node (centralized) Originating node (source)	**Network Information Source** None Local Adjacent node Nodes along route All nodes **Network Information Update Timing** Continuous Periodic Major load change Topology change

- **AS (Autonomous System)**: is a set of routers and networks in a single organization**.** There is a path between any pair of nodes in AS.
- **IRP (Interior Router Protocol)**: a shared routing protocol for passing routing information **within an AS.**
- **ERP (Exterior Router Protocol)**: protocol use for passing routing information **between different ASs.**

Eg., BGP (Border Gateway Protocol), OSPF (Open Shortest Path First)

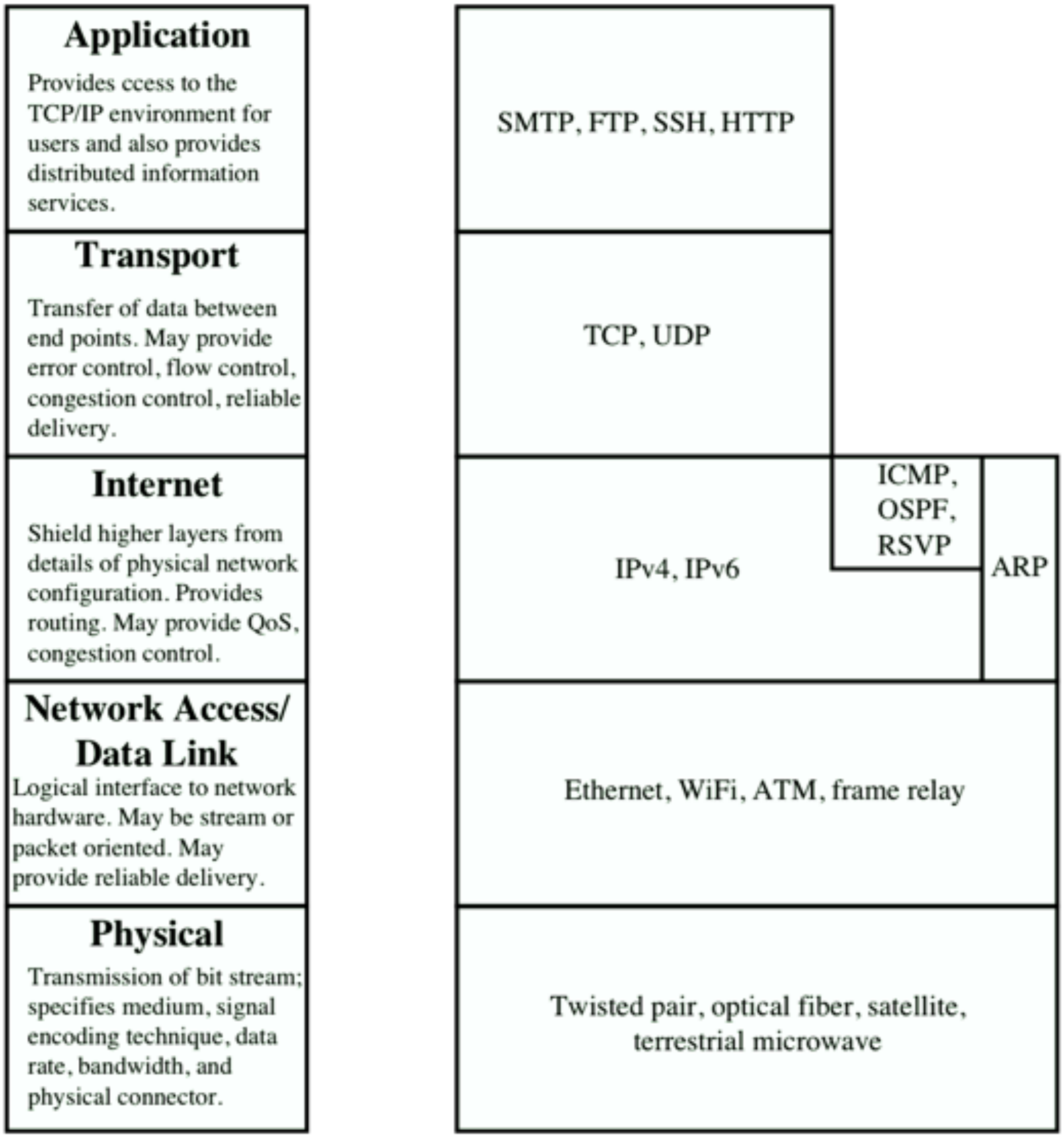
- **Internet Routing protocol** uses 3 approaches for gathering routing information:
  - **Distance-vector routing**: exchange of vector of **link costs** between each node and **its neighbors** (next hop). Used by RIP.
  - **Link-state routing**: the router determines the link cost **on each of its interfaces** and advertise **to ALL other routers** in the same network, <u>not just the neighbors</u>. This is a better version of Distance vector routing.
  - **Path-vector routing**: does not include a distance or cost est, but include the routing information list of all the ASs that need to be crossed in order to reach the destination. Usually used for security purpose (to avoid certain ASs) or for QOS (base on the quality metrics such as link speed, capacity).

2. Network Layers

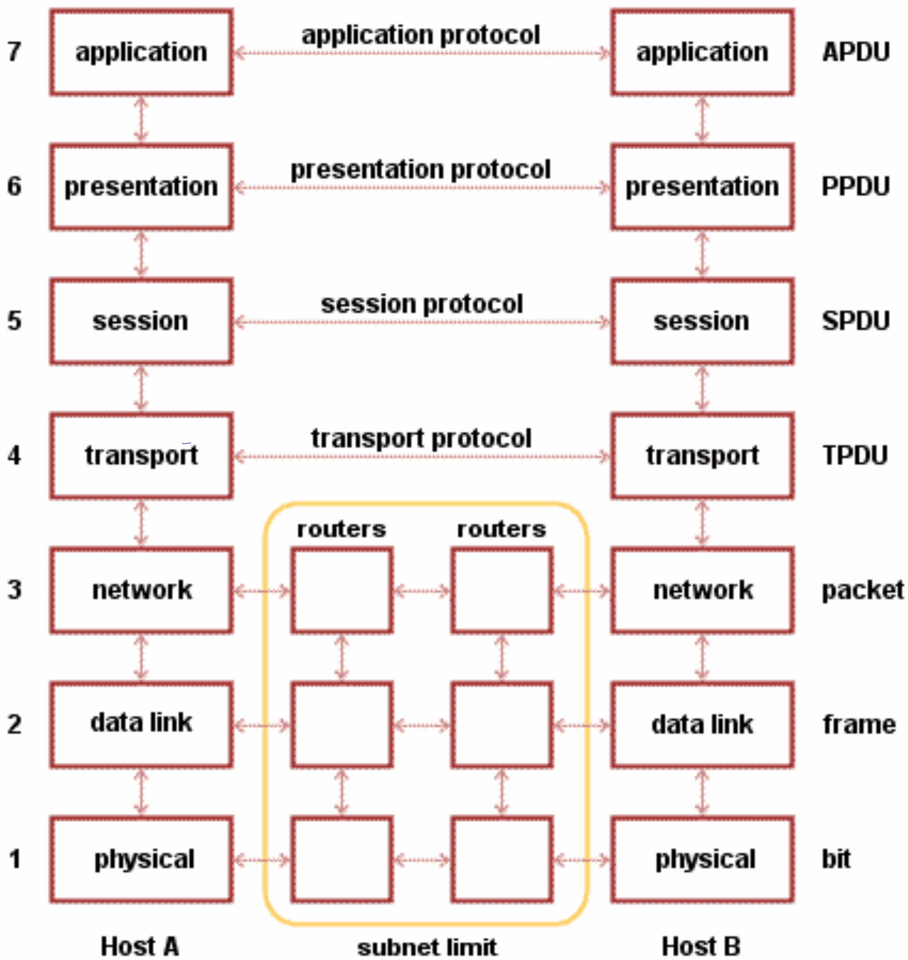
This section will go through the network layers from bottom up.

2.1. Some sample protocols/models

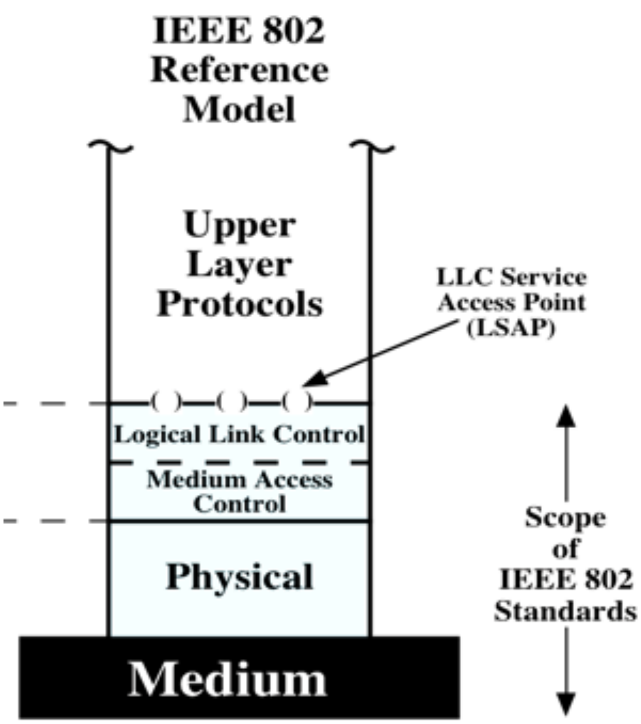
2.1.1. TCP/IP Layers and example protocols



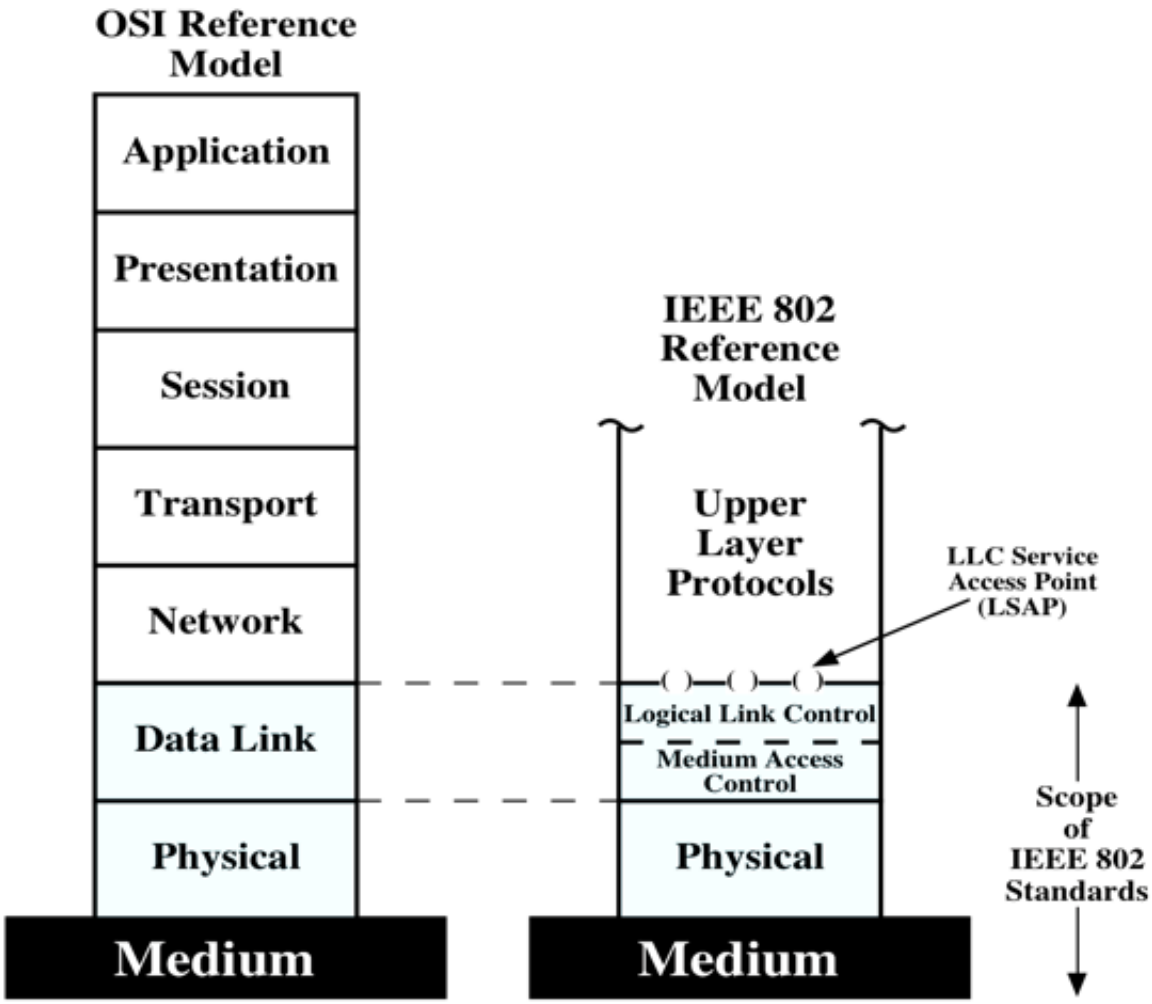
2.1.2. OSI Model



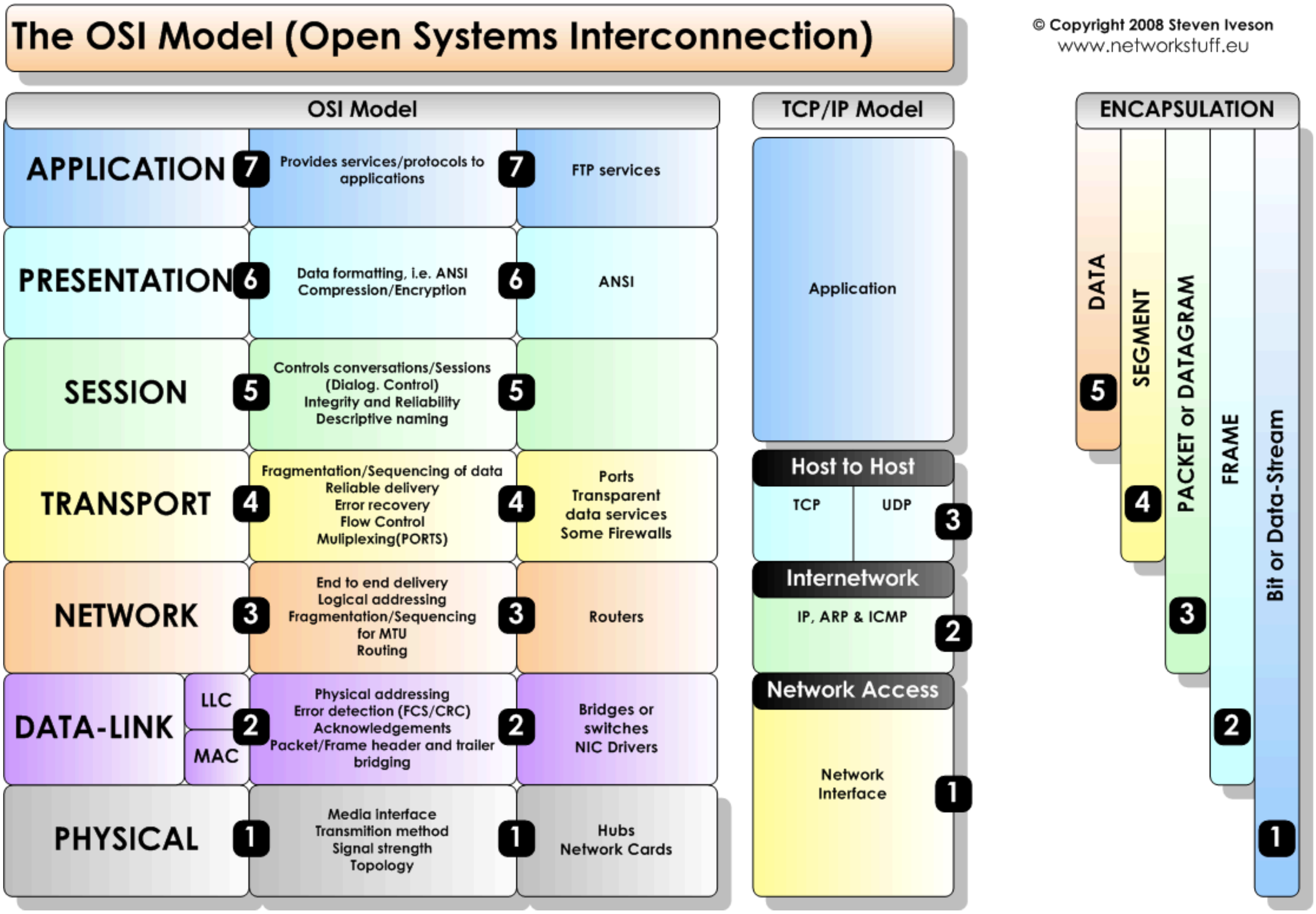
2.1.3. IEEE 802 Protocol Layers



2.1.4. OSI v/s IEEE 802



2.1.5. OSI v/s TCP/IP



Notes: in TCP/IP, sometimes Network Access also includes the Physical layer.

2.2. Physical layer

Has the same definition for OSI, IEEE 802 or TCP/IP.

It covers the **physical interface** between computer and network and concern with:

- Transmission Medium
- Nature of signals
- Data Rates

In **IEEE 802**, physical layer includes functions:

- Encoding/decoding of signals
- Preamble generation / removal (for synchronization)
- Bit transmission/reception

2.3. Network Access / Data Link Layer

Covers the **exchange of data** between an end system and the network, concerned with:

- **access and routing** of data between the system and the neighborhood networks.

This layer is equivalent to these layers in different protocols/schemes.

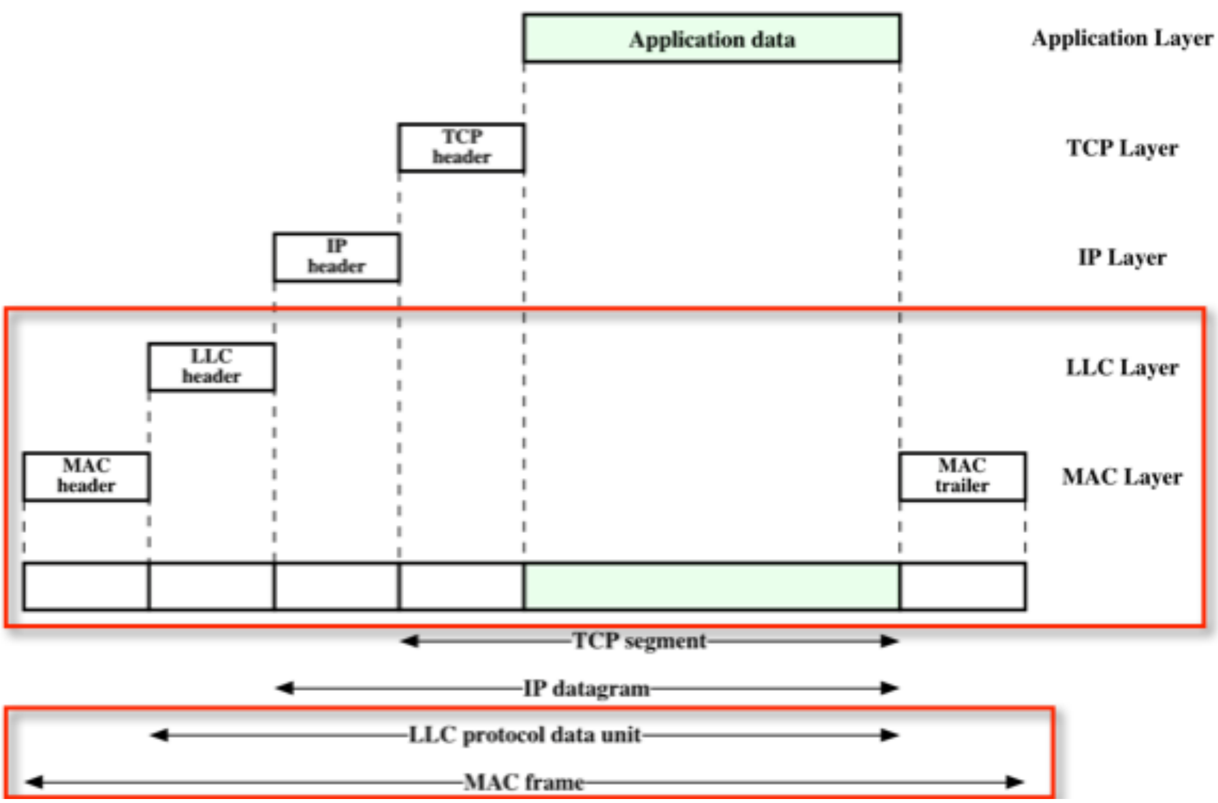
- Data Link (OSI)
- LLC / MAC [1] (IEEE 802)
- Network Access / Data Link (TCP/IP)

In **TCP/IP**, Network Access Layer can be Ethernet, Token Ring, Frame Relay, or ATM.

In **IEEE 802**, this layer consists of 2 sub-layers, from bottom up:

- **MAC** (Medium Access Control):
    - assembles data into frame on transmision
    - disassembles frame into data on reception
    - performs address recognition & error detection (NO flow control)
    - controls access to transmission medium
- **LLC** (Logical Link Control):
    - performs flow and error control.
    - provides interface to higher level by **service access points** (SAPs).

2.3.1. MAC and LLC data frame structure:

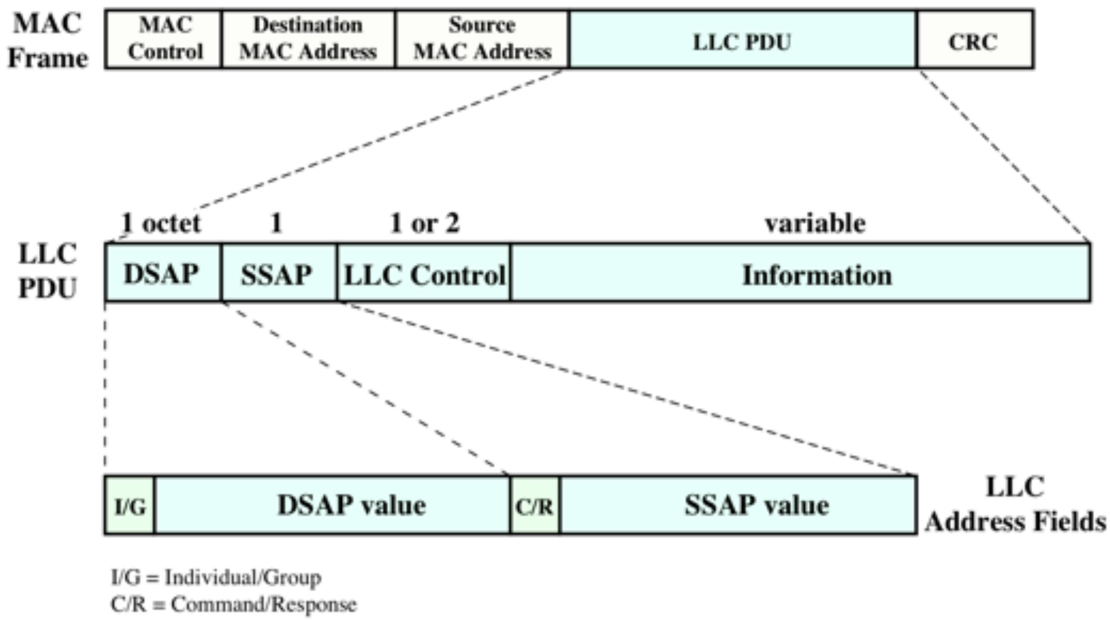


Notes:

- MAC has header and trailer (CRC), while

- LLC only has header.

2.3.2. LLC PDU (Protocol Data Unit) Structure:



2.3.3. MAC Protocol

- Control of access to transmission medium in 2 schemes:
  - **Centralized**: a controller is designated to grant access to network; or
  - **Distributed**: each station works out how it should transmit the data in order.
- Access control techniques using:
  - **Synchronous**: specific capapcity is dedicated to a connection. Similar approach used in Circuit Switching, FDM, and TDM.
  - **Asynchronous**: dynamic allocation of capacity on demand, subdivided into 2 cats: round robin, reservation, and contention.

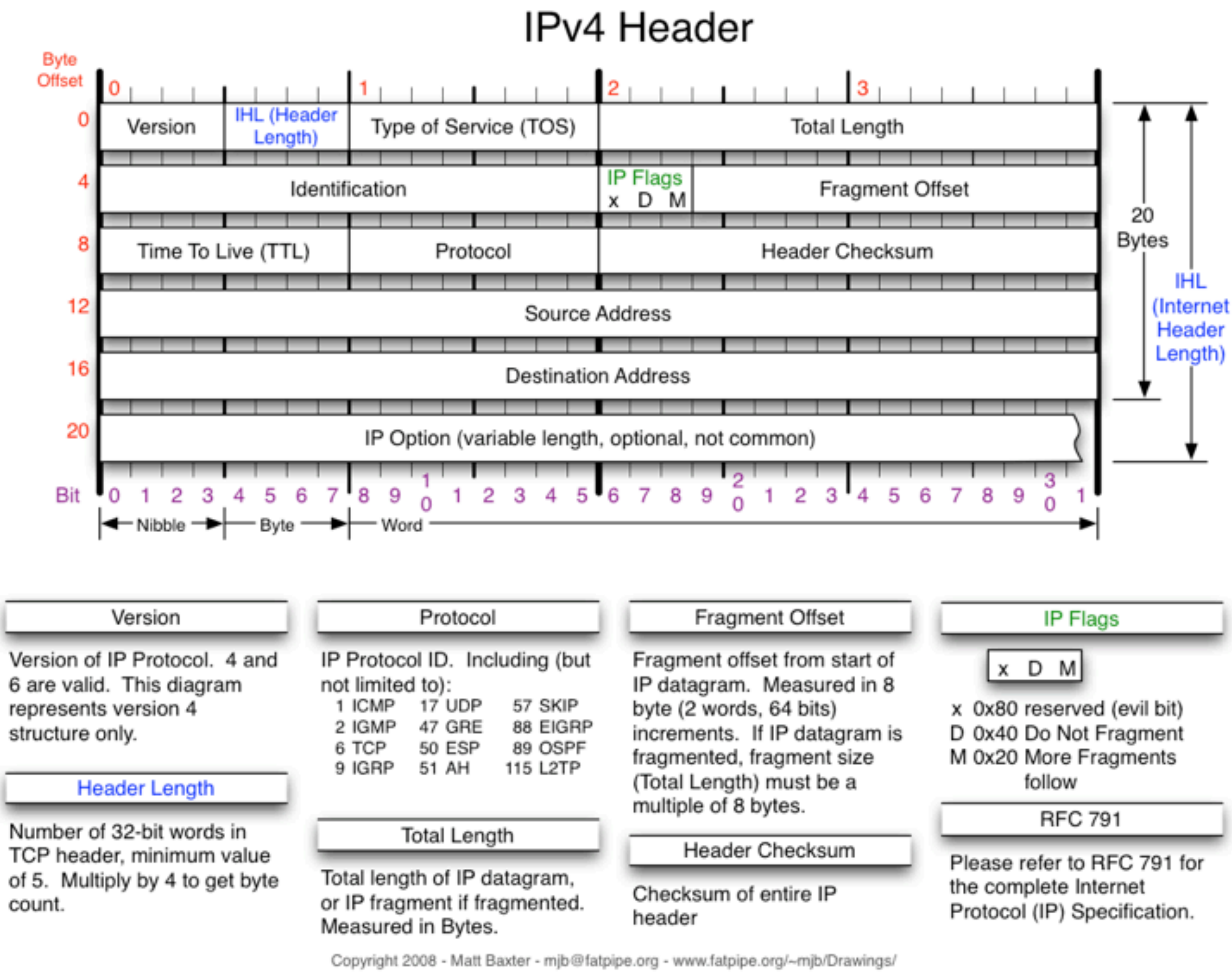
MAC frame fields:

2.4. Internet Layer

- named Internet Layer (TCP/IP), or Network layer (OSI)
- use **IP (Internet Protocol)** to provide routing function across multiple networks.
  - Some **IP design issues**:
    - Routing, includes:
      - a **routing table** (dynamic, static) is maintained on each node.

            - a routing technique called **Source Routing** can also be used to predefine a special path.
            - a service called **Route Recording**, useful for testing and debugging.
        - Datagram lifetime: prevent looping.
        - Fragmentation and reassembly: break the data up into smaller blocks, for effecient transmission.
        - Error control: discard datagrams if lifetime expires, congestion or FCS error.
        - Flow control: allows routers to limit the data rate they receive, using ICMP messages, usually when destination unreacheable, time exceeded, parameters problem,, source quench, redirect, echo, address mask request/response or timestamp.
    - **IP Services**:
        - the **primitives** specify the function to be performed, and
        - the **parameters** are used to pass data and control info. These parameters are defined in the IP header.
        - other IP Options (extended after the Header) are security, source routing, route recording, stream identification and timestamping.
- use **ARP (Address Resolution Protocol)** to convert an IP address into a physical address (MAC address), usually on the last hop to deliver the data to the correct host. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
- connectionless operation at the Internet Protocol (IP) level.
    - <u>Advantage</u>: flexible, can be made robust, no unecessary overhead.
-

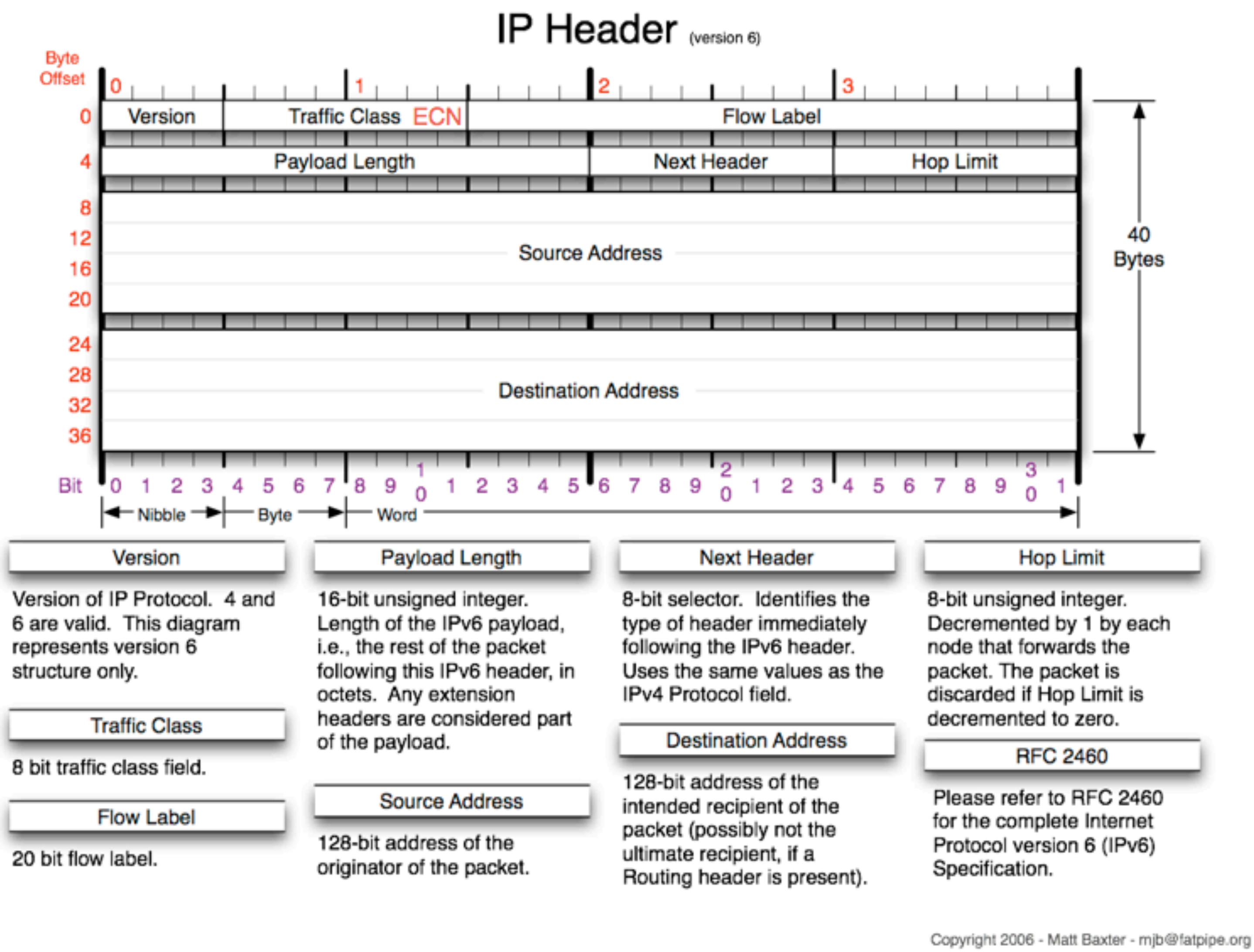
2.4.1. IPv4 Header



Notes:

- IPv4 Header size is 20 bytes (or 20 octets)
- Source address, destination address occupies 4 bytes (32 bits) each.
- each row is 4 bytes

2.4.2. IPv6 Header



Notes:

- IPv6 Header size is 40 bytes (or 40 octets), twice the size of IPv4 Header.
- Source address, destination address occupies 16 bytes (128 bits) each.
- Fragmentation is removed from main header (moved to extension header).
- each row is 4 bytes

2.4.2.1. IPv6 Enhancements

- 128 bit address space
- improves option mechanism with extension headers
- dynamic address assignment
- introduces anycast (one of a set of interface addresses) and multicast (all of a set of interfaces)
- flow label: to relate sequence of packets that have the same flow, or special handling of packets.

IPv6 from an IPv4 Perspective

List and order of IPv6 extension headers

Order	Header	Code	Description
1	Basic IPv6 header		
2	Hop-by-hop options	0	Examined by all hosts in path
3	Destination options	60	Examined only by destination node
4	Routing	43	Specify the route for a datagram (mobile v6)
5	Fragment	44	Fragmentation parameters
6	Authentication (AH)	51	Verify packet authenticity
7	ESP	50	Encrypted data
8	Destination options	60	Examined only by destination node
9	Mobility	135	Parameters for use with mobile IPv6

2.4.3. Example of Internet Protocol Operation

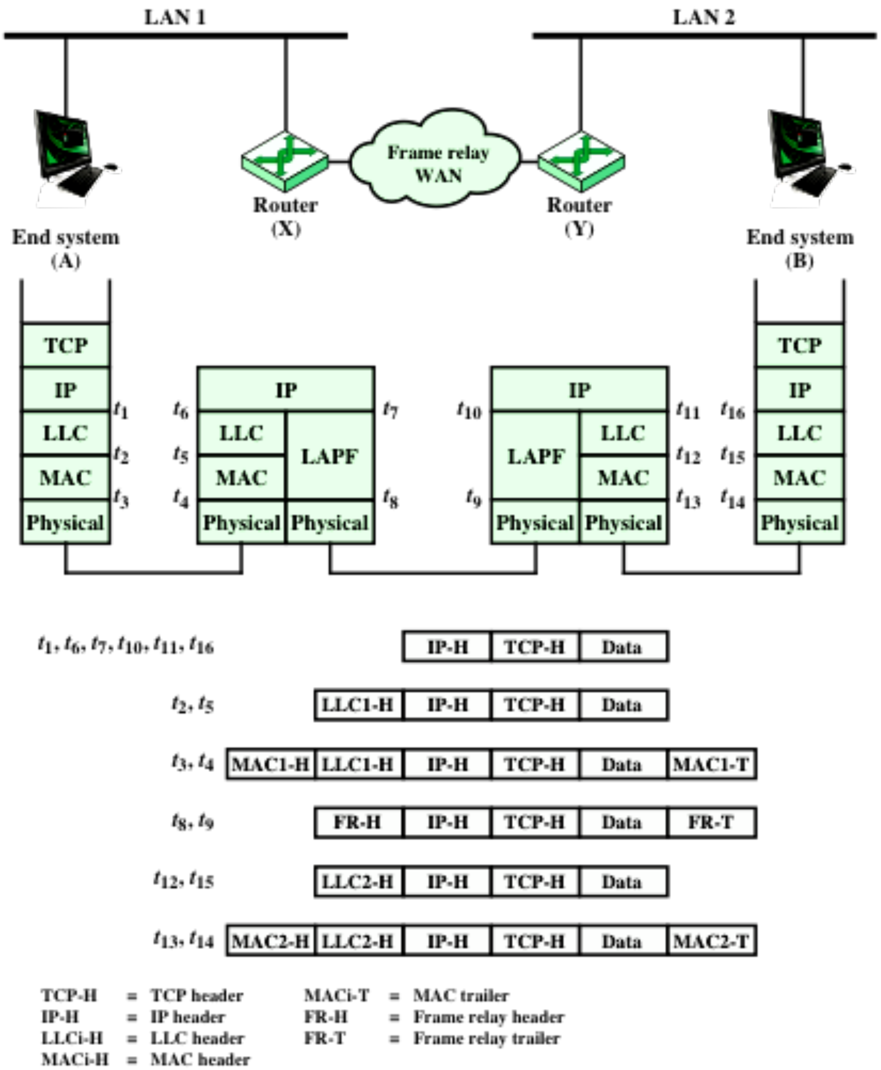


Figure 14.2 Example of Internet Protocol Operation

Notes:

- No change to IP Header, only change at MAC, LLC, FR.

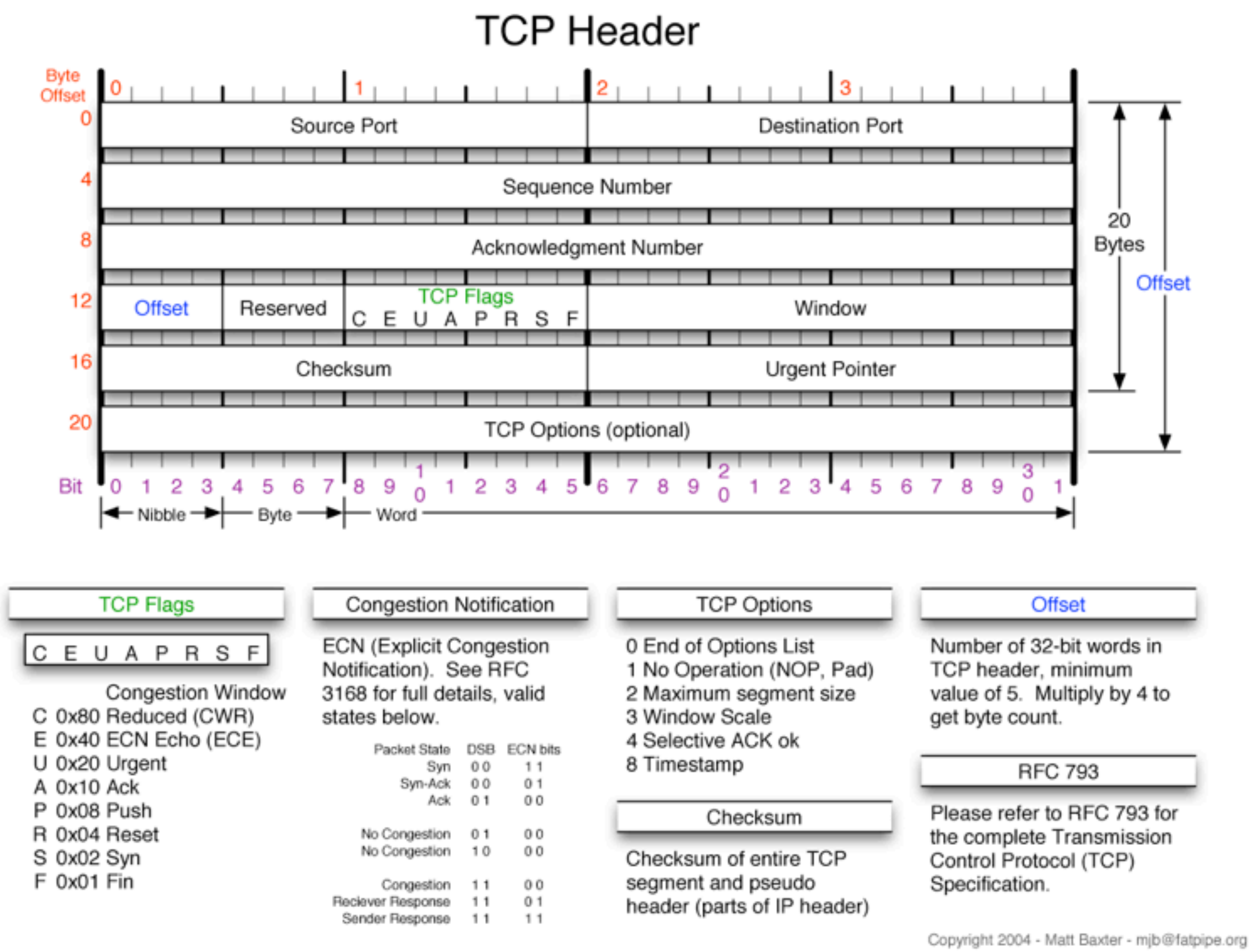
2.5. Transport Layer

- uses the same name in both TCP/IP and OSI.
- provides reliable end-to-end service (TCP) or unreliable service (UDP)

2.5.1. TCP – Transmission Control Protocol

- Transport layer protocol used by most applications.
- Reliable, connection oriented to deal with these issues: addressing, multiplexing, flow control, and connection establishment/termination.
- Basic protocol unit is TCP segment

- Seven issues to be addressed in TCP
    - Ordered delivery
    - Retransmission strategy
    - Duplicate detection
    - Flow control
    - Connection establishment
    - Connection termination
    - Failure recovery



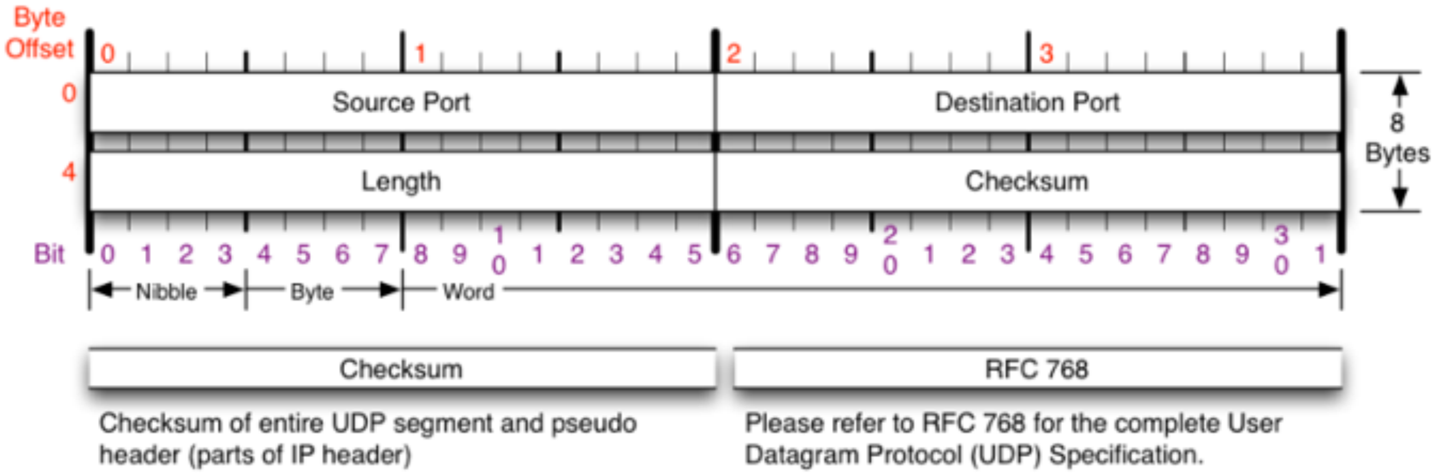
<u>Notes:</u>

- TCP Header size is 20 bytes (similar to IPv4 header)
- each row is 4 bytes

2.5.2. UDP - User Datagram Protocol

- **Unreliable**, **no guarantee** of delivery, order, or duplication.

- **Connectionless** (datagram service), fast, small header.
- Usually used for SNMP.
- Has a CRC check, but optional.



3. Don’t know where to put yet

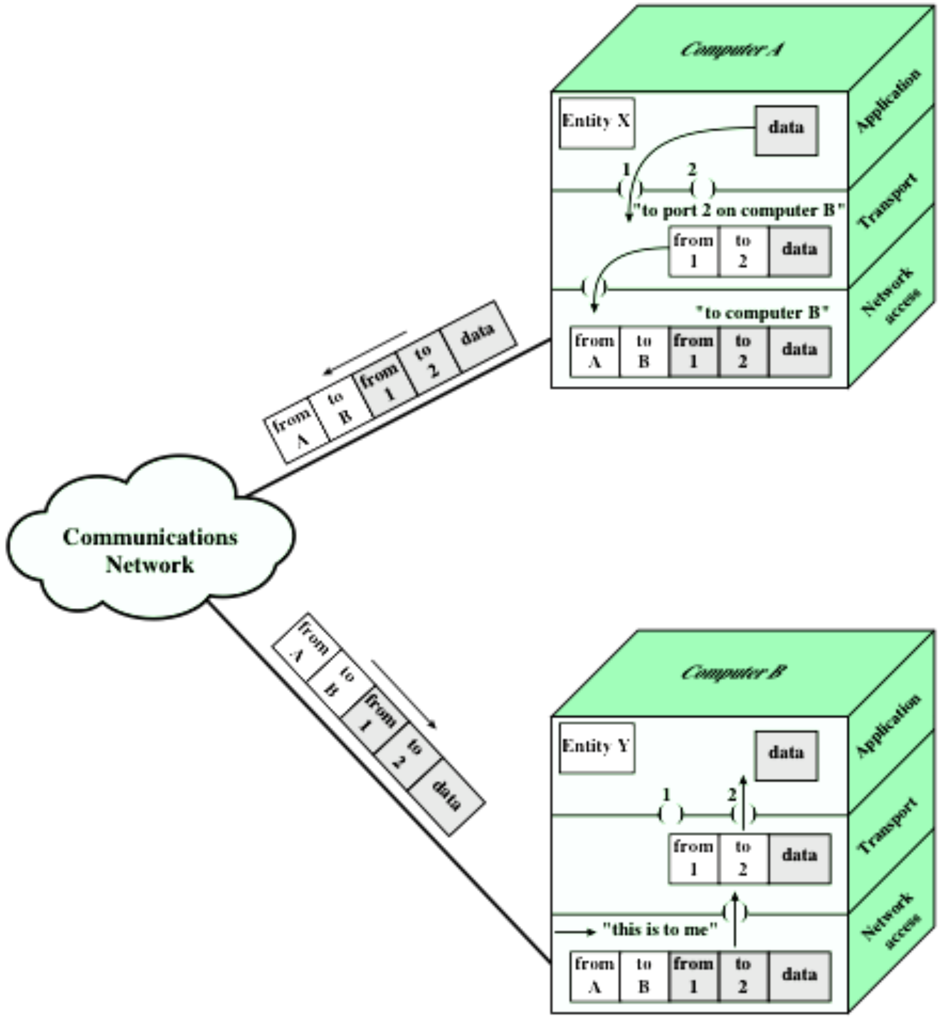
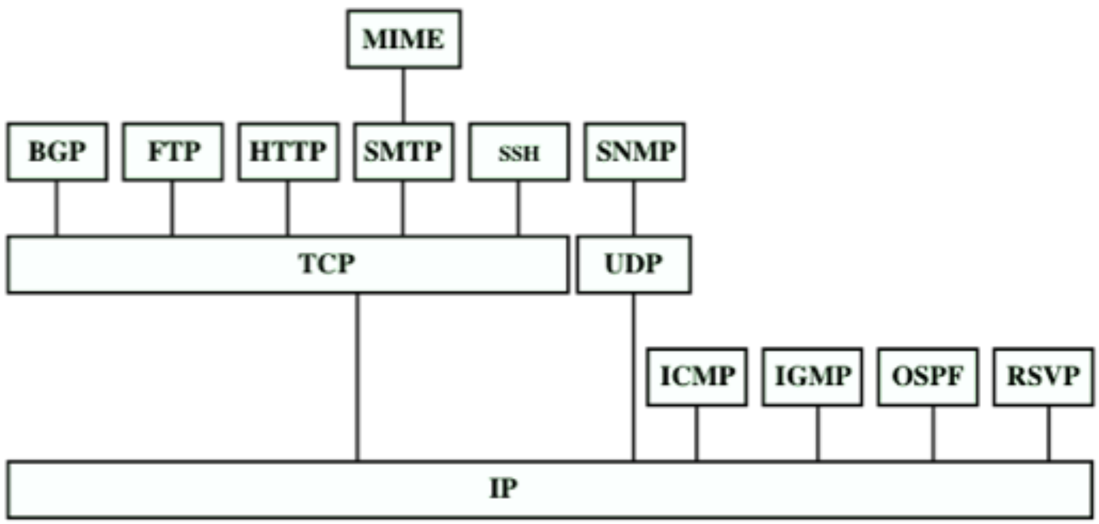


Figure 2.2 Protocols in a Simplified Architecture



BGP	=	Border Gateway Protocol	OSPF	=	Open Shortest Path First
FTP	=	File Transfer Protocol	RSVP	=	Resource ReSerVation Protocol
HTTP	=	Hypertext Transfer Protocol	SMTP	=	Simple Mail Transfer Protocol
ICMP	=	Internet Control Message Protocol	SNMP	=	Simple Network Management Protocol
IGMP	=	Internet Group Management Protocol	SSH	=	Secure Shell
IP	=	Internet Protocol	TCP	=	Transmission Control Protocol
MIME	=	Multipurpose Internet Mail Extension	UDP	=	User Datagram Protocol

Figure 2.8 Some Protocols in the TCP/IP Protocol Suite

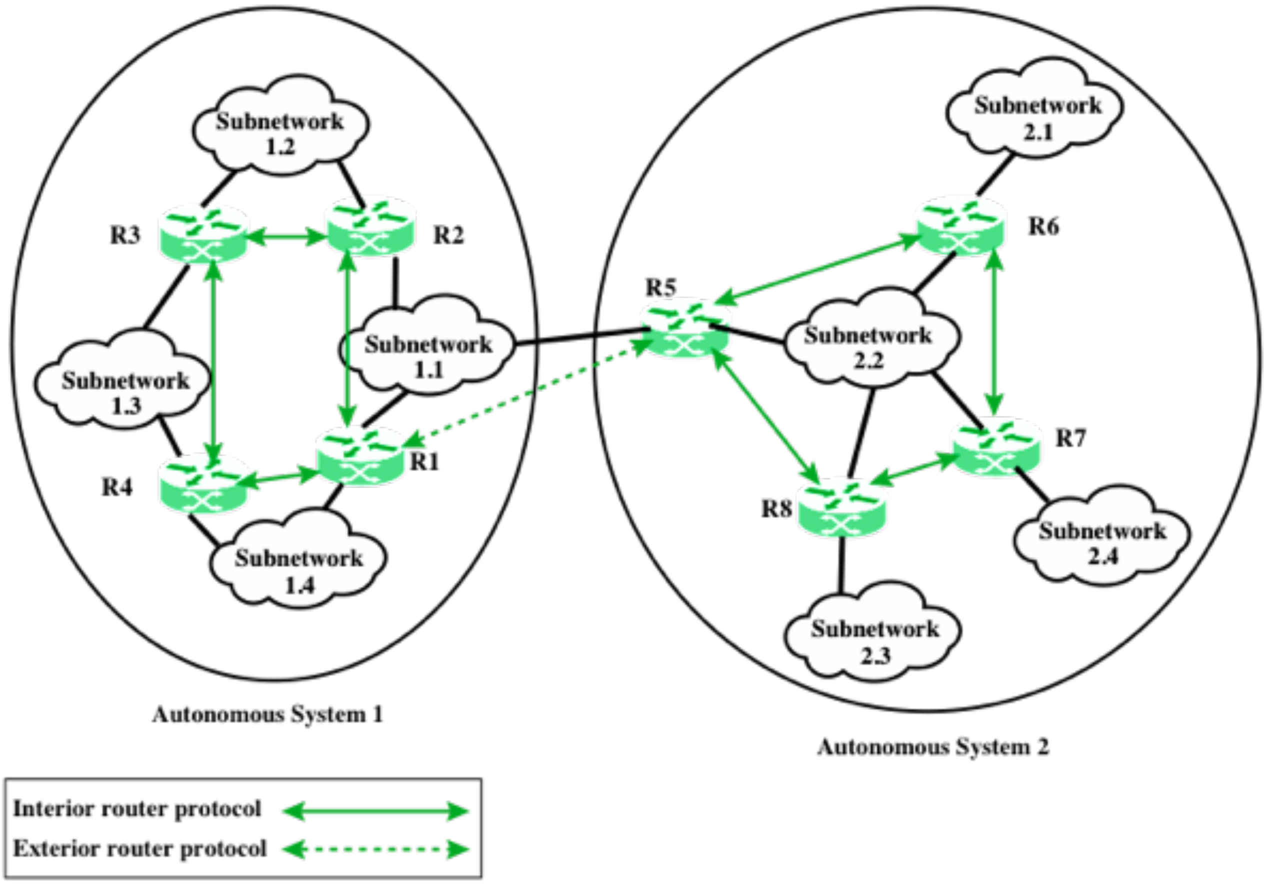


Figure 19.9 Application of Exterior and Interior Routing Protocols

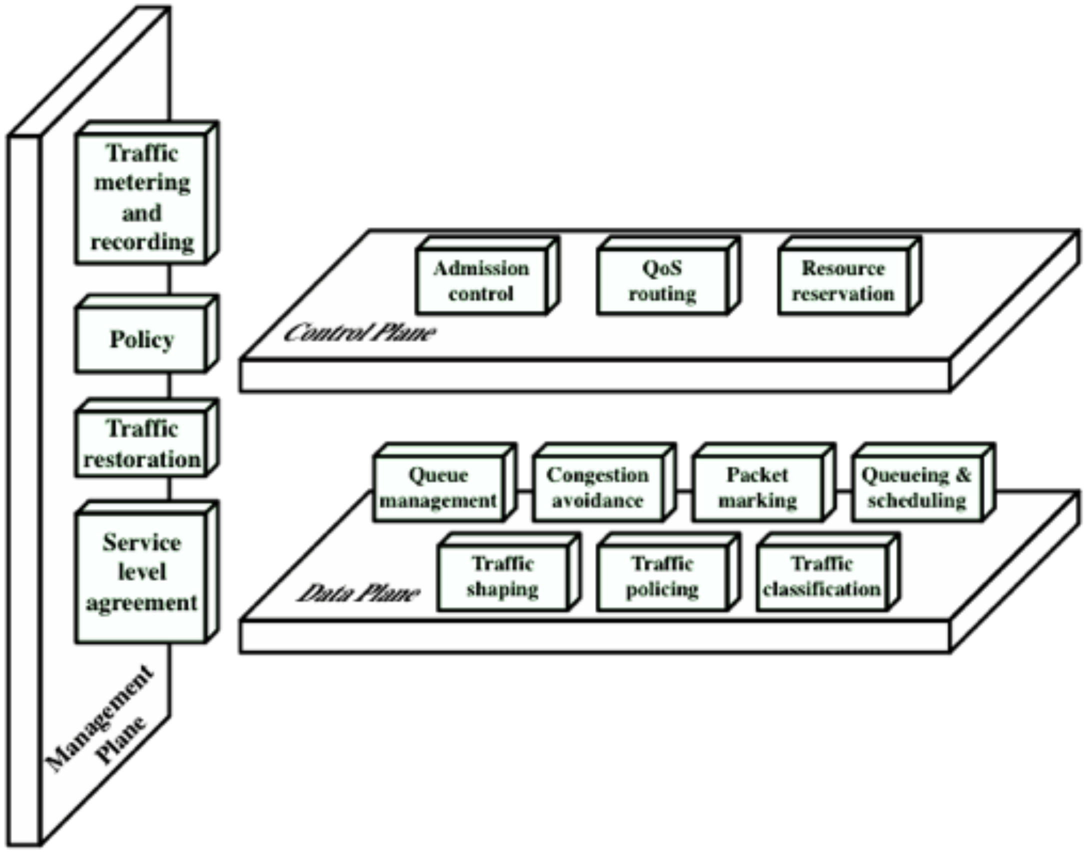


Figure 22.1 Architectural Framework for QoS Support

---

1. LLC: Logical Link Control, MAC: Medium Access Control. ↩