Topic 6: Network and Transport Layers

- Chapter 4 : TCP/IP and OSI

Business Data Communications, 4e

Outline

- Introduction
- OSI Model
- TCP/IP Model
- IPv4 vs. IPv6

What is a Protocol?

- A standard that allows entities (i.e. application programs) from different systems to communicate
- Shared conventions for communicating information
- Includes syntax, semantics, and timing

Standardized Protocol Architectures

- Vendors like standards because they make their products more marketable
- Customers like standards because they enable products from different vendors to interoperate
- Two protocol standards are well-known:
  - TCP/IP: widely implemented
  - OSI: less used, still useful for modeling/conceptualizing

Internet Standards

- Email related standards
  - IMAP, POP, X.400, SMTP, CMC, MIME, binhex, uuencode
- Web related standards
  - http, CGI, html/xml/vrml/sgml
- Internet directory standards
  - X.500, LDAP
- Application standards
  - http, FTP, telnet, gopher, wais
- Videoconferencing standards
  - H.320, H.323, Mpeg-1, Mpeg-2

*Telecommunication Standards Organizations

- International Telecommunications Union - Telecommunication Standardization Sector (**ITU-TSS**). Formerly called the Consultative Committee on International Telegraph and Telephone (**CCITT**)
- International Organization for Standards (**ISO**). Member of the ITU, makes technical recommendations about data communications interfaces.
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (**IEEE**)
- Internet Engineering Task Force (**IETF**)
- Electronic Industries Association (EIA)
- National Institute of Standards and Technology (NIST)
- National Exchange Carriers Association (NECA)
- Corporation for Open Systems (COS)
- Electronic Data Interchange -(EDI) of Electronic Data Interchange for Administration Commerce and Transport (EDIFACT).

*Internet Engineering Task Force

A protocol proposed by a vendor

IETF working group study the proposal

IETF issues a request for comment (RFC)

IETF reviews the comments

IETF proposes an improved RFC

The RFC becomes a proposed standard

The proposed standard becomes a draft standard if two or more vendors adopt it

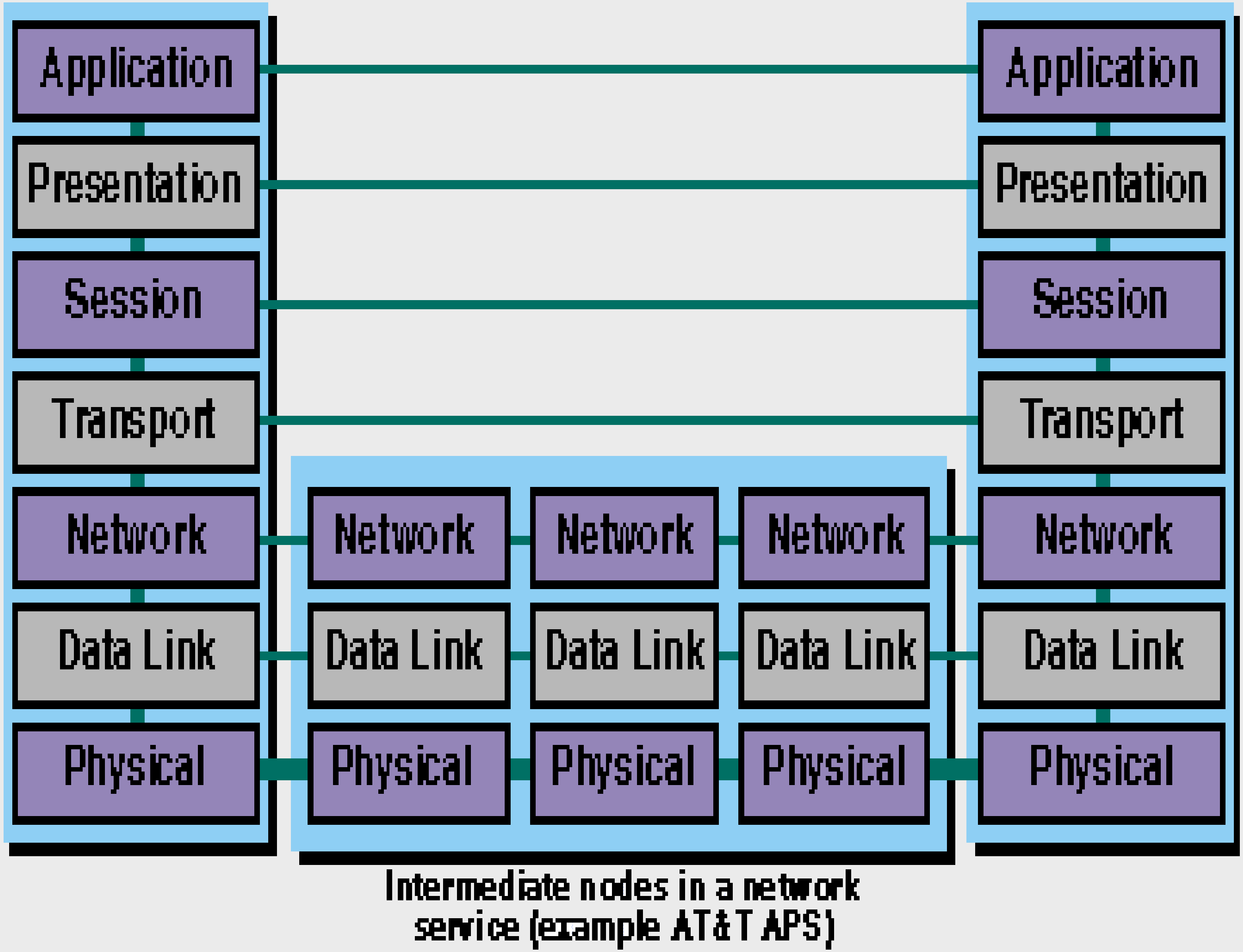
What is OSI?

- Developed by the International Organization for Standardization (ISO) in 1984
- The primary architectural model for intercomputer communications.
- A conceptual model composed of seven layers, each specifying particular network functions.
- Describes how information from a software application in one computer moves through a network medium to a software application in another computer.

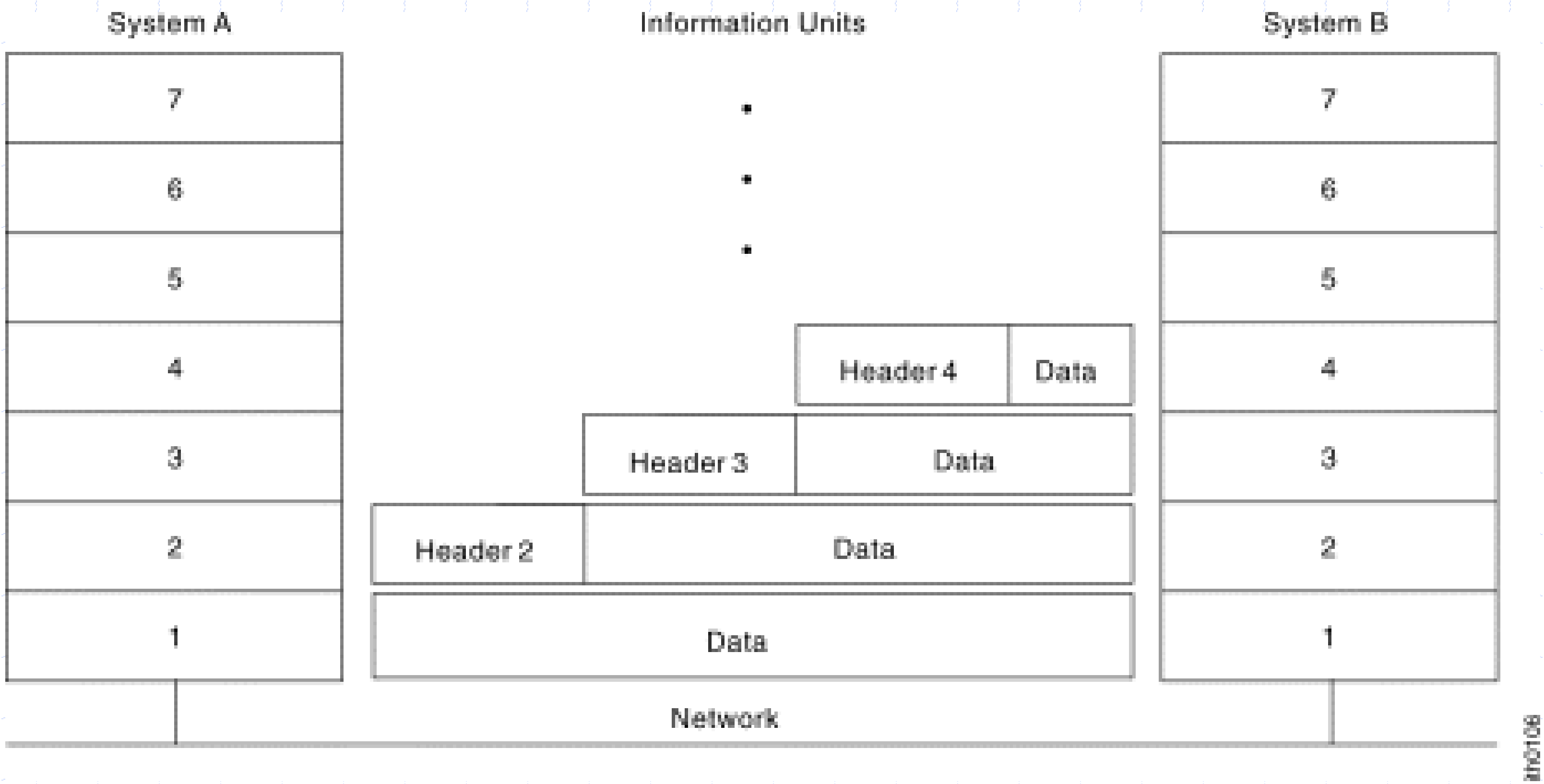
Why Study OSI?

- Still an excellent model for conceptualizing and understanding protocol architectures
- Key points:
  - Modular
  - Hierarchical
  - Boundaries between layers=interfaces

OSI Stack


Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Presentation
Session
Transport
Network
Data Link
Physical
Network
Data Link
Physical
Network
Data Link
Physical
Network
Data Link
Physical
Intermediate nodes in a network service (example AT&T APS)

Headers and Data



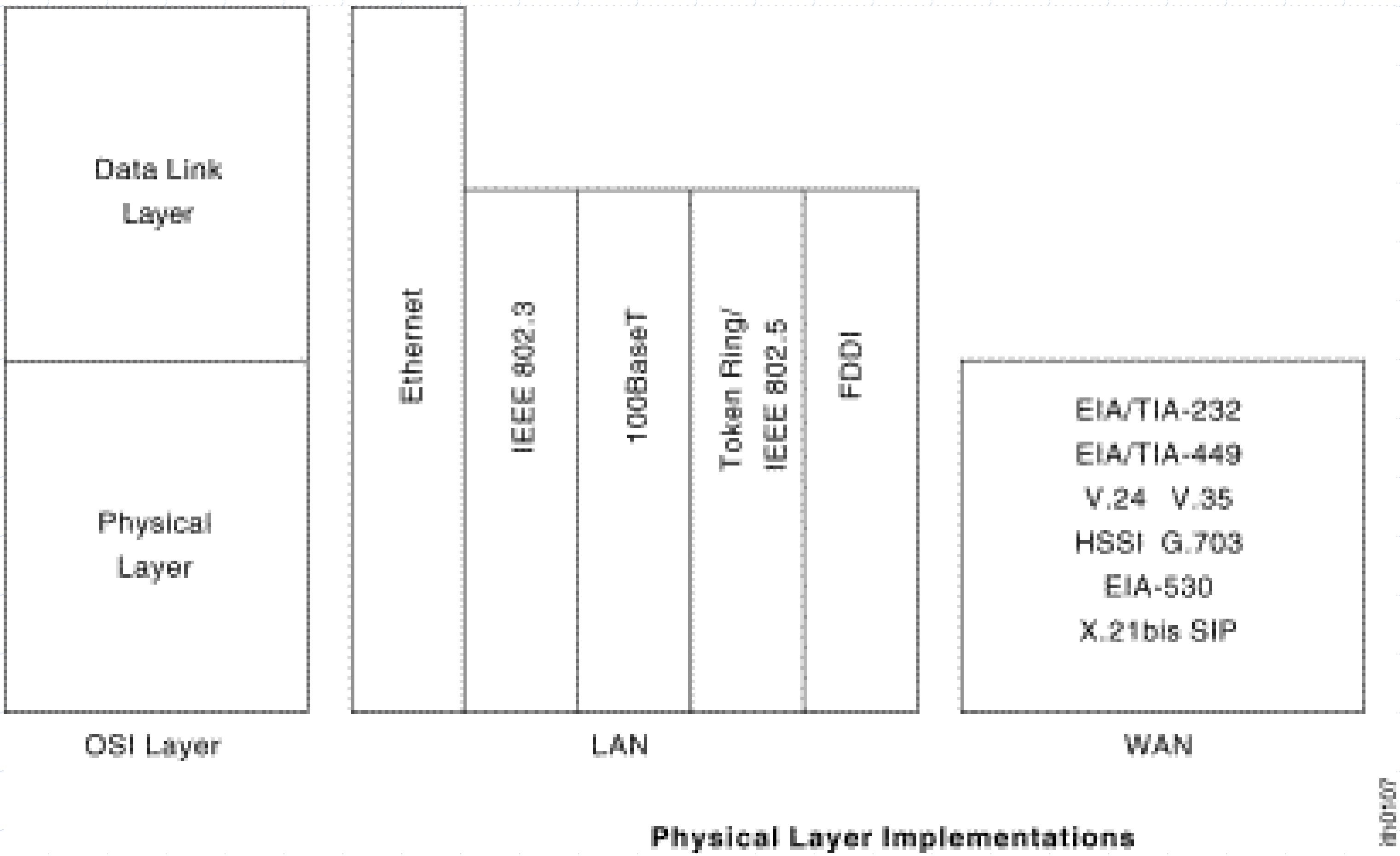
OSI Lower Layers

- Physical – Layer 1
- Data Link – Layer 2
- Network – Layer 3

OSI Physical Layer

- Responsible for transmission of bits
- Always implemented through hardware
- Encompasses mechanical, electrical, and functional interfaces
- e.g. RS-232

*Physical-layer Implementation

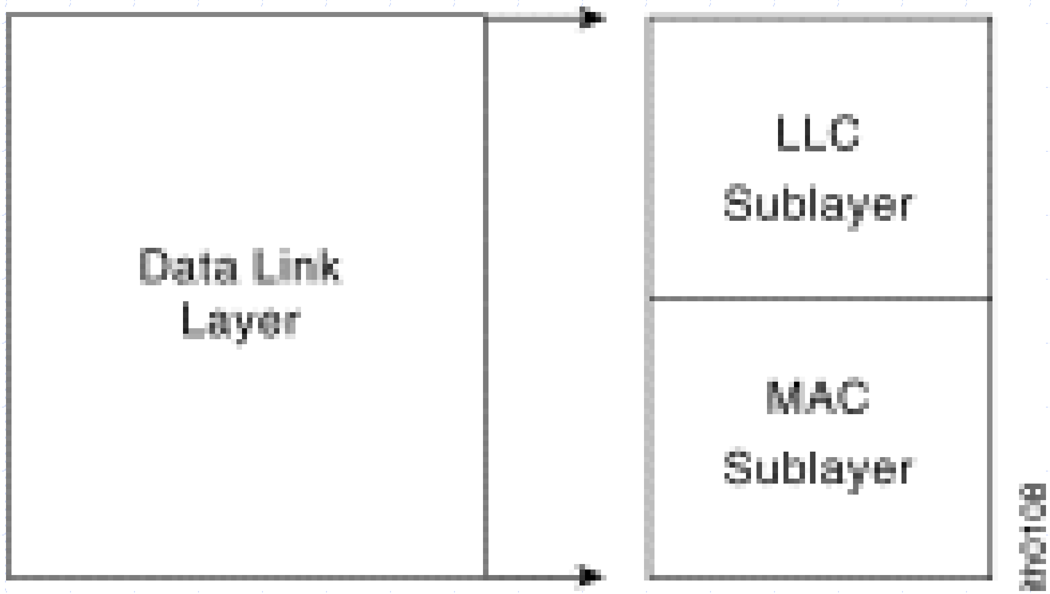


Physical Layer Implementations

OSI Data Link Layer

- Responsible for error-free, reliable transmission of data
- Flow control, error correction
- e.g. HDLC

OSI Data Link Layer



IEEE has subdivided data link layer into two sub-layers.

OSI Network Layer

- Responsible for routing of messages through network
- Concerned with type of switching used (circuit v. packet)
- Handles routing between networks, as well as through packet-switching networks

Network Access Layer

- Concerned with exchange of data between computer and network
- Includes addressing, routing, prioritizing, etc
- Different networks require different software at this layer
- Example: X.25 standard for network access procedures on packet-switching networks

OSI Upper Layers

- Transport
- Session
- Presentation
- Application

OSI Transport Layer

- Isolates messages from lower and upper layers
- Breaks down message size
- Monitors quality of communications channel
- Selects most efficient communication service necessary for a given transmission

Transport Layer

- Concerned with reliable transfer of information between applications
- Independent of the nature of the application
- Includes aspects like flow control and error checking

OSI Session Layer

- Establishes logical connections between systems
- Manages log-ons, password exchange, log-offs
- Terminates connection at end of session

OSI Presentation Layer

- Provides format and code conversion services
- Examples
  - File conversion from ASCII to EBDIC
  - Invoking character sequences to generate bold, italics, etc on a printer

OSI Application Layer

- Provides access to network for end-user
- User’s capabilities are determined by what items are available on this layer
- Logic needed to support various applications
- Each type of application (file transfer, remote access) requires different software on this layer

Application Viewpoint of a Network

- Distributed data communications involves three primary components:
  - Networks
  - Computers
  - Applications
- Three corresponding layers
  - Network access layer
  - Transport layer
  - Application layer

TCP/IP

- Transmission control Protocol/Internet Protocol
- Developed by DARPA
- No official protocol standard
- Can identify five layers
  - Application
  - Host-to-Host (transport)
  - Internet
  - Network Access
  - Physical

An OSI View of TCP/IP

Internet Model

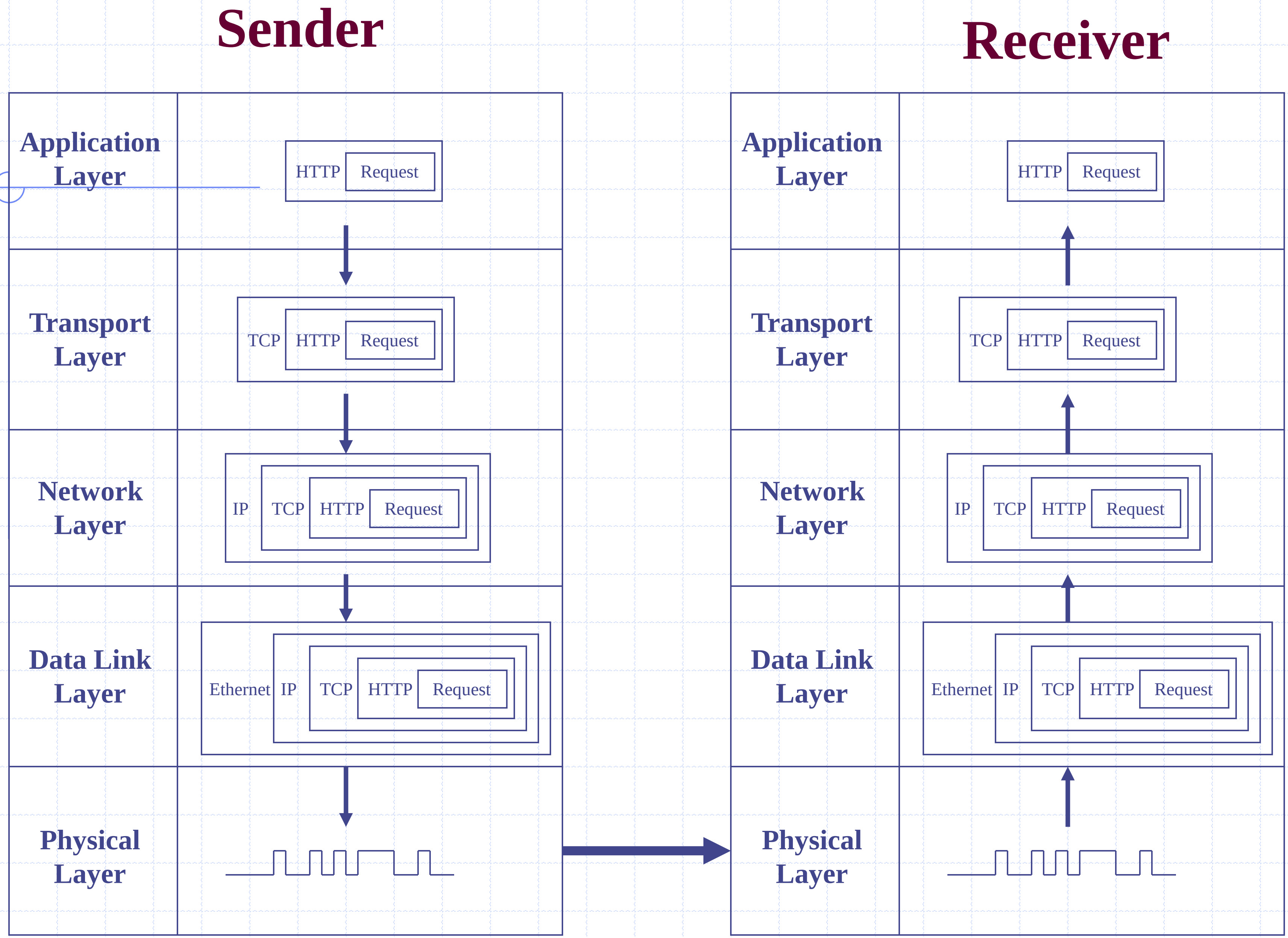
- Application (http, telnet, snmp, smtp, nfs, ftp)
- Transport (TCP, UDP)
- Internet (IPv4/IPv6)
- Network Access
- Physical layer

OSI Model

- Application
- Presentation
- Session
- Transport
- Network
- Data Link (HDLC)
- Physical

F-D's Model

- Application layer
- Network layer
- Data Link layer
- Physical layer


Sender
Receiver
Application Layer
HTTP Request
Transport Layer
TCP HTTP Request
Network Layer
IP TCP HTTP Request
Data Link Layer
Ethernet IP TCP HTTP Request
Physical Layer
Application Layer
HTTP Request
Transport Layer
TCP HTTP Request
Network Layer
IP TCP HTTP Request
Data Link Layer
Ethernet IP TCP HTTP Request
Physical Layer

TCP/IP Network Access Layer

- Exchange of data between end system and network
- Address of host and destination
- Prioritization of transmission
- Software at this layer depends on network (e.g. X.25 vs. Ethernet)
- Segregation means that no other software needs to be concerned about net specifics

TCP/IP Internet Layer

- An Internet is an interconnection of two or more networks
- Internet layer handles tasks similar to network access layer, but between networks rather than between nodes on a network
- Uses IP for addressing and routing across networks
- Implemented in workstations *and* routers

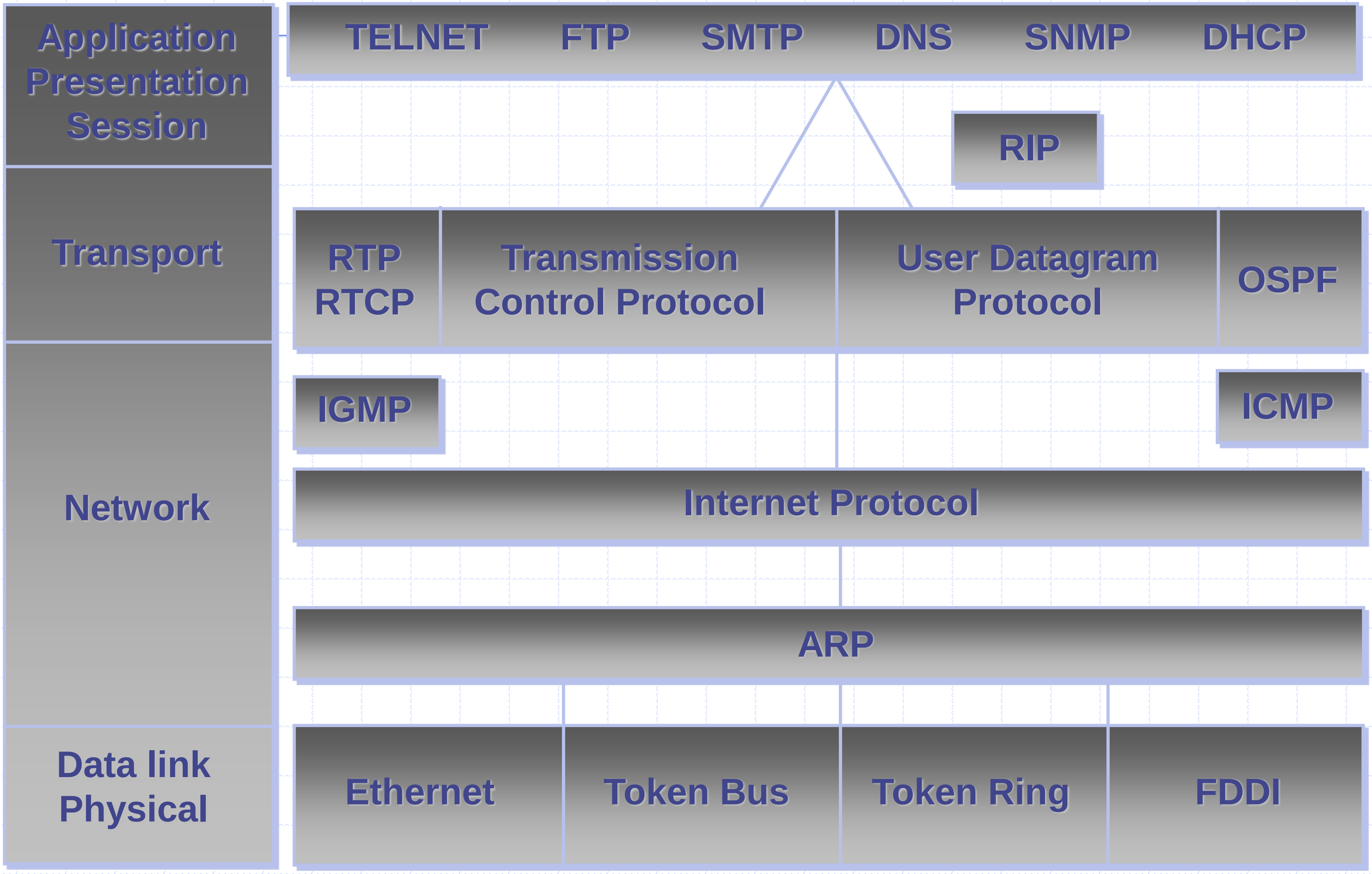
TCP/IP Transport Layer

- Also called host-to-host layer
- Reliable exchange of data between applications
- Uses TCP protocols for transmission

TCP/IP Application Layer

- Logic needed to support variety of applications
- Separate module supports each type of application (e.g. file transfer)
  - FTP
  - HTTP
  - Telnet
  - News
  - SMTP

*TCP/IP


Application
Presentation
Session
Transport
Network
Data link
Physical
TELNET
FTP
SMTP
DNS
SNMP
DHCP
RIP
RTP
RTCP
Transmission
Control Protocol
User Datagram
Protocol
OSPF
IGMP
ICMP
Internet Protocol
ARP
Ethernet
Token Bus
Token Ring
FDDI

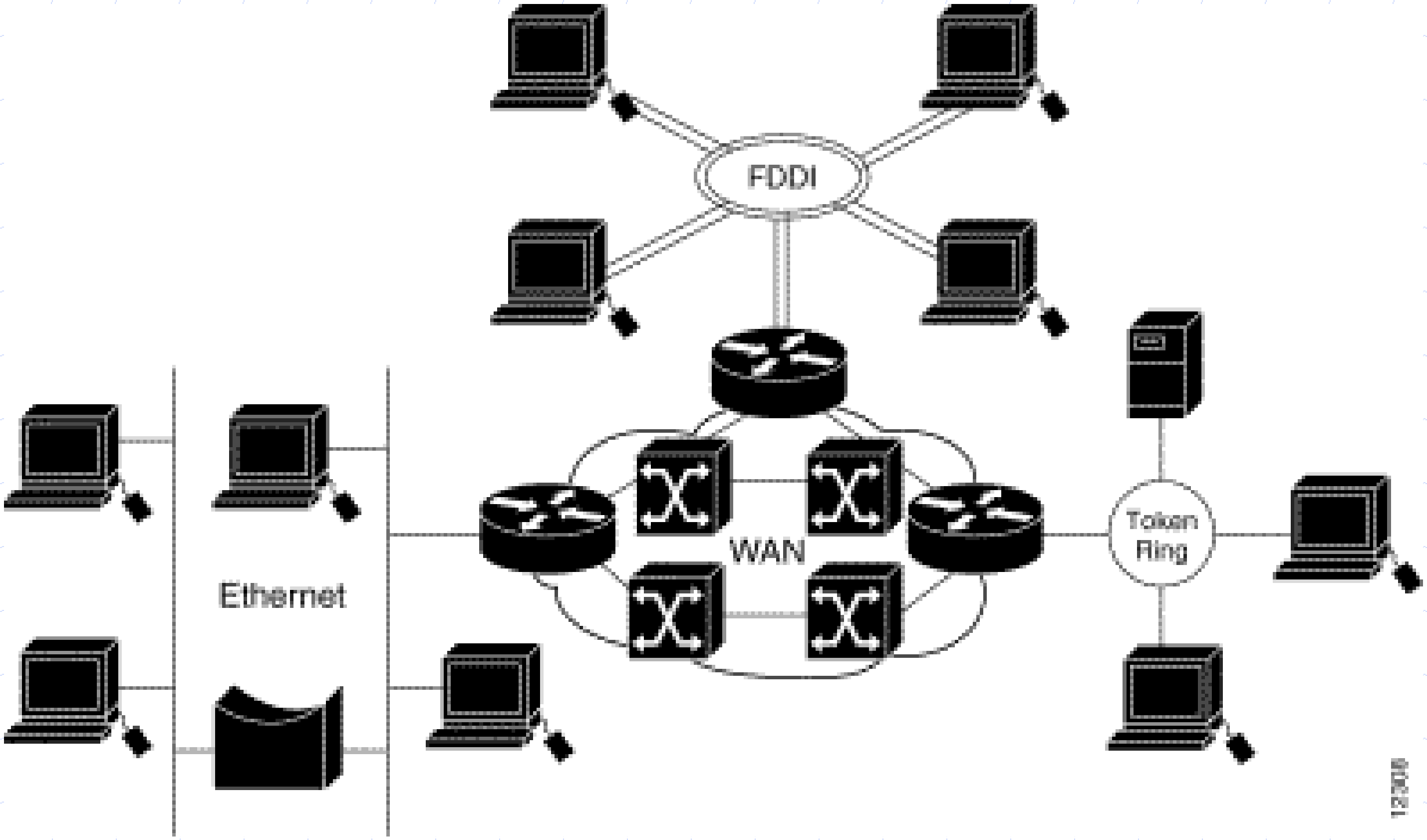
TCP & UDP

- Most TCP/IP applications use TCP for transport layer
- TCP provides a connection (logical association) between two entities to regulate flow check errors
- UDP (User Datagram Protocol) does not maintain a connection, and therefore does not guarantee delivery, preserve sequences, or protect against duplication

Internetworking

- Interconnected networks, usually implies TCP/IP
- Can appear to users as a single large network
- The global Internet is the largest example, but intranets and extranets are also examples

Internetworking



TCP Segment (TCP PDU)

- Source port (16 bits)
- Destination port (16 bits)
- Sequence number (32 bits)
- Acknowledgment number (32 bits)
- Data Offset (4 bits)
- Reserved (6 bits)
- Flags (6 bits) : URG, ACK, PSH, RST, SYN, FIN
- Window (16 bits)
- Checksum (16 bits)
- Urgent Pointer (16 bits)
- Options (variable)

The size of TCP header is 192 bits = 24 byes.

IPv4 and IPv6

- IP (IPv4) provides for 32-bit source and destination addresses, using a 192-bit header
- IPv6 (1996 standard) provides for 128-bit addresses, using a 320-bit header.
- Migration to IPv6 will be a very slow process

*History of IPng Effort

- By the Winter of 1992 the Internet community had developed four separate proposals for IPng. These were "CNAT", "IP Encaps", "Nimrod", and "Simple CLNP". By December 1992 three more proposals followed; "The P Internet Protocol" (PIP), "The Simple Internet Protocol" (SIP) and "TP/IX". In the Spring of 1992 the "Simple CLNP" evolved into "TCP and UDP with Bigger Addresses" (TUBA) and "IP Encaps" evolved into "IP Address Encapsulation" (IPAE).
- By the fall of 1993, IPAE merged with SIP while still maintaining the name SIP. This group later merged with PIP and the resulting working group called themselves "Simple Internet Protocol Plus" (SIPP). At about the same time the TP/IX Working Group changed its name to "Common Architecture for the Internet" (CATNIP).
- The IPng area directors made a recommendation for an IPng in July of 1994 [RFC 1752].
- The formal name of IPng is IPv6

Why Need IPv6?

- Internet Growth
  - Network numbers and size
  - Traffic management
- Quality of Services (QoS)
- Internet Transition
  - Routing
  - Addressing
- No question that an IPv6 is needed, but when

IP Packet version

IP4

1	2	3	4	5	6	7	8	9	**10**	11	12	13	14

1	Version number	4 bits	9	Protocol	8 bits
2	Header length	4 bits	10	**CRC 16**	**16 bits**
3	Type of Service	8 bits	11	Source address	32 bits
4	Total length	16 bits	12	Destination Address	32 bits
5	Identifiers	16 bits	13	Options	varies
6	Flags	3 bits	14	User data	varies
7	Packet offset	13 bits	15	Flow name	24 bits
8	Hop limit	8 bits	16	Next header	8 bits

IP6

1	15	4	16	8	11 (128 bits)	12 (128 bits)	14

IPv4 Header

- Version (4 bits)
- Internet header length (4 bits)
- Type of Service (8 bits)
- Total Length (16 bits)
- Identification (16 bits)
- Flags (3 bits
- Fragment Offset (13 bits)
- Time to Live (8 bits)
- Protocol (8 bits
- Header Checksum (16 bits)
- Source Address (32 bits)
- Destination Address (32 bits)
- Options (variable)
- Padding (variable)