2. Principle of Layering concept

1

Updated by,
Dr. Ashwini Chavan
DYPIMED

What is a Protocol?

2

- 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

3

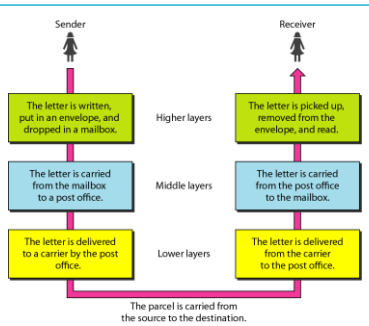
- Vendors like standards because they make their products more marketable
- Customers like standards because they enable products from different vendors to interoperate
- Two protocol standards are well-known:
  - TCP/IP: widely implemented
  - OSI: less used, still useful for modeling/conceptualizing

Internet Standards

4

- 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

Figure 2.1 Tasks involved in sending a letter



Learning outcomes

6

- Understand the need of layering in Networked computing
- Understand the OSI model and the tcp/ip model
  - Understand the function protocols and their role at each layer.
    - TCP protocol
    - UDP protocol
- Understand the role of header in communication between layers
- Understand how data sent from one host arrive to the target host.

Models and Standards in Communication

7

- Communication
  - Established standards
  - Standards are known as protocols
- Implementation
  - A framework is helpful in the design of hardware and software for communication
  - ISO-OSI Model serves this purpose
  - ISO-OSI supersedes the TCP/IP model

ISO and OSI Defined

8

- ISO
  - International Standards Organization
- OSI
  - Open Systems Interconnect

OSI Model Background

9

- Introduced in 1978 and revised in 1984
- Formulates the communication process into structured layers
- There are seven layers in the model, hence the name the 7-Layer model
- The model acts as a frame of reference in the design of communications and networking products

10

AN OVERVIEW OF ISO AND ITS 7-LAYER OSI MODEL

Figure 2.3 *The interaction between layers in the OSI model*

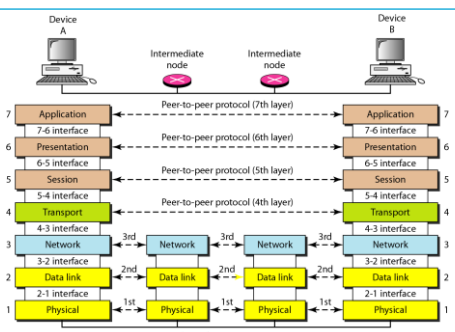
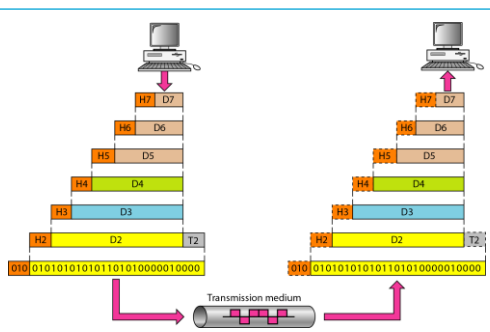


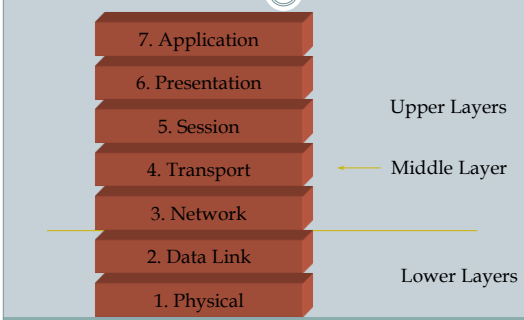
Figure 2.4 *An exchange using the OSI model*



A- User Understandable Form
P – Machine –"-
S – Session 100
T - Segments 50 50
N – Packet 10
D – Frames 1
P – Bits/ Analog or Digital Signals

Division of Layers

14



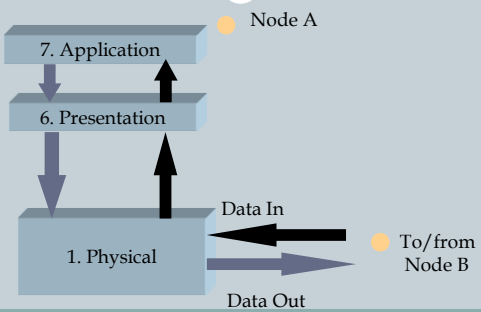
The Function of a Layer

15

- Each layer deals with one aspect of networking
  - Layer 1 deals with the communication media
- Each layer communicates with the adjacent layers
  - In both directions
  - Ex: Network layer communicates with:
    - Transport layer
    - Data Link layer
- Each layer formats the data packet
  - Ex: Adds or deletes addresses

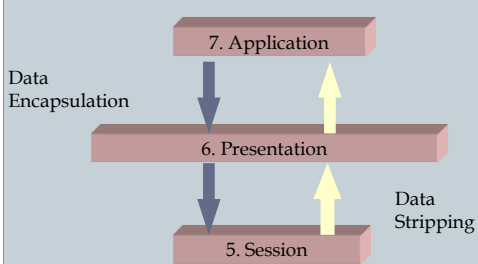
Role of Layers

16



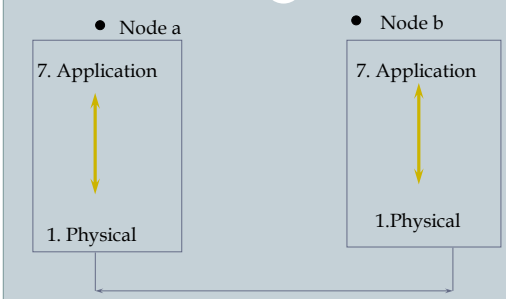
Communication Between Layers

17



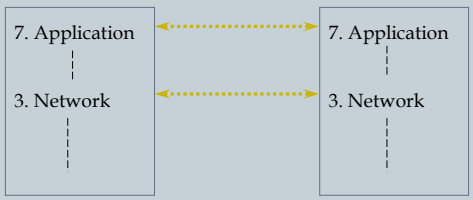
The Role of Layers in Point-to-point Communication

18



Virtual Communication Between Layers

19



Module

20

SUMMARY OF ISO-OSI FUNCTIONAL LAYERS

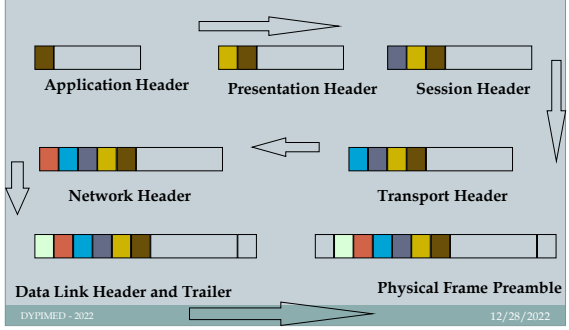
Layer Operations

21

- At each layer, additional information is added to the data packet
- An example would be information related to the IP protocol that is added at Layer 3

Formatting of Data Through the Layers

22



Packet : General Format

23

A general concept of packets serves as a prerequisite to the understanding of the ISO-OSI model.

Some Header Information Added at Various Layers

24

- Packet arrival information
- Receiver's address
- Sender's address
- Synchronization character

a/P - 100 MB

S1- 50 MB S2- 50 MB

S1 Seg 1-10 Mb S1Seg2 10 mb S1seg3 10 mb

S2 seg 110 mb S2 seg 210 mb

Data

25

- Actual data
- May contain error correction code
  - Performed on individual characters of the data
  - Example: Parity
- Size may vary
  - Depending on the protocol
  - Example
    - 802.3 specifies range of data packet length

Even / odd
11111101 - 0
7' of 1's

Some Trailer Information Added at Various Layers

26

- Error correction code
  - Character oriented
  - VRC (Parity Checking)
- Packet oriented error correction codes
  - LRC
  - CRC

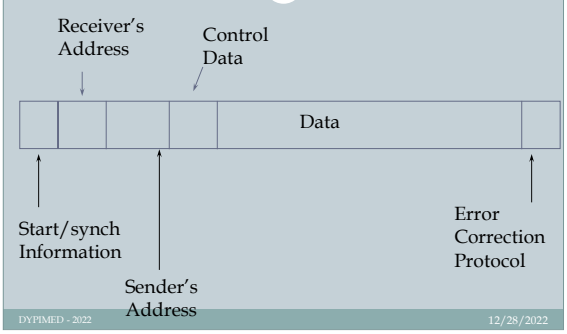
A Note on CRC

27

- Used widely
- Sophisticated
  - Polynomial of deferent degrees are used for error correction
  - Example: Degrees 16, 32 etc.
- CRC-32 is a more stringent error checking procedure than CRC-16

Some of the Major Components of the Data Packet

28



Standardizing Packet Formatting

29

- Packets must conform to a standard in order for the nodes in a network to be able to communicate with one another
- The International Standards Organization (ISO) has provided a reference model
- Standards are established for operations at each layer of the ISO/OSI model in the form of protocols

30

End of Module 1

Module 2

31

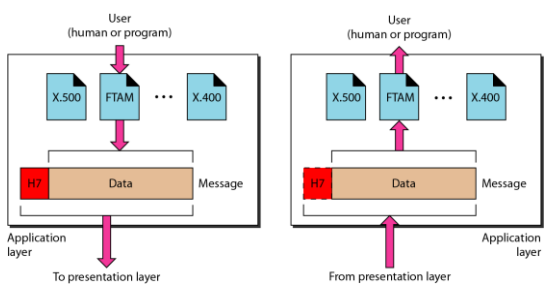
THE ISO UPPER LAYERS

Module Objectives

32

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer

Figure 2.14 *Application layer*



Note

The application layer is responsible for providing services to the user.

7. Application Layer

35

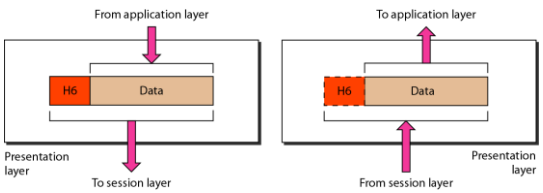
- Purpose
  - User application to network service interface
- Examples
  - File request from server
  - E-mail services
  - etc.

Application Layer Function

36

- General network access
- Flow control
- Error recovery

Figure 2.13 *Presentation layer*



Note

The presentation layer is responsible for translation, compression, and encryption.

6. Presentation Layer

39

- Purpose
  - Formats data for exchange between points of communication
    - Ex: Between nodes in a network
- Example:
  - Redirector software
    - Formats for transmission to the server

Presentation Layer Function

40

- Protocol conversion
- Data translation
- Encryption
- Character set conversion
- Expansion of graphics command

Redirector Example

41

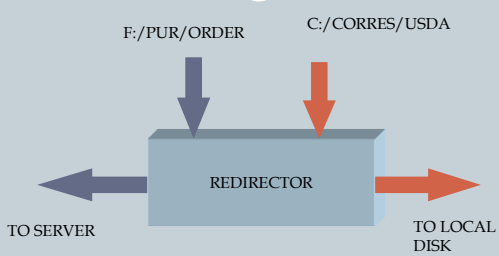
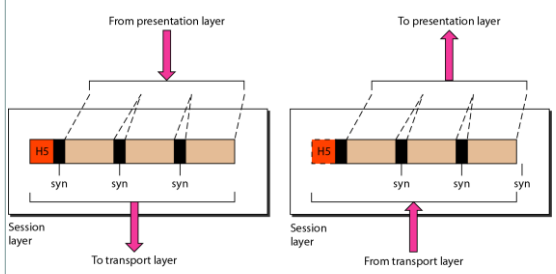


Figure 2.12 *Session layer*



Note

The session layer is responsible for dialog control and synchronization.

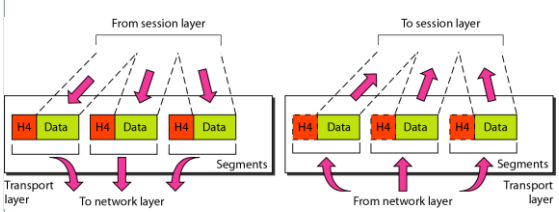
5. Session Layer

- Purpose
  - Oversee a communication session
    - Establish
    - Maintain
    - Terminate
- Example

Session Layer Function

- Performs name recognition and related security
- Synchronization between sender and receiver
- Assignment of time for transmission
  - Start time
  - End time etc.

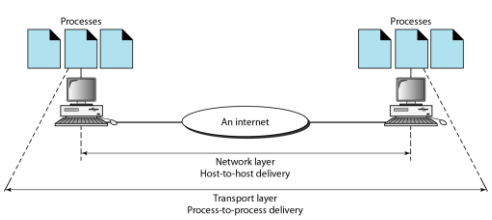
Figure 2.10 *Transport layer*



Note

The transport layer is responsible for the delivery of a message from one process to another.

Figure 2.11 *Reliable process-to-process delivery of a message*



A2 + B2 = C

1) A2
2) B2
3) +
4) C=

4. Transport Layer

50

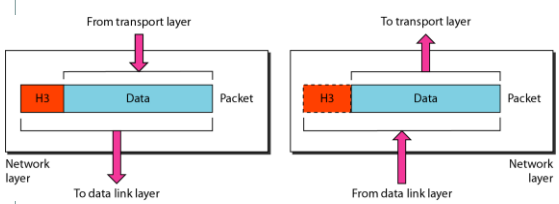
- Purpose
  - Repackage proper and efficient delivery of packages
    - Error free
    - In sequence
    - Without duplication
    - Routing
- Example

Transport Layer Function

51

- For sending data
  - Repackage the message to fit into packets
    - Split long messages
    - Assemble small messages
- On receiving data
  - Perform the reverse
  - Send an acknowledgment to the sender
- Solve packet problems
  - During transmission and reception

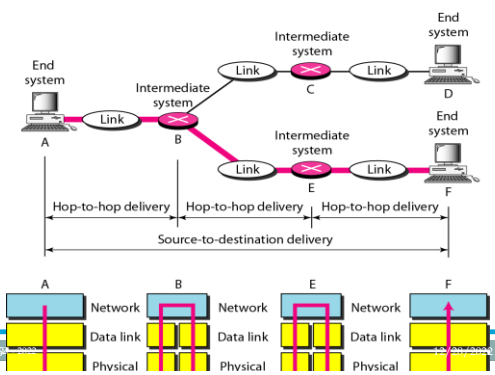
Figure 2.8 *Network layer*



Note

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Figure 2.9 *Source-to-destination delivery*



3. Network Layer

55

- Purpose
  - Addressing and routing the packets
- Example application at the router
  - If the packet size is large, splits into small packets

56

Network Layer Function

57

- Address messages
- Address translation from logical to physical
  - Ex: nganesa ----------> 102.13.345.25
- Routing of data
  - Based on priority
  - Best path at the time of transmission
- Congestion control

Logical address is know to the outside world…
But physical address is known to only your network…

58

End of Module 2

Module 3

59

THE ISO LOWER LAYERS

2. Data Link Layer

60

- Purpose
  - Manages the flow of data over the physical media
- Responsible for error-free transmission over the physical media
- Assures error-free data submission to the Network Layer

Data Link Layer Function

61

- Point of origin
  - Packages data for transmission over physical line
- Receiving end
  - Packages data for submission to the network layer
- Deals with network transmission protocols
  - IEEE 802. protocols

Data Link Layer Subdivision

62

- Improvement to ISO Model
- Logical Link Control (LLC) sub-layer
  - Manages service access points (logical link)
  - Error and flow control
- Media Access Control (MAC) sub-layer
  - Applies directly to network card communication
  - Access control

Logical Link Control

63

Media Access Control Application

64

- Network Interface Card driver

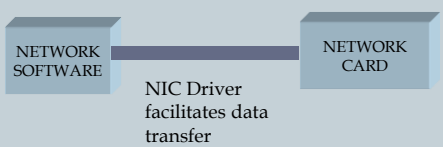
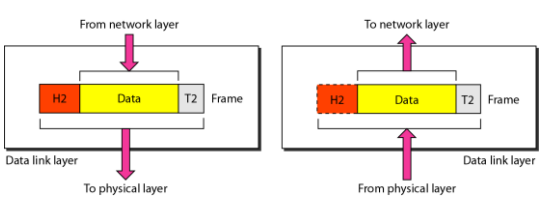


Figure 2.6 *Data link layer*



Note

The data link layer is responsible for moving frames from one hop (node) to the next.

Figure 2.7 *Hop-to-hop delivery*

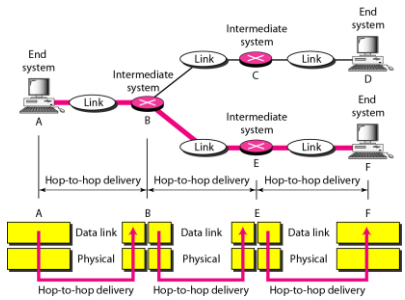
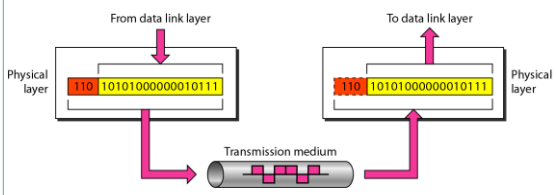


Figure 2.5 *Physical layer*



1. Physical Layer

69

- Purpose
  - Deals with the transmission of 0s and 1s over the physical media
    - Translation of bits into signals
- Example
  - Pulse duration determination
  - Transmission synchronization
  - etc.

Physical Layer Function

70

- Encode bits into signals
  - Carry data from the h higher layers
- Define the interface to the card
  - Electrical
  - Mechanical
  - Functional
  - Example: Pin count on the connector

Lower Layers Application Areas

71

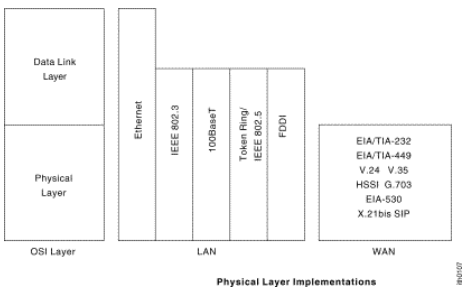
- Special significance to network card design
- Applies to general LAN hardware design
  - Exceptions
    - Routers etc.
- 802. standards
  - Centered around the lower layers
  - Applies to networks

Note

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

*Physical-layer Implementation

73



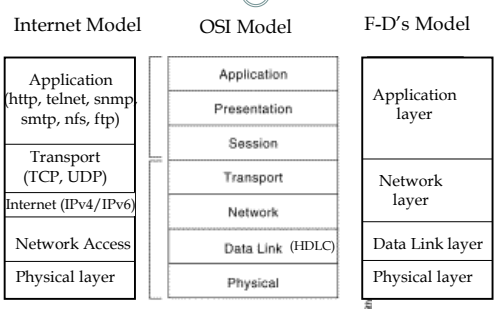
TCP/IP

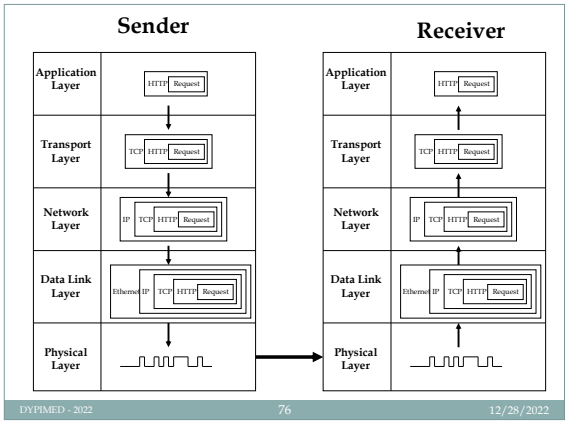
74

- 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

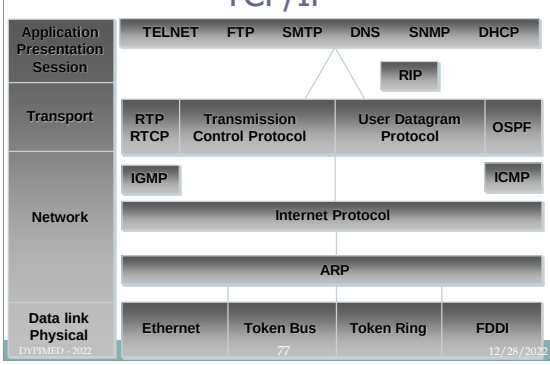
An OSI View of TCP/IP

75





*TCP/IP



TCP/IP Network Access Layer

78

- 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

79

- 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

80

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

TCP/IP Application Layer

81

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

TCP & UDP

82

- 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

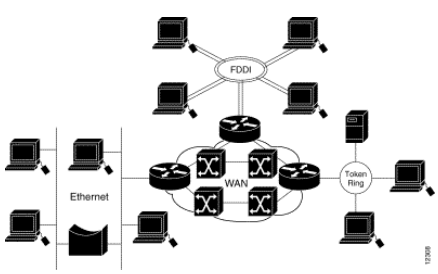
Internetworking

83

- 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

84



TCP Segment (TCP PDU)

85

- 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

86

- 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

2^32= 10 digits - 0.0.0.0
2^128= 50 digits -
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0

*History of IPng Effort

87

- 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?

88

- 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

84

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

90

- 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)

Compare of OSI and TCP/IP

91

Contents

92

- Concept
- General Compare
- Lower Layers Compare
- Upper Layers Compare
- Critique

Concept

93

- OSI: Open Systems Interconnection. It was developed by ISO as a first step toward international standardization of the protocol used in various layers. It deals with connecting open system..
- TCP/IP: Transport Control Protocol/Internet Protocol. TCP is used in connection with IP and operates at the transport layer. IP is the set of convention used to pass packets from one host to another.

General Compare

94

- Similarity
- Difference

Similarity

95

- Both are based on the concept of a stack of independent protocols.
- The functionality of the layers is roughly similar.

Difference

96

- OSI makes the distinction between services, interfaces, and protocol.
- The OSI model was devised before the protocols were invented. It can be made to work in diverse heterogeneous networks.
- TCP/IP does not originally clearly distinguish between services, interface, and protocol.
- TCP/IP model was just a description of the existing protocols. The model and the protocol fit perfectly.

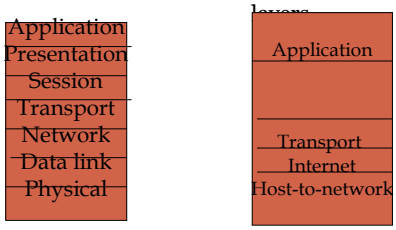
Difference (continue)

97

- The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer.
- The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer, giving the user choice.

Difference (continue)

- OSI has seven layers
- TCP/IP has four layers



Difference (continue)

99

- OSI emphasis on providing a reliable data transfer service, Each layer of the OSI model detects and handles errors, all data transmitted includes checksums. The transport layer checks source-destination reliability.
- TCP/IP treats reliability as an end to end Problem. The transport layer handles all error detection and recovery, it was checksums, acknowledgments, and timeouts to control transmissions and provides end-to-end verification.

Difference (continue)

100

- Host on OSI implementations do not handle network operations.
- TCP/IP hosts participate in most network protocols.

Lower Layers Compare

101

- Data link/Physical vs Subnet
- Network vs Internet
- Transport vs TCP/UDP

Data link/Physical vs Subnet

102

- OSI has Data Link/Physical layers. Data link layer dear with error detection and correction. Physical layer refer to the physical connection of network.
- The lower layers below the Interface or Network layer of TCP/IP seldom discussed. This protocol has not defined and varies from host to host and network to network.

Network vs Internet

103

- Protocols of the network/internet layer
- Ways of addressing
- The routing architecture

Protocols of the network layer
X.25 IP

104

- A connection-oriented protocol.
- Virtual circuit approach is used.
- Logical connection or virtual circuit is established before any packet are sent i.e. Call Setup phase.

- A connectionless oriented protocol.
- Data-gram approach is used.
- Each packet is treated independently.

Protocols of the network layer
X.25 IP

105

- Each packet contains a virtual circuit identifier as well as data.
- Node need not make a routing decision. It is made only once for each connection.

- Packets of the message do not all follow the same route and may arrive at the destination in a different sequence from the one in which they were sent

Internetworking Protocols
OSI TCP/IP

106

- CLNP accommodates variable-length addresses.

- IP supports fixed, 32-bit address.

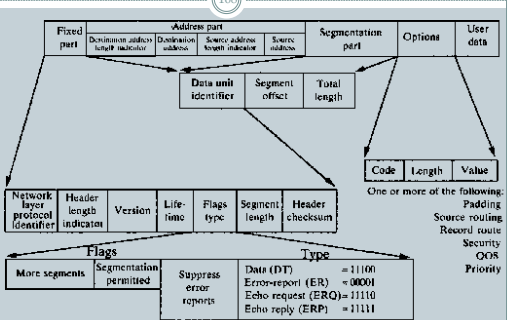
Compares the functions of CLNP to those of IP

107

Function	ISO CLNP	IP
Version identification	1 octet	4 bits
Header length	1 octet, represented in octets	4 bits, represented in 32-bit words
Quality of service	QOS maintenance option	Type of service
Segment/fragment length	16 bits, in octets	16 bits, in octets
Total length	16 bits, in octets	Not present
Data unit identification	16 bits	16 bits
Flags	Don't segment, more segments, suppress error reports	Don't fragment, more fragments
Segment/fragment offset	16 bits, represented in octets	13 bits, represented in units of 8 octets
Lifetime, time to live	1 octet, represented in 500-millisecond units	1 octet, represented in 1-second units
Higher-layer protocol	Not present	Protocol identifier
Lifetime control	500-millisecond units	1-second units
Addressing	Variable length	32-bit fixed
Options	Security Priority Complete source routing Partial source routing Record route Padding Not present	Security Precedence bits in TOS Stricter source route Loose source route Record route Padding Timestamp

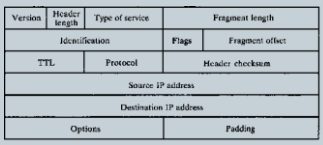
Header formats of CLNP

108



Header formats of IP

109



Network Layer Addresses

OSI Network Layer Addressing IP Addresses

110

- The network-layer addressing defines network addressing domains--IDP (AFI, IDI) and DSP.
- It identifies the abstract service access point between the transport and network layers.

- IP address consists of 32 bits, include network-number part and host-number part.
- It identifies the actual point of attachment of a computer system to a real sub-network (the "network interface").

Three different classes of IP address

111

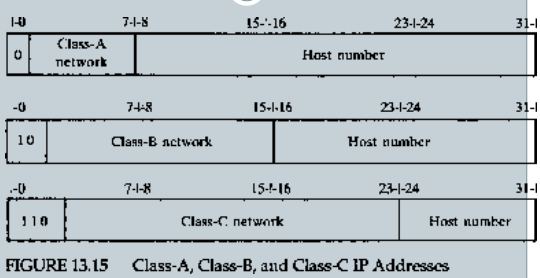


FIGURE 13.15 Class-A, Class-B, and Class-C IP Addresses

NSAP address

112

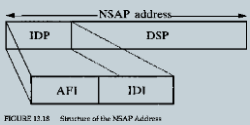


FIGURE 13.18 Structure of the NSAP Address

The routing architecture (OSI)

113

- A set of routing protocols that allow end systems and intermediate systems to collect and distribute the information necessary to determine routes. A routing information base containing this information, from which routes between end systems can be computed A routing algorithm that uses the information contained in the routing information base to derive routes between end systems.
- End systems (ESs) and intermediate systems (ISs) use routing protocols to distribute ("advertise") some or all of the information stored in their locally maintained routing information base.

The routing architecture (OSI Continue)

114

- The routing information base consists of a table of entries that identify a destination; the sub-network over which packets should be forwarded to reach that destination; and some form of routing metric, which expresses one or more characteristics of the route.
- The routing algorithm uses the information contained in the routing information base to compute actual routes.

The routing architecture (TCP/IP)

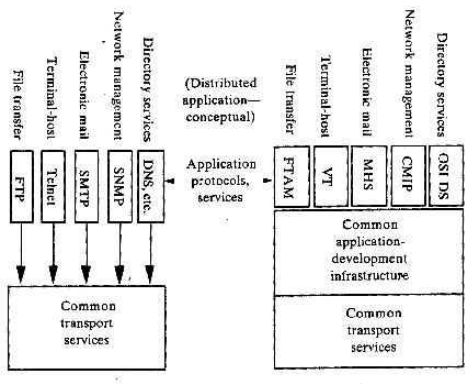
115

- The TCP/IP routing architecture looks very much like the OSI routing architecture. Hosts use a discovery protocol to obtain the identification of gateways and other hosts attached to the same network (sub-network). Gateways within autonomous systems (routing domains) operate an interior gateway protocol (intra-domain IS-IS routing protocol), and between autonomous systems, they operate exterior or border gateway protocols (inter-domain routing protocols).

Transport vs TCP/ UDP

116

- OSI Transport layer
- TCP/UDP
- Compare of Transport and TCP/IP



TCP/UDP

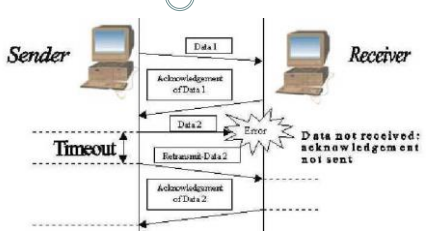
TCP

119

- Provide reliable data transmission.
- Responsible for data recovery.
- Allows the receiver to specify the amount of data it wants sent to it. (Important status information is sent by TCP connection).

UDP

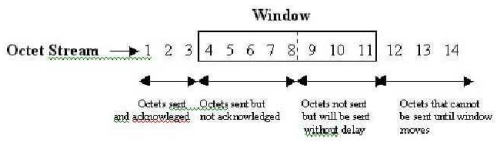
- It's fast but does not provide reliable data transmission. (main data stream sent by UDP).



TCP/UDP (continue)

121

- TCP, UDP both communicate using the concept ports (FTP, TELNET, SMTP, HTTP, POP3). By specifying ports and including port numbers with TCP/UDP data, the process of multiplexing is achieved.
- The port numbers, along with the source and destination addresses for the data, determine a socket. Socket make the communication reliably.



Compare of the Two Model

123

- Most of the TCP and UDP functions and specifications map to the OSI Transport Layer.
- The TCP/IP and OSI architecture models both employ all connection and connectionless models at transport layer.

Compare of the Two Model

OSI TCP/IP

124

- uses the terms connection-mode and connection-oriented for the connection model and the term connectionless-mode for the connectionless model.
- its network layer controls the operation of a sub-net, provides routing, congestion control and accounting.
- simply "connections" and data-grams.

Upper layers Compare

125

- Session
- Presentation
- Application

Session Layer

OSI TCP/IP

126

- The Session layer handles session setup, data or message exchanges, and tear down when the session ends.
- It also monitors session identification so only designated parties can participate and security services to control access to session information.
- The TCP/IP model does not have a general session layer protocol.
- In TCP/IP the term "sockets" and "ports" are used to describe the path over which cooperating application communicates.

Presentation Layer

OSI TCP/IP

127

- The Presentation Layer handles data format information for networked communications. For outgoing messages, it converts data into a generic format that can survive the rigors of network transmission; for incoming messages, it converts data from its generic networked representation into a format that will make
- Presentation layer is not present in TCP/IP model. Instead this function is frequently handled within the applications in TCP/IP through External Data Representation Standard(XDR) and Multipurpose Internet Mail Extensions (MIME).

Application Layer

128

- **Application** provides a set of interfaces for applications to obtain access to networked services such as networked file transfer, message handling, and database query processing.

Application Layer (Continue)

129

- An end-user interface that provides a human or another application with:
- The means to enter commands that direct the application to send files to and receive file from a remote host, list or change directories, rename or delete file, etc.
- The means of performing input to and output from mass storage device(s) (disk-tape).
- The means of transferring the files and file-related information between hosts.

Approach

130

OSI	TCP/IP
• Application entities in OSI may have many. • End-user applications developed using common application-development infrastructure.	• Application entities in TCP/IP have a single service element. • Each application was developed independently, from "top" to "bottom".

Critique

131

OSI	TCP/IP
• Bad timing, by the time the OSI protocols appeared, the competition TCP/IP protocols were already in widespread use. • Bad technology, both the model and the protocols are flawed, the model along with the associated service definitions and protocols are very complex.	• The model does not clearly distinguish the concepts of services, interface, and protocol. • It is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.

Critique (continue)

132

OSI	TCP/IP
• Bad implementation, the initial implementations were huge, unwieldy, and slow. (poor quality) • Bad politics, it was thought to be the creature of the government.	• The host-to-network layer is not really a layer. • The model does not distinguished the physical and data link layers