Data Communication

Diploma in Embedded System Design
Diploma in Integrated VLSI and Embedded System Design
Diploma in System Software Development

Ashish Kuvelkar
Hardware Technology Development Group
C-DAC, Pune

Why we are studying this?

- Data communication is a vital need for computing elements
- Computing elements are diversified in design resulting in heterogeneous platforms
  - Protocol stacks perform important tasks of binding them together
- Networking standards help in interoperability

What will be covered

- Topologies
- Network Architecture
  - OSI Model
- Physical layer protocols
- Data link layer protocols
  - LAN
  - WAN
- Data Security
- TCP/IP Suite

Prerequisites

- Knowledge of
  - Data communication basics
  - Serial transmissions
  - Programming in C

Introduction

- What is Data Communication
  - electronic transmission of information that has been encoded digitally
  - It concerns the transmission of digital messages to devices external to the message source.
- A communications channel is a pathway over which information can be conveyed.
- It may be defined by a physical wire that connects communicating devices,
  - or by a radio, laser, or other radiated energy source

Introduction

- As a rule, the maximum permissible transmission rate of a message is
  - directly proportional to signal power
  - inversely proportional to channel noise.
- The aim of any communications system is
  - to provide the highest possible transmission rate
  - at the lowest possible power
  - with the least possible noise.

A brief History

Generation	Time Frame	Application	Technology
Emergence	Through 70's	Voice	Circuit switched PSTN over copper wire
		Data	Serial link over copper, Modem
		Entertainment	Broadcast RF
Consolidation	Through 80's	Voice	Digital switched PSTN, Cellular mobile telephony
		Data	Store and forward packet, Gateway Subnetworks, Transoceanic FO cable
		Entertainment	CATV over copper coax

A brief History

Generation	Time Frame	Application	Technology
Convergence	Through 90's	Web, Multimedia	Fast packet switching over fiber, IP based global internet, Switched satellite network
Internet	2000+	Mobile, Ubiquitous	Wireless access network All optical network Widely deployed Transoceanic FO cable

Pervasive Computing Pyramid

Server

Store & Process Information

Workstation

Edit & Manage Information

Devices

Create & Access Information

Interoperability Standards

HTML Java WAP HTTP Bluetooth

Embedded Communication System

- What is Embedded Communication System
  - Embedded systems with communication capabilities
- Are stand alone systems not good enough
  - Serve specific and limited purpose
  - Adding a link enhances the usability manifold
  - Some systems are build around a link
  - Adding link has become cheap and easy

Few Examples

- Stand alone embedded systems
  - Digital watch
  - Calculator
  - Digital Thermometer
- Enhancing feature of Stand alone systems
  - Home Security system
  - LCD projector
  - Digital Diary
- Adding embedded system to a communicating device
  - Caller ID phone
  - Manageable Ethernet Switch

Few Examples (contd.)

- Embedded system with an inherent link
  - USB Thumb drive
  - Printer
  - Digital Camera
  - PDA
- Systems that connect to multiple communication links
  - Mobile Phone
  - USB to RS-232 converter
  - Ethernet to Wireless Router
  - GPS

Types of links

- Wired
- Wireless
- Special Purpose

Types of links

- Wired
  - Point to Point, low speed, short distance
    - RS-232
    - RS-422
  - High speed, Medium distance (LAN)
    - Ethernet
    - ATM
  - Point to Point, Low speed, Large Distance(WAN)
    - X.25, Frame relay
    - DSL, ADSL

Types of links (contd)

- Wireless
  - Short distance
    - IrDA, Bluetooth
  - Medium Distance
    - Wireless Ethernet
  - Long Distance
    - Microwave, VSAT
- Special purpose
  - CAN for automobile and industrial application
  - IEEE-488 instrumentation bus

Communication

- Similarity between People-People communication and Computer-Computer communication
- Types of communications
  - One to one
    - Private
    - Public
  - One to many
  - Many to one
  - Many to Many

Attributes

- Understanding
  - Language
  - Speed/Accent
  - Error correction
- Privacy
- Medium

Computer Communication

- Only one can talk, many can listen
- Many talking can be a transient phase
- Arbitration authority
- Understanding
  - Protocols
  - Data Rates/Interfaces
  - CRCs and checksums
- Privacy
  - Encryption,Tunneling
- Distance, speed and media are related
- Standards

Building a Computer Network

- What is a Network
  - Set of serial lines to attach terminals to Mainframe?
  - Telephone Network?
  - Cable TV Network?
- How is computer network different?
  - Generality
    - Carry different types of data
    - Ever growing range of applications

Fundamental Characteristics

- Delivery
  - Data should be delivered to correct destination
  - Data should be received only by the intended device or user

- Accuracy
  - Data should be delivered accurately
  - Data altered during communication become unusable for the receiver

Fundamental Characteristics

- Timelessness
  - Data should be delivered in timely manner
  - Data delivered late, may be useless

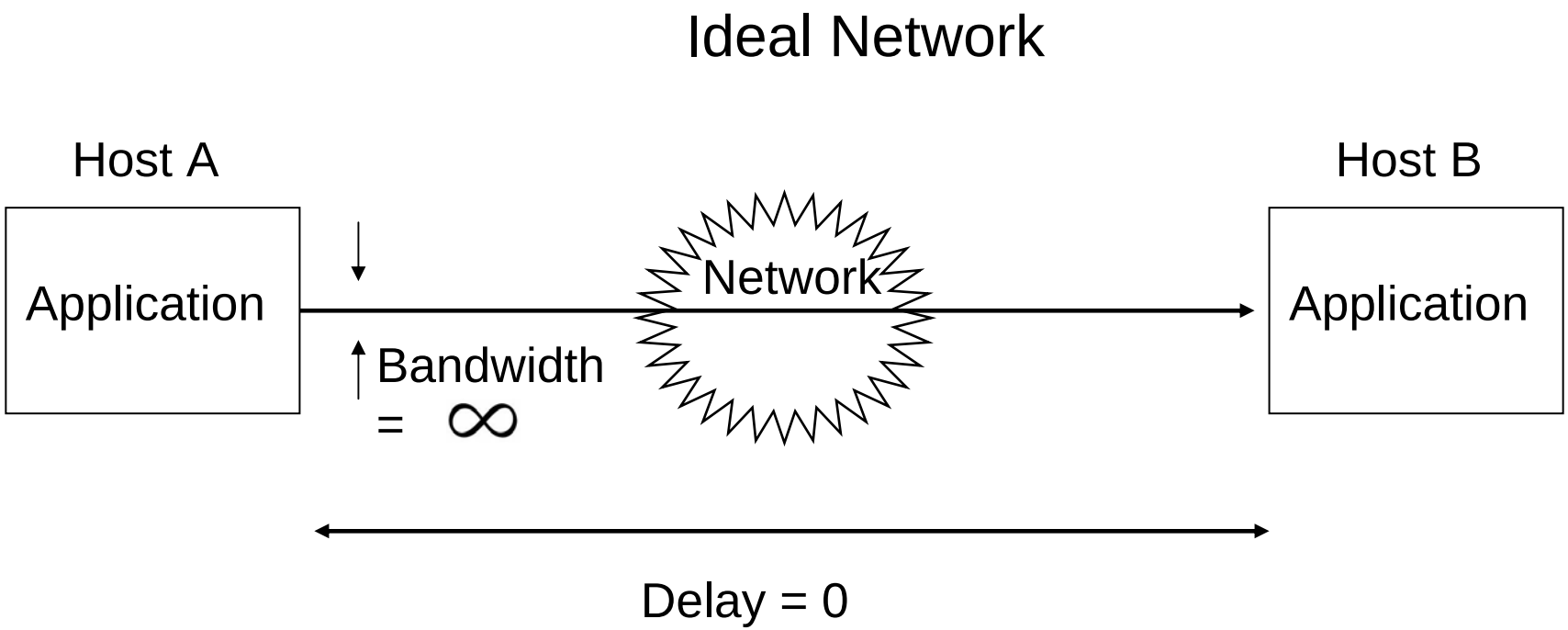
- Jitter
  - Jitter is variation is packet arrival time
  - Uneven delays affect isochroous type of traffic

Requirements

- Expectations from network depend on perspective
  - Application Programmer
    - Services, application would need
      - Guaranteed delivery of message in time
  - Network designer
    - Cost effective components
    - Efficient usage of network resources
  - Network provider
    - Easy to administer and manage
    - Accounting

Driver and Constraints

- Applications are the whole point of doing networking



Limiting Constraints

- Real world constraints make it difficult to provide high performance paths to applications
  - Speed of light
  - Channel capacity
  - Switching speed
  - Cost and feasibility
  - Heterogeneity
  - Policy and administration

Connectivity

- Private network
  - Limited network that connects selected machines
  - For reasons of privacy and security
- Public networks
  - Designed to grow in way, that they have potential to connect all computers in the world (scale)
- Links
  - Connect two or more nodes
  - Point-to-point or multiple access (topology)

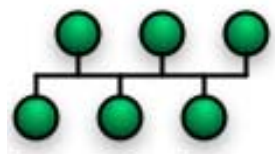
Topology

- It is the shape or physical connectivity of the network.
- Goals when establishing topology
  - Provide maximum possible reliability to assure proper receipt of all traffic
  - Route the traffic across the least cost path within the network.
  - Give the end user the best possible response time and throughput
- Each topology has advantages & disadvantages

Types of Topologies

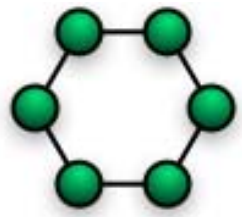
- Star
  - Easy to install
  - Central element, a hub or a switch
  - Localisation of problem
  - Hub is the weakest element

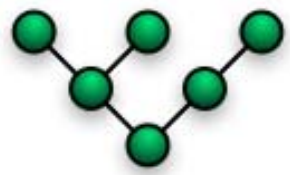
- Bus
  - Easy to expand, shorter cables
  - Single conversation, all station can hear every transmission
  - Bus is the weakest element



Types of Topologies

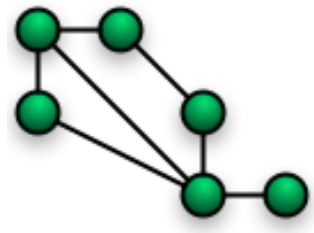
- Ring
  - Deterministic
  - Dual path, redundant
  - Poor scalability
- Line
  - Open ring
- Tree
  - Mesh network with no redundancy
  - Provides a concentration point for control and error resolution and potential bottleneck

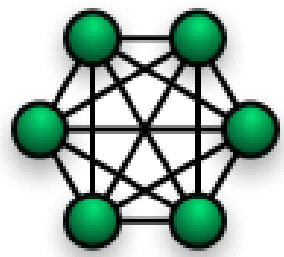




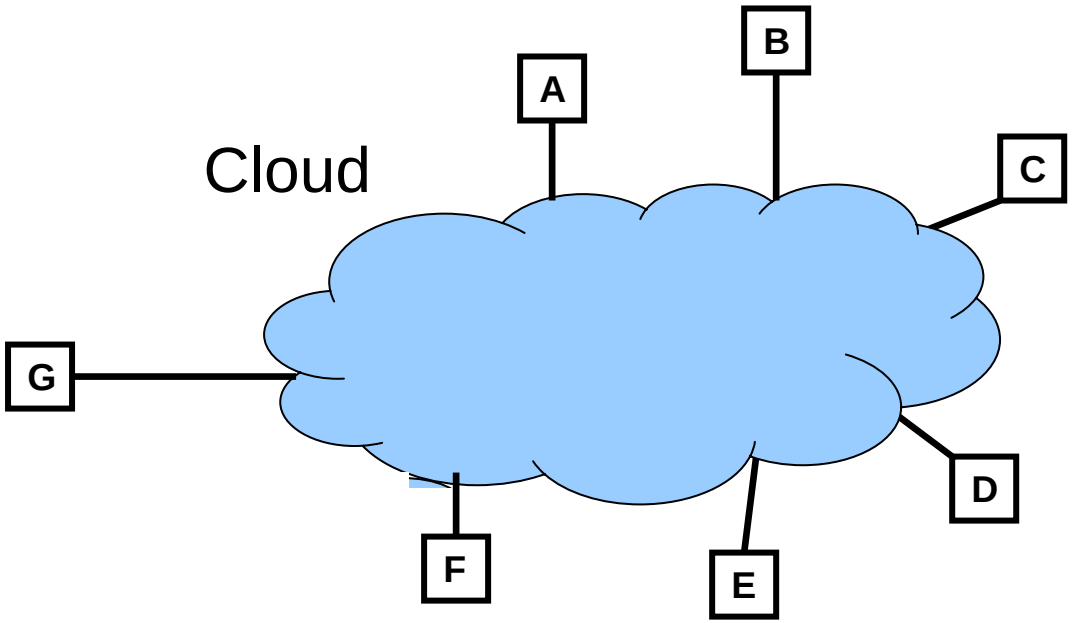
Types of Topologies

- Mesh
  - Multiple paths are available
  - Reconfiguration possible
  - Multiple hops
  - Wiring complicated
- Fully connected network
  - Extended mesh network
  - Fast, no hops
  - Poor scalability





Cloud



Cloud

- Circuit Switched
  - a dedicated physical path is established through the network and is held for as long as communication is necessary.
  - Normally used by telephone systems
- Packet switched
  - Data moves in small blocks called packet
  - Each packet has destination address
  - When received, message is assembled in order
  - Usually “store and forward” strategy is used

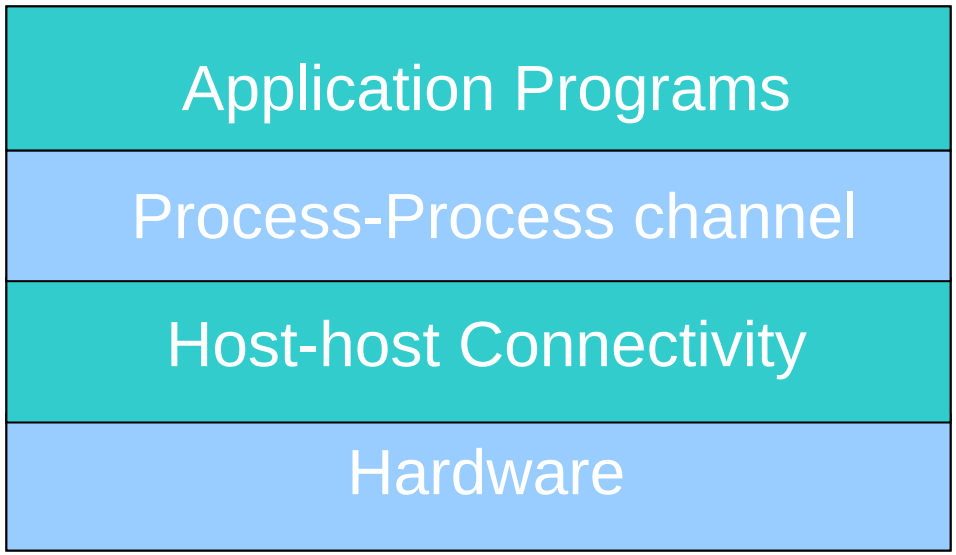
Cloud (contd.)

- The two technologies are converging
- Formerly, packet-switched digital networks would connect to circuit-switched ports
- Nowadays, remote dial-up access to corporate computers is usually over the Internet
- Packet switching makes efficient use of available bandwidth
- Using packet switching for voice results in poor voice quality and call latency
- Hybrid systems will stay for a long time.

Network Architecture

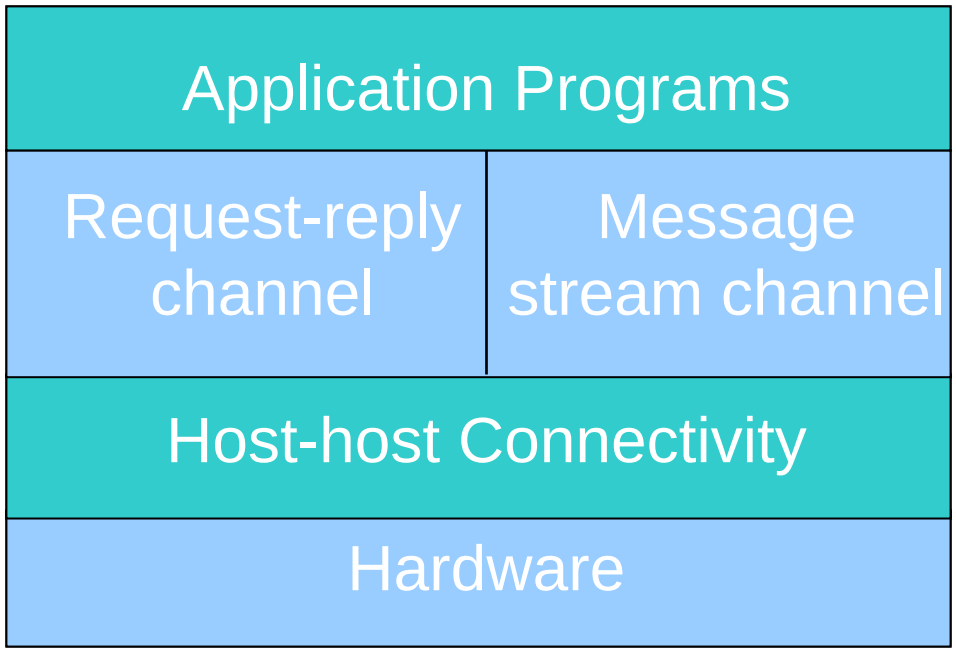
- Requirements
  - Cost-effective, fair, robust, high-performance connectivity
  - Evolve to accommodate changes
- Layering
  - When system becomes complex, level of abstraction are introduced
  - The services provided at higher layer are implemented in terms of services provided by lower layer

Layering



- Decomposes network building into more manageable components
- Modular design – adding a service becomes easy
- It becomes available to all upper layers

Layering

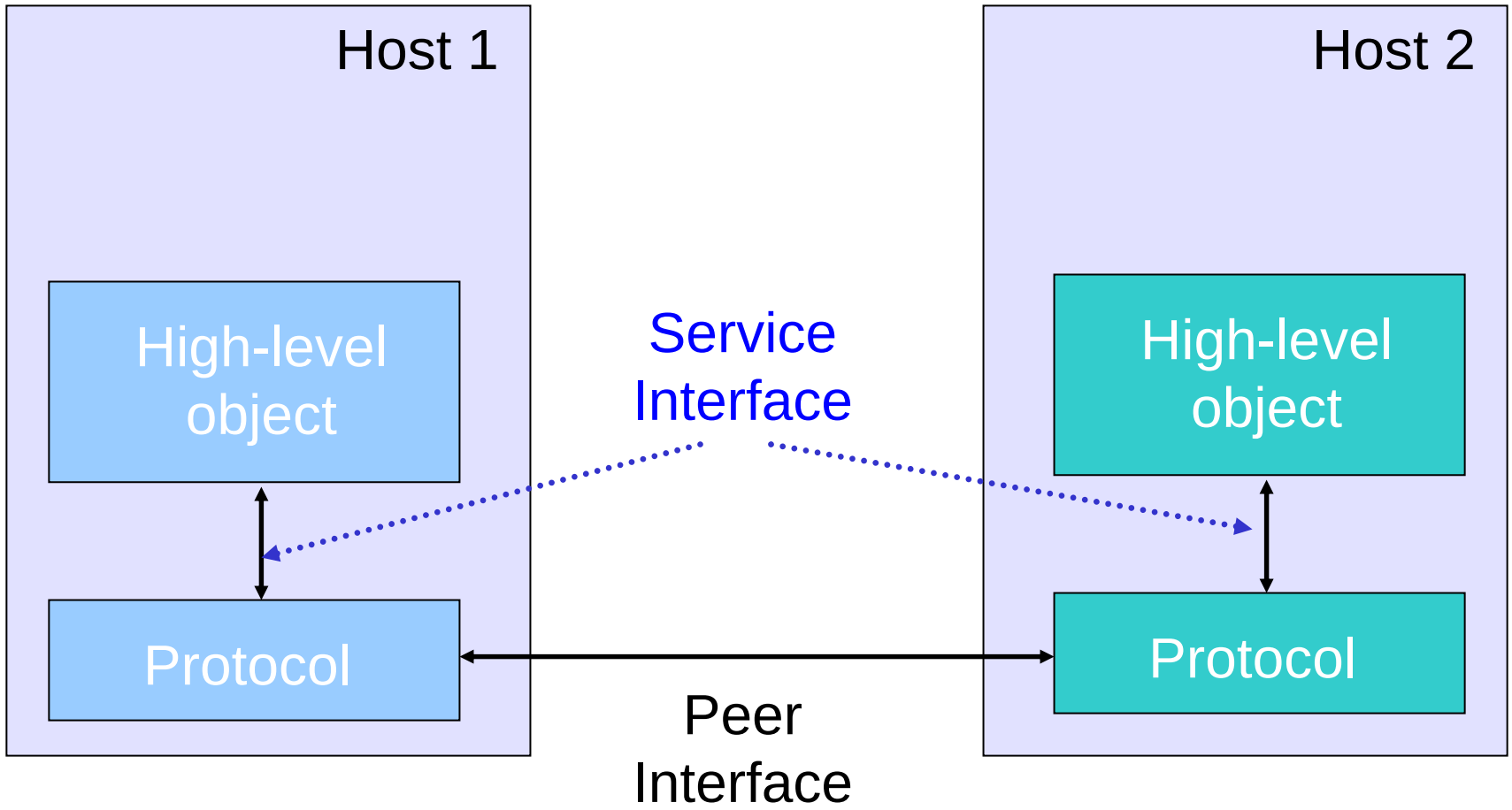


- Sometimes multiple abstractions are provided at the same level
- Each provides different service to upper layer but build on the same lower layer

Protocols

- The abstract objects that make a up the layers are protocols
- It provides communication service that higher level objects(processes/protocols) use to exchange messages
- Each protocol defines two interfaces
  - Service interface: to other object on same computer
  - Peer interface: to its counterpart on another machine

Service and Peer interface



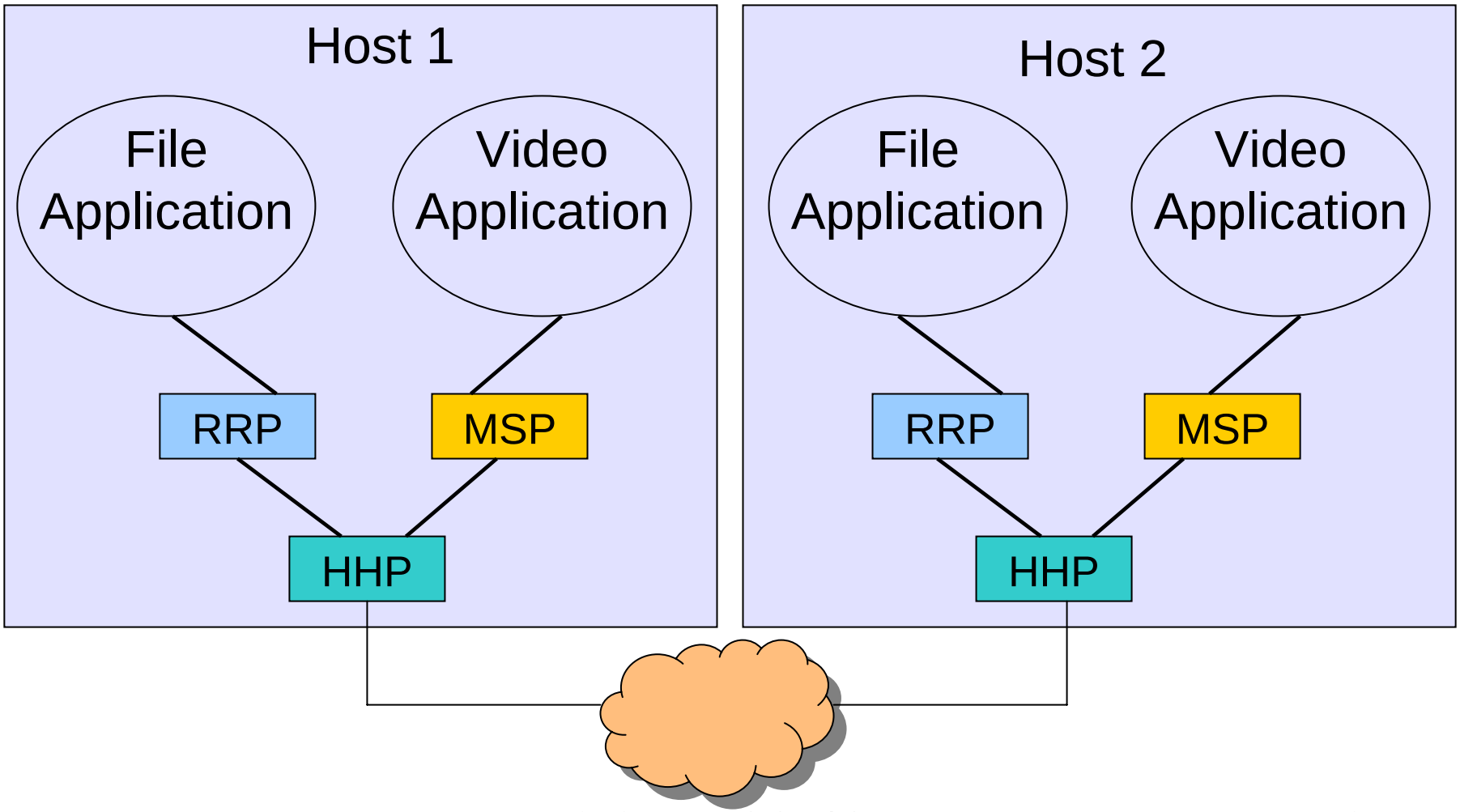
Peer Interfaces

- Except for hardware level, peer-peer communication is indirect, through lower level
- The suite of protocols that make up a network system is represented using protocol graphs
  - Nodes correspond to protocols
  - Edges correspond to “depend on” relation
- “Protocol” is used in two ways
  - Abstract interface (aka. Protocol specification)
    - Service and peer interface
  - Module that implements these two interfaces

Protocol

- A protocol defines what is communicated, how it is communicated and when it is communicated
- Syntax – Format or structure of data and order in which it is presented
- Semantics – meaning of each section of bits. How they are to be interpreted and what action is to be taken
- Timing – When to send responses, acknowledgements etc.

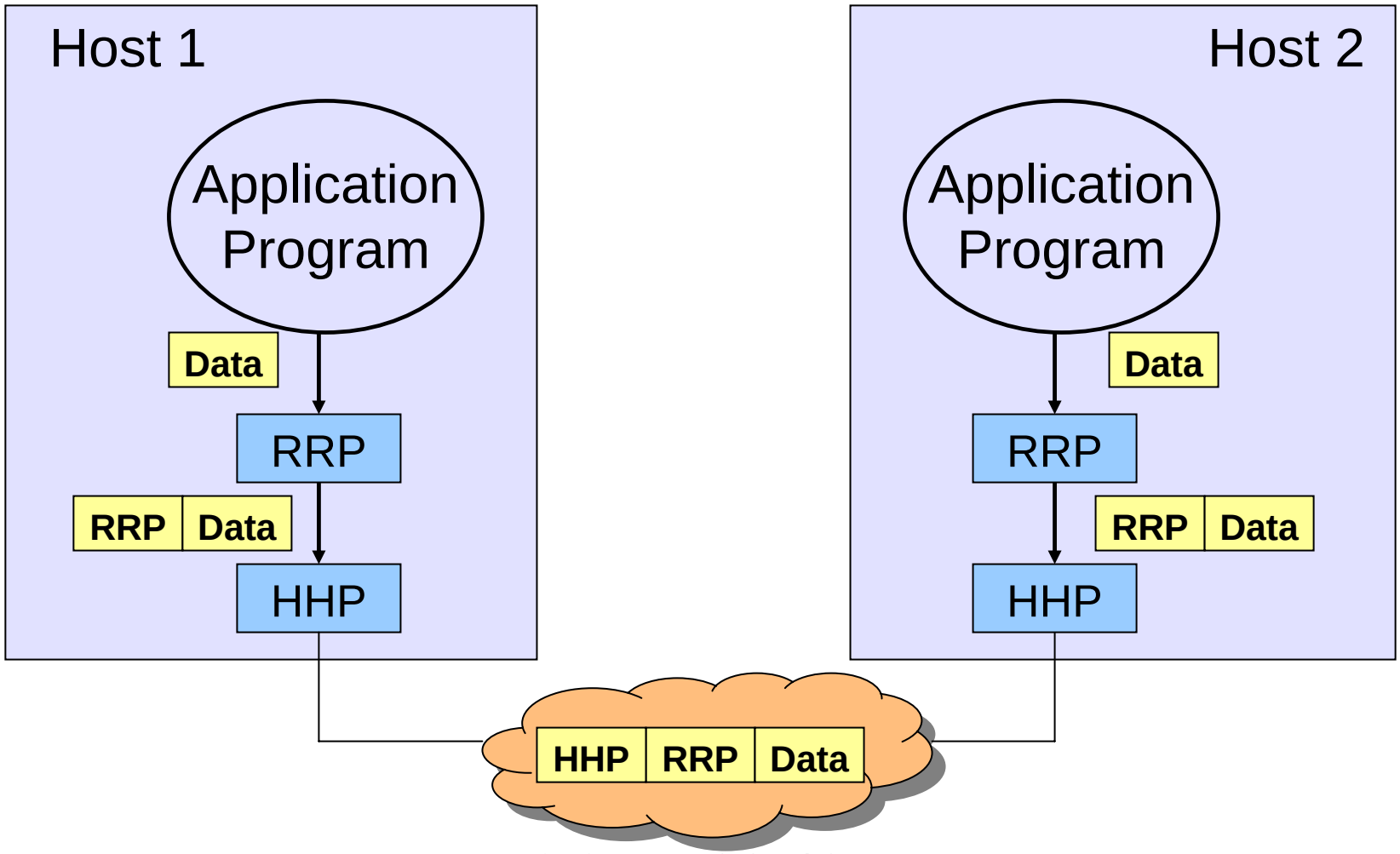
Protocol Graph



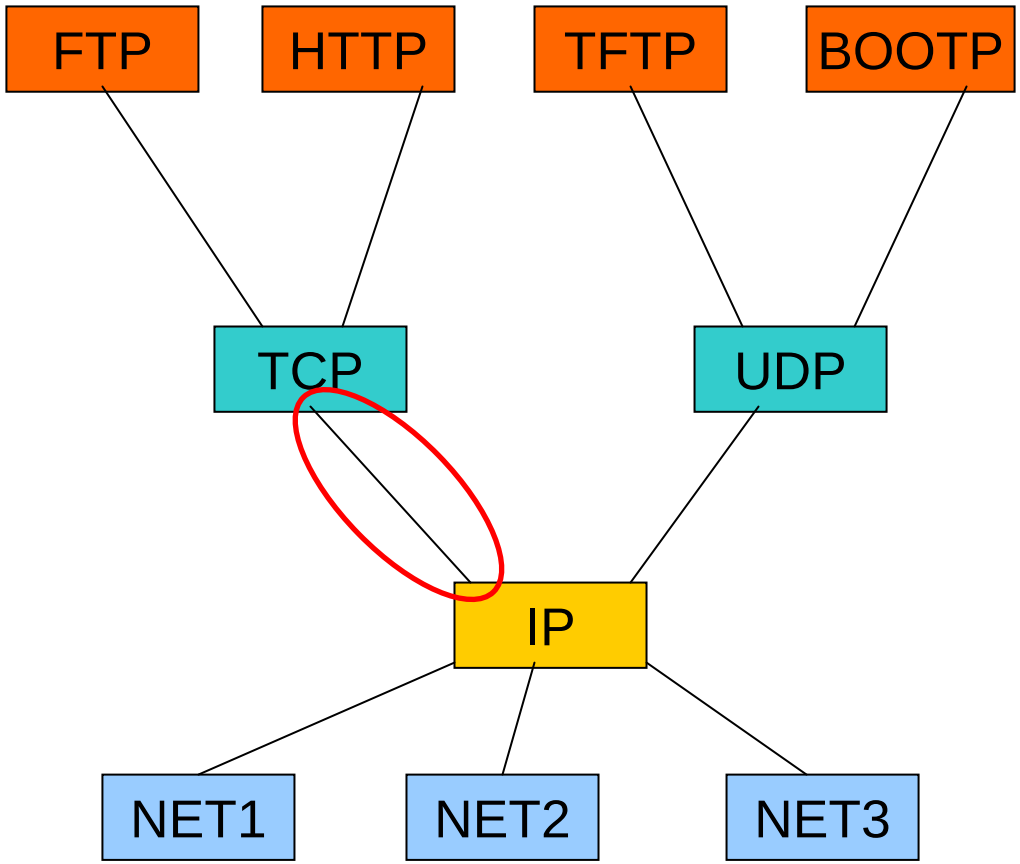
Encapsulation

- Message coming from an upper layer is treated as a string of bytes
- A layer has responsibility of delivering it to its peer
- So a header is attached to the message before it is passed on to the lower layer
  - Small data structure, few byte to few dozen bytes
  - Communicates control information to the peer
- Encapsulation is repeated at every layer of graph
- At destination the corresponding header are stripped and the payload is passed to upper layer

Encapsulation



Protocol Graph



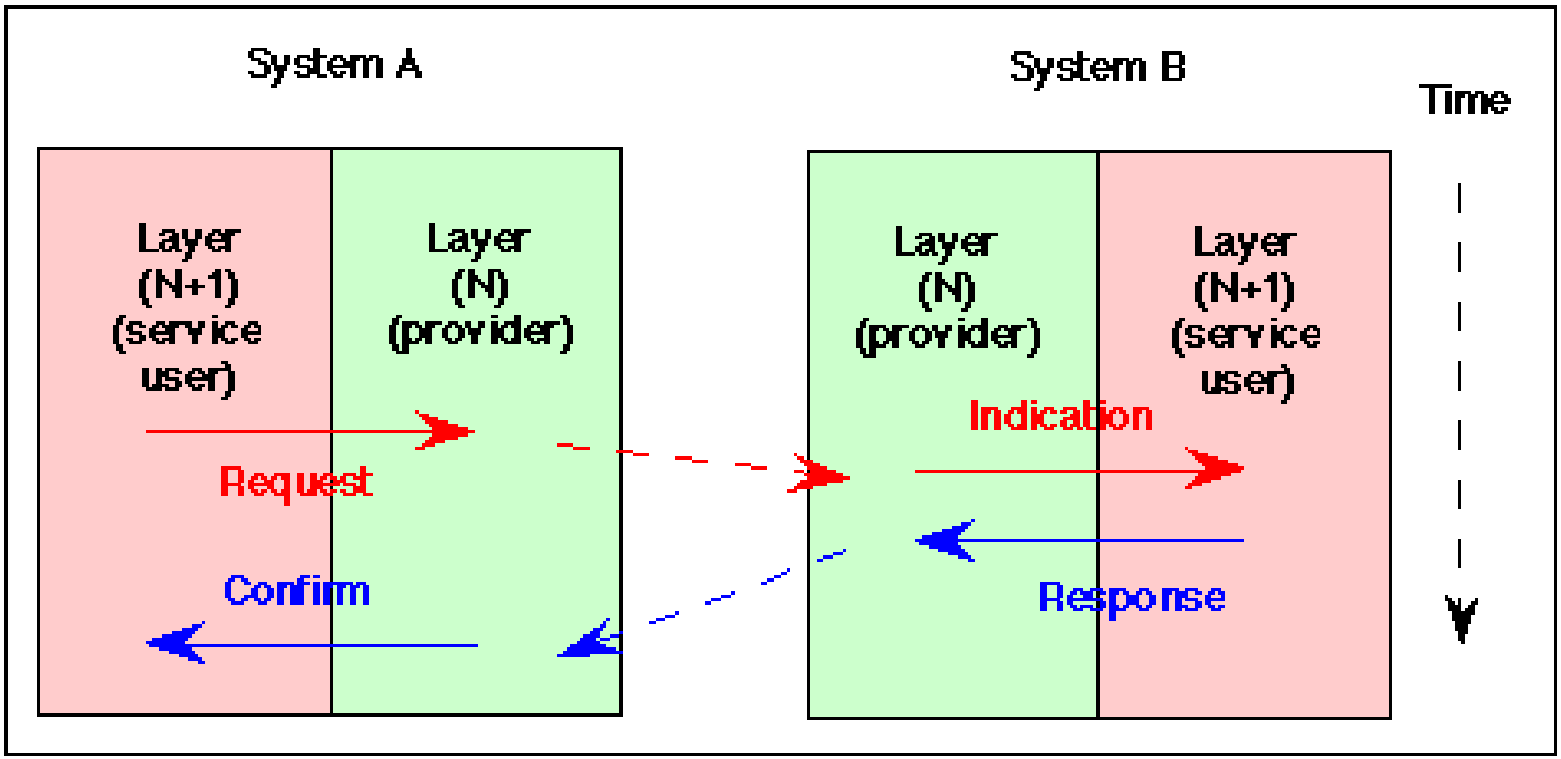
Communication between layers

- A layer is a service provider
  - May consist of several functions
- Communication between adjacent layers (within the same node) are managed by calling functions, called primitives
- Various types of actions that may be performed by primitives like Connect , Data, Flow Control, Disconnect etc.

Primitives

- Each primitive specifies the action to be performed or
- Advises the result of a previously requested action.
- A primitive may also carry the parameters needed to perform its functions.
- One of the typical parameter is the packet to be sent/received to the layer above/below
  - rather a pointer to data structures containing a packet (buffer).

Communication between layers



Primitives

- Request: A primitive sent by layer (N + 1) to layer N to request a service. It invokes the service and passes any required parameters.
- Indication: A primitive returned to layer (N + 1) from layer N to advise of activation of a requested service or of an action initiated by the layer N service.
- Response: A primitive provided by layer (N + 1) in reply to an indication primitive from layer N. It may acknowledge or complete an action previously invoked by an indication primitive.
- Confirm: A primitive returned to the requesting (N + 1) layer by the Nth layer to acknowledge or complete an action previously invoked by a request primitive.

Performance

- Measured in two fundamental ways
  - Bandwidth(also called throughput)
  - Latency (also called delay)
- Bandwidth – number of bits that can be transmitted over the network in certain period of time
  - Ethernet : 10 million bits in a second
    0.1 usec to transmit a bit
- Latency – how long it takes for a message to travel from one end of network to the other
- In some situations, Round Trip Time is important

Performance (contd.)

- Latency has three components
  - Speed-of-light propagation delay
  - Time required to transmit a bit of data
    - Network bandwidth and packet size
  - Queuing delay

Latency = Propagation + Transmit + Queue

Where Propagation = distance/speed_of_light

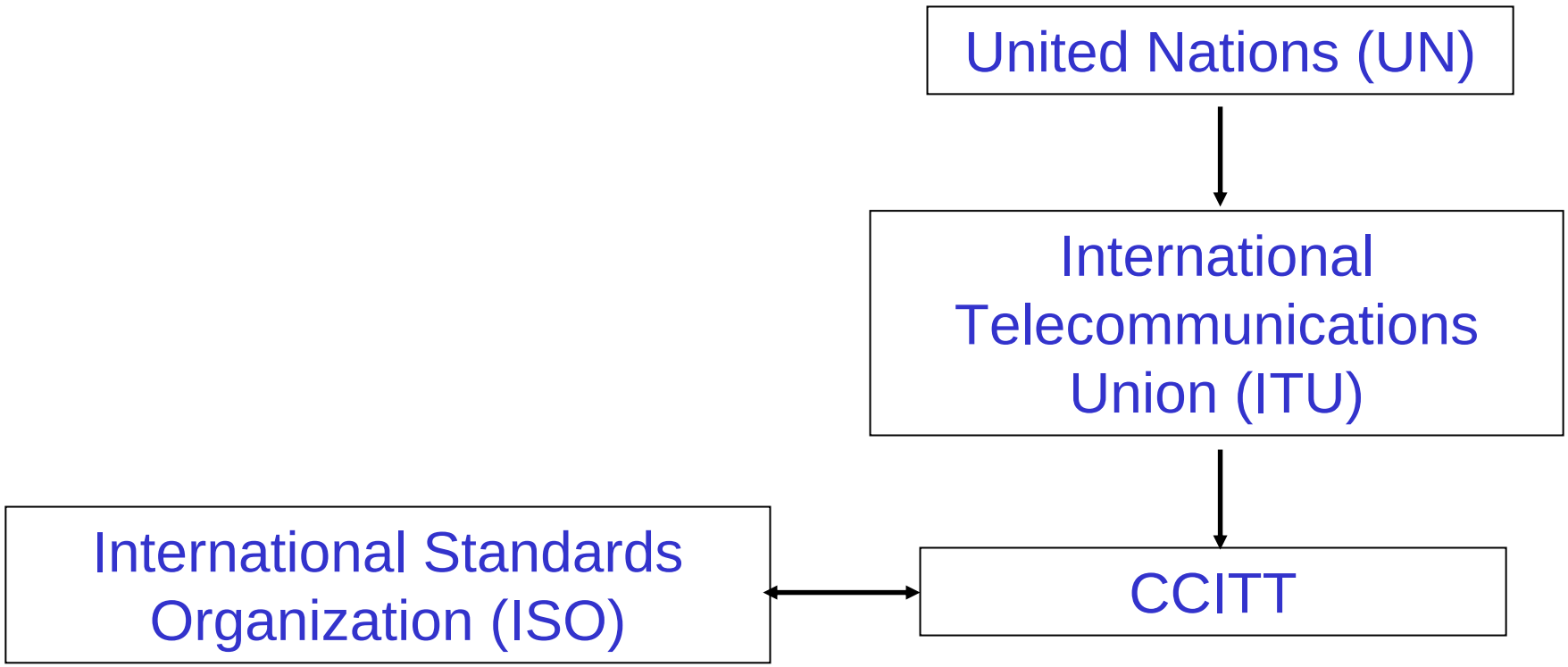
Transmit = size/bandwidth

Performance (contd.)

- Bandwidth and latency combine to define performance characteristics of a given link of channel
- Their relative importance depends on application
  - Client that sends 1 byte message and gets 1 byte reply is latency bound
  - A client that requests 25MB image is bandwidth bound

OSI Architecture

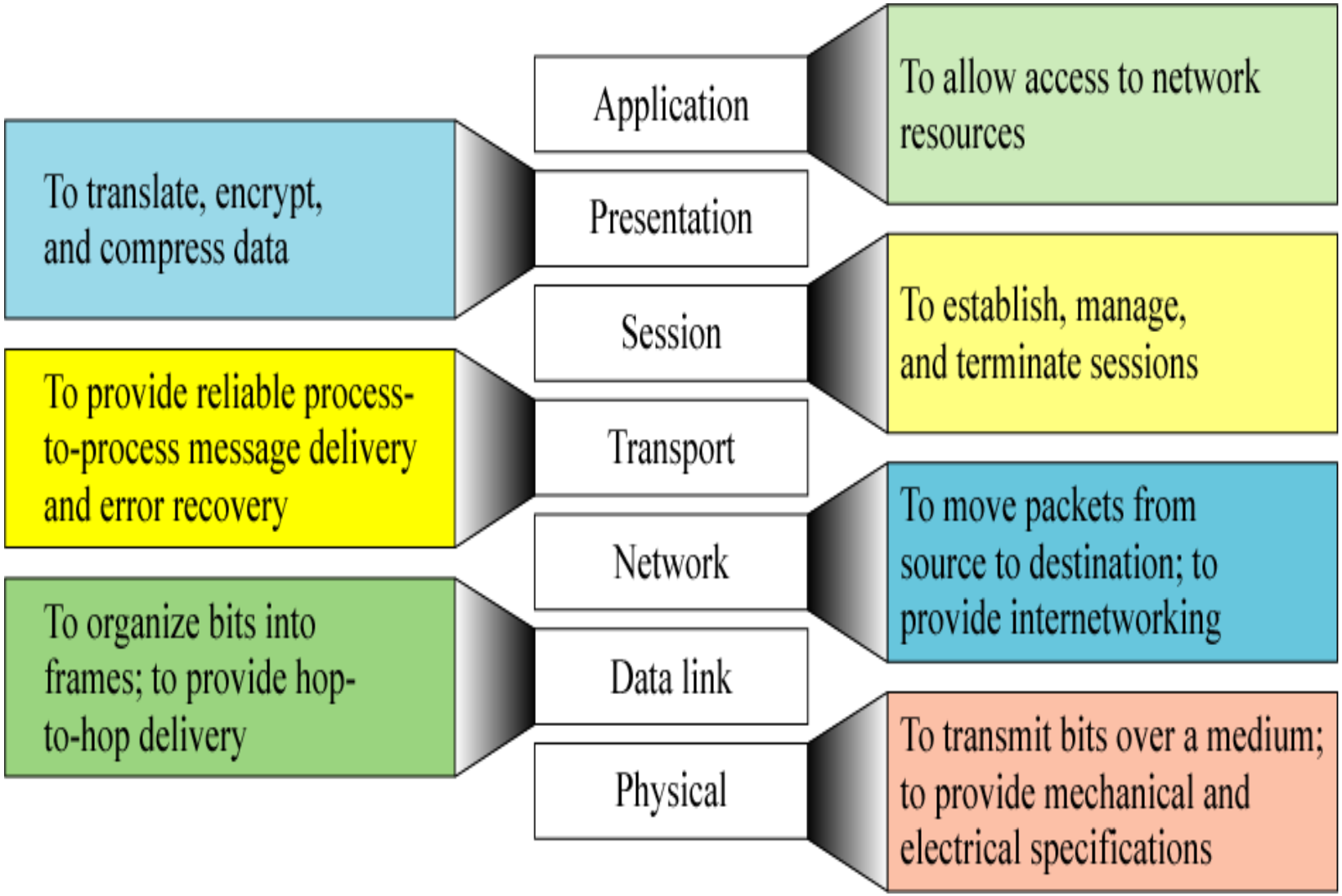
Standards Organizations



OSI Model

- OSI model is a seven layer standard
- Was developed as a basic reference model to define layered networks and layered protocols
- Each layer is meant to provide certain services to the other layers adjacent to it

OSI Architecture



Open System Interconnection

- The idea is to provide a modular framework, allowing diverse entities to communicate with each other
- A buggy implementation of a layer can be changed without changing other layers since interfaces are well-defined
- There were already quite a few implementations before the OSI model was proposed
- All implementations follow the layered model, but the layer-boundaries are fuzzy, sometimes even merging layers

OSI Physical Layer

- Concerned with transmission of unstructured bit stream over physical medium
  - How many volts for 0, how many for 1?
  - Number of bits of second to be transmitted.
  - Synchronization of bits
  - Standardized protocol dealing with electrical, mechanical and signaling interfaces.
- Line configuration

OSI Physical Layer

- Physical Topology
- Transmission mode
  - Simplex
  - Half Duplex
  - Full Duplex

- Examples: RS-232, X.21, Ethernet

OSI Data link Layer

- Provides for the reliable transfer of information across the physical link
  - Makes Physical layer appear error free to upper layers
- Consists of two sub-layers:
  - Logical Link Control (LLC) defines how data is transferred over the cable and provides data link service to the higher layers.
  - Medium Access Control (MAC) defines who can use the network when multiple computers are trying to access it simultaneously (i.e. Token passing, Ethernet [CSMA/CD]).

Responsibilities of Data Link Layer

- Framing – Bits arrived from Physical layer are grouped together into frames
- Physical Addressing – Headers identify source and destination of the frames
- Flow Control – Comes into effect when receiver is unable to cope up with rates of the sender
- Error Control – Mechanisms for detection of errors and re-transmission
- Access Control – To find the ‘right’ time to send data

OSI Network Layer

- Concerned with the transmission of packets.
- Responsible for
  - establishing,
  - maintaining, and
  - terminating connections

- Two protocols are most widely used.
  - X.25 (Connection Oriented)
  - IP (Connectionless)

Responsibilities of Network Layer

- Logical addressing
  - Comes handy when packets cross local network boundaries
  - Contained in the header of Network Layer
- Routing
  - Delivery of data from source to destination
  - Choosing the best path at given point of time

OSI Transport Layer

- Transport is responsible for
  - creating and
  - maintaining the

  basic end-to-end connection between communicating open systems,
- It ensures that
  - the bits delivered to the receiver are the same
  - as the bits transmitted by the sender;
  - in the same order
  - without modification, loss or duplication

OSI Transport Layer

- Transport Layer protocols include the capability to acknowledge the receipt of a packet; if no acknowledgement is received, the Transport Layer protocol can retransmit the packet or time-out the connection and signal an error
- Transport protocols can also mark packets with sequencing information so that the destination system can properly order the packets if they're received out-of-sequence

Responsibilities of Transport Layer

- Service-point addressing – process to process communication running on a pair of computers
- Segmentation and Reassembly - information to be sent is broken into individual packets that are sent and reassembled into a complete message by the Transport Layer at the receiving node
- Connection control – connection less or connection oriented
- Flow Control – End to end flow control
- Error Control – process to process error control

OSI Transport Layer

- Example: TCP/IP
  - Defines two standard transport protocols: TCP and UDP
  - TCP implements a reliable data-stream protocol
    - connection oriented
  - UDP implements an unreliable data-stream
    - connectionless

OSI Session Layer

- Provides the control structure for communication between applications
- Establishes, manages, and terminates connections (sessions) between cooperating applications
- Not found in TCP/IP model
- In TCP/IP,its characteristics are provided by the TCP protocol. (Transport Layer)

OSI Presentation Layer

- Provides independence to the application processes from differences in data representation (syntax)
- Handles data format information for networked communications. This is done by converting data into a generic format that could be understood by both sides.
- Not found in TCP/IP model
- In TCP/IP, this function is provided by the Application Layer.

  e.g. Multipurpose Internet Mail Extensions (MIME)

Responsibilities of Presentation Layer

- Translation
  - Interoperability between different encoding schemes between communicating systems. Like, conversion of an EBCDIC-coded text file to an ASCII-coded file.
- Encryption
  - sensitive information is encrypted before sending and decrypted by the receiver
- Compression
  - Compression is used to conserve limited bandwidth, useful for multimedia transmissions

OSI Application Layer

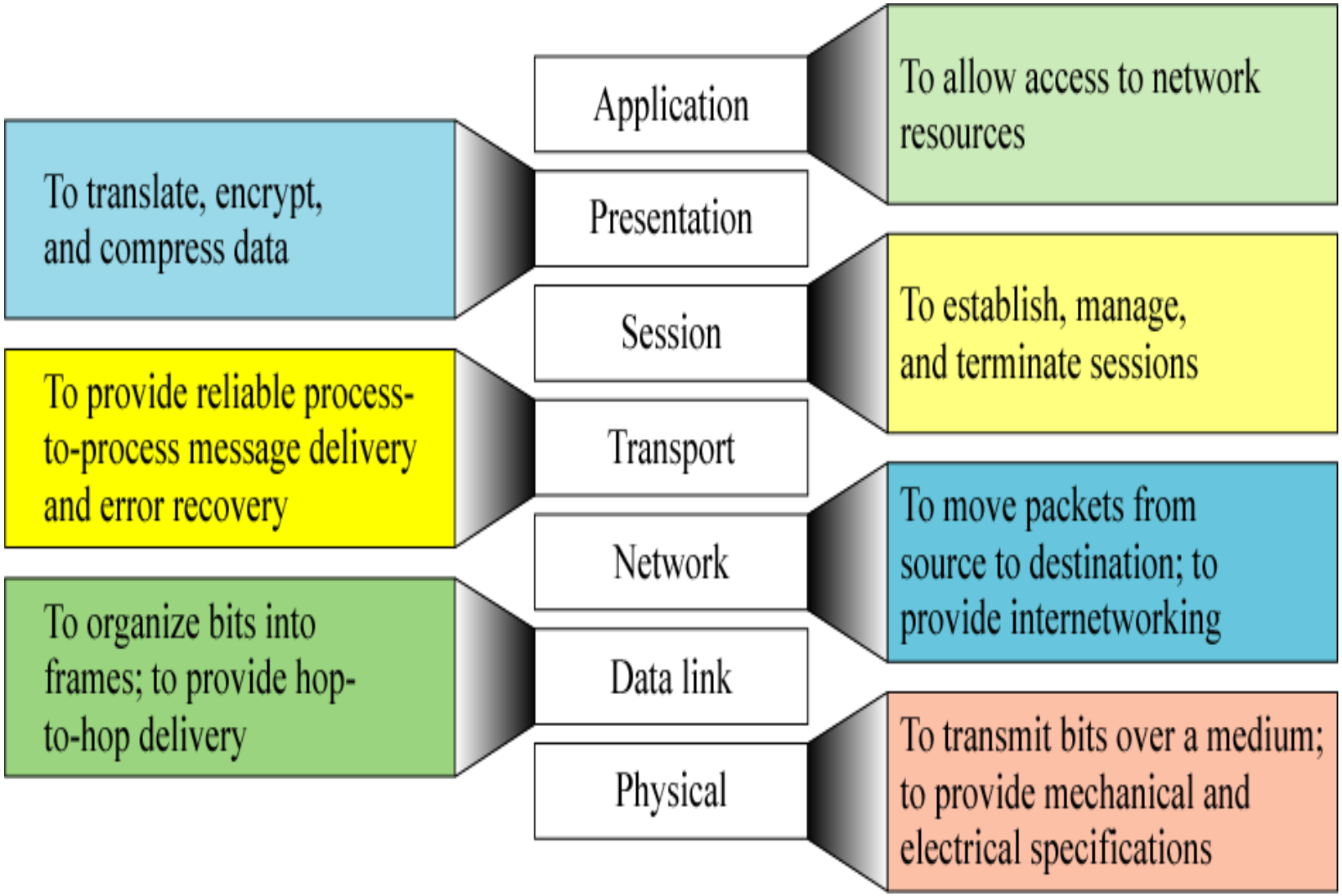
- It is the top layer of the reference model.
- It provides a set of interfaces for applications to obtain access to networked services as well as access to the kinds of network services that support applications directly.
- Examples

  TCP/IP - FTP,SMTP,TELNET,DNS,SNMP

TCP/IP Architecture Dominance

- TCP/IP protocols matured quicker than similar OSI protocols
  - When the need for interoperability across networks was recognized, only TCP/IP was available and ready to go
- OSI model is unnecessarily complex
  - Accomplishes in seven layers what TCP/IP does with fewer layers

OSI Architecture

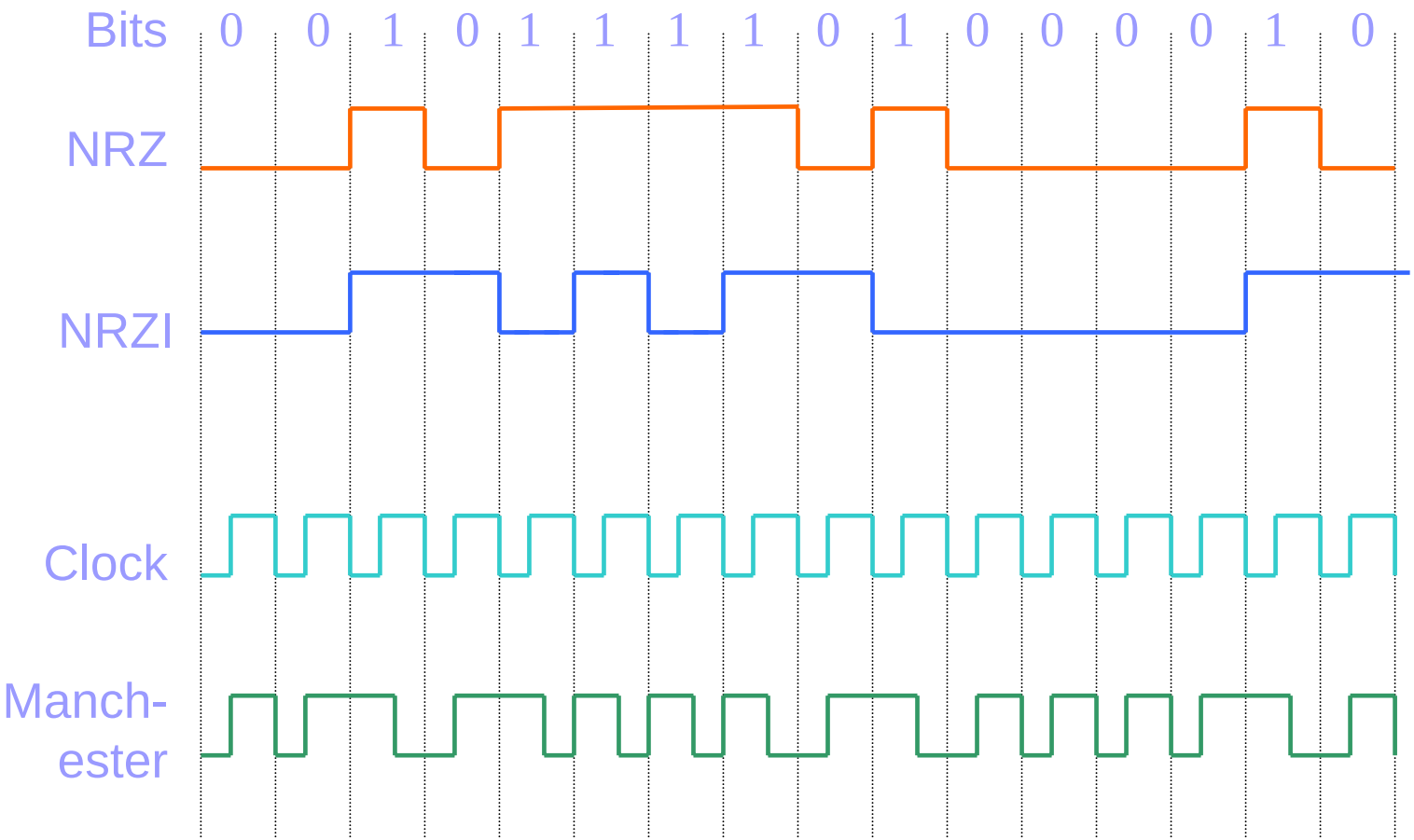


Physical Layer

Data Encoding Techniques

- Binary data needs to be encoded before it can be sent over the link
- 1 and 0 correspond to
  - Two different voltage levels on copper link
  - Different power levels on optical link
- Encoding is handled by signaling component on NIC
- Encoding schemes
  - NRZ
  - NRZI
  - Manchester
  - 4B/5B

Encoding strategies



NRZ

- Obvious thing to do
  - Map ‘low’ level to 0
  - Map ‘high’ level to 1
- Problem
  - Consecutive 1s means signal stays high for long
  - Receiver and sender clocks are not precisely synchronised
  - Clock recovery at receiver becomes difficult

NRZI

- Transition from current signal level to encode ‘1’
- Stay at current level to encode ‘0’
- This solves the problem of consecutive 1s but does nothing for consecutive 0s

Manchester

- Clock is merged with signal
- Transmits EXOR of clock with NRZ data
- Encoding
  - ‘0’ as low to high transition
  - ‘1’ as high to low transition
- Clock can be very easily recovered at receiver
- But it doubles the signal transitions
  - Encoding efficiency becomes 50%

4B/5B

- Attempts to address inefficiency of Manchester encoding without suffering from the problem of having extended duration of high or low signals
- Idea is to insert extra bits into bit streams to break long sequence of 0s or 1s
- 4 bits of data is encoded into 5 bit code
- 5 bits codes are so selected that each has no more than one leading and two trailing 0s, resulting in not more than three consecutive 0’s
- Resulting codes are transmitted using NRZI
- Efficiency is 80%

4B/5B codes

4 bit data	5 bit code
0000	11110
0001	01001
…	
1110	11100
1111	11101

Data Link Layer

IEEE 802

- IEEE 802 refers to a family of IEEE standards dealing with LANs and MANs
- IEEE 802 standards deal with networks carrying variable-size packets.
- The number 802 was simply the next free number IEEE could assign
  - 802 is sometimes associated with the date the first meeting was held — February 1980.
- The services and protocols specified in IEEE 802 map to the lower two layers - Data Link and Physical
  - IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC)

Some members of 802 family

Name	Protocol
IEEE 802.1	Bridging and Network Management
IEEE 802.2	Logical link control
IEEE 802.3	Ethernet
IEEE 802.4	Token bus
IEEE 802.5	MAC layer for a Token Ring
IEEE 802.6	Metropolitan Area Networks
IEEE 802.15	Wireless PAN
IEEE 802.15.1	Bluetooth
IEEE 802.15.4	ZigBee
IEEE 802.16	Broadband Wireless Access (WiMAX)

Ethernet

A Brief History

- In late 1972, Robert Metcalfe and his Xerox PARC colleagues developed the first experimental Ethernet system.
- The network was called Alto Aloha Network.
- The experimental Ethernet was used to link Altos to one another, and to servers and laser printers.
- Data transmission rate on the experimental Ethernet was 2.94 Mbps.
- In 1973 Metcalfe changed the name to "Ethernet," to make it clear that the system could support any computer.

Ethernet Sketch by Bob

Ethernet standards over years

Standard	Year	Description
802.3	1982	CSMA/CD based Ethernet (Thick Ethernet)
802.3a	1985	10Base-2 (Thin Ethernet)
802.3i	1990	10Base-T (Twisted pair)
802.3u	1995	100Base-T (Fast Ethernet and auto negotiation)
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ae	2002	10-Gigabit Ethernet

Ethernet

- Ethernet uses CSMA/CD protocol to transfer data over the shared medium
- Transmission
  - Wait until Frame is ready for transmission and medium becomes idle
  - Start transmitting.
  - Did a collision occur? If so, go to collision handling procedure.
  - Reset retransmission counters and end frame transmission

Ethernet

- Collision handling procedure
  - Continue transmission until minimum packet time is reached (jam signal) to ensure that all receivers detect the collision
  - Increment retransmission counter
  - If maximum number of transmission attempts are reached, abort transmission.
  - Calculate and wait for random backoff period based on number of collision and Go to Transmission procedure

Fast Ethernet

- The need for faster speed resulted in a 1995 standard for 100 Mb/s
- Although the 100Base-T standard was close to 10Base-T, network designers had to determine which customers needed the extra bandwidth.
- Ethernet networks then could be 10 Mb/s or 100 Mb/s (Fast Ethernet) and connected with 10/100 Mb/s Ethernet devices that automatically switched network speeds.

Fast Ethernet

- Because there was a choice of bandwidths, the standard also allowed for equipment that could auto-negotiate the two speeds.
  - If Ethernet device was transmitting or receiving from a 10 Mb/s network, it could support that network.
  - If the network operated at 100 Mb/s, the same device could switch automatically to the higher rate.

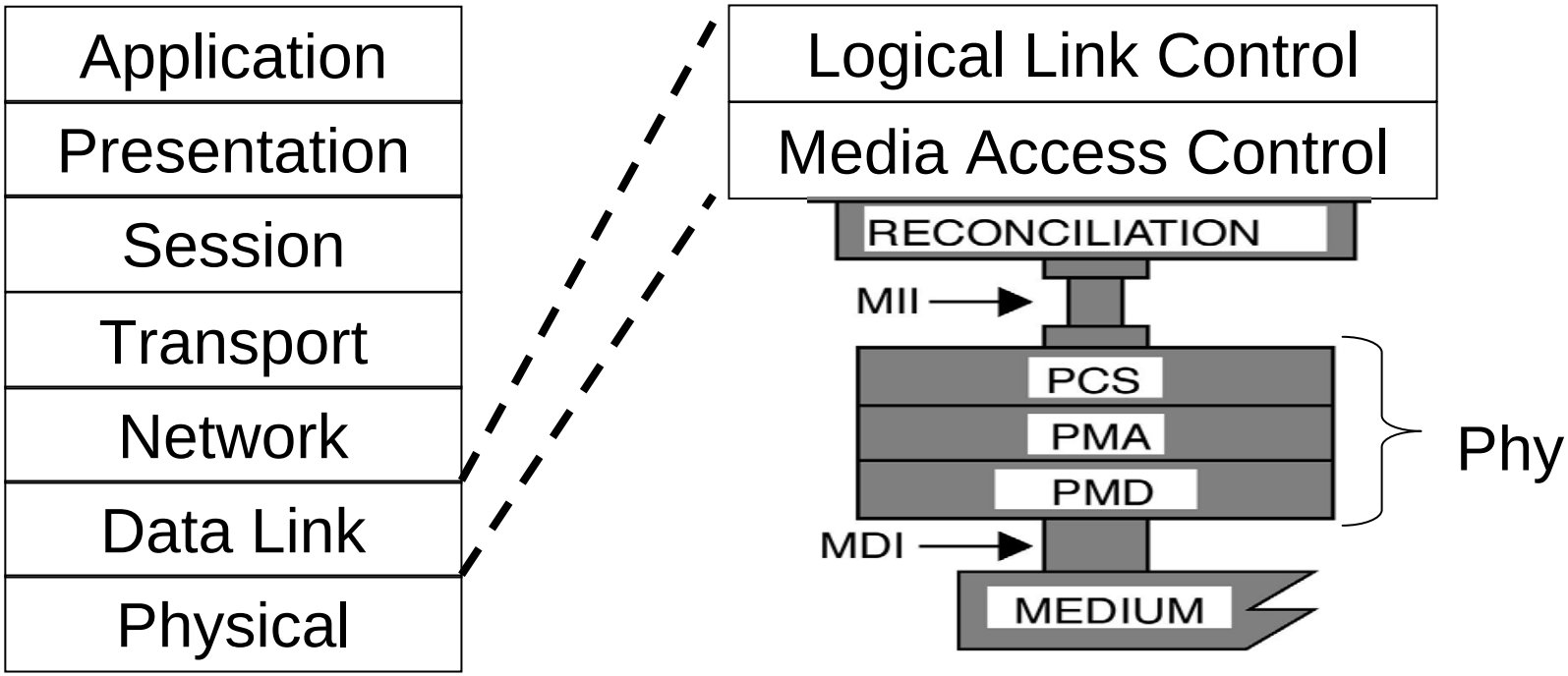
Gigabit Ethernet

- Gigabit Ethernet takes advantage of jumbo frames to reduce the frame rate
  - Standard Ethernet frame size is 64 to 1518 bytes.
  - Jumbo frames are between 64 to 9215 bytes.
  - Using jumbo frames on Gigabit Ethernet links greatly reduces the number of packets (from more than 80,000 to less than 15,000 per second)
- Gigabit Ethernet can be transmitted over CAT 5 cable and optical fiber

10Gigabit Ethernet

- The operation of 10 Gigabit Ethernet is similar to that of lower speed Ethernets.
- It maintains the IEEE 802.3 Ethernet frame size and format that preserves layer 3 and higher protocols.
- However, 10 Gigabit Ethernet only operates over point-to-point links in full-duplex mode.
- It uses fiber as well as copper as medium for transporting Ethernet frames.
- There are seven media types, which are designed for use in either local or wide area networking.

802.3 Layers (For 100 Mbps)

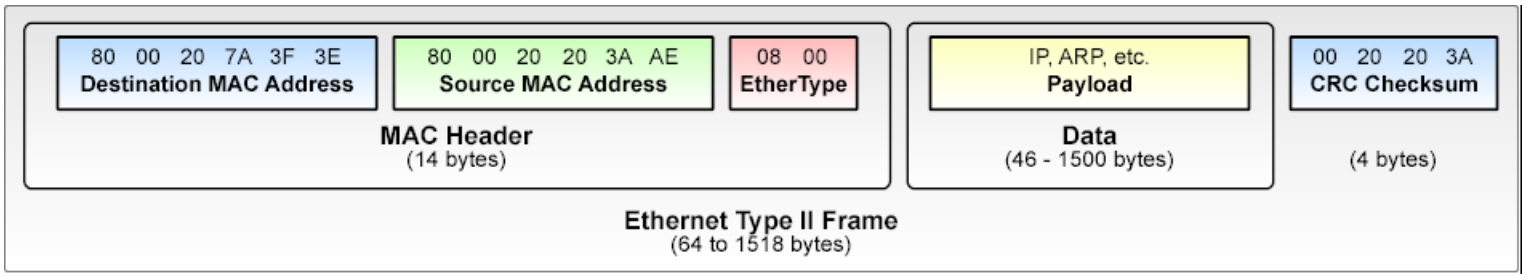


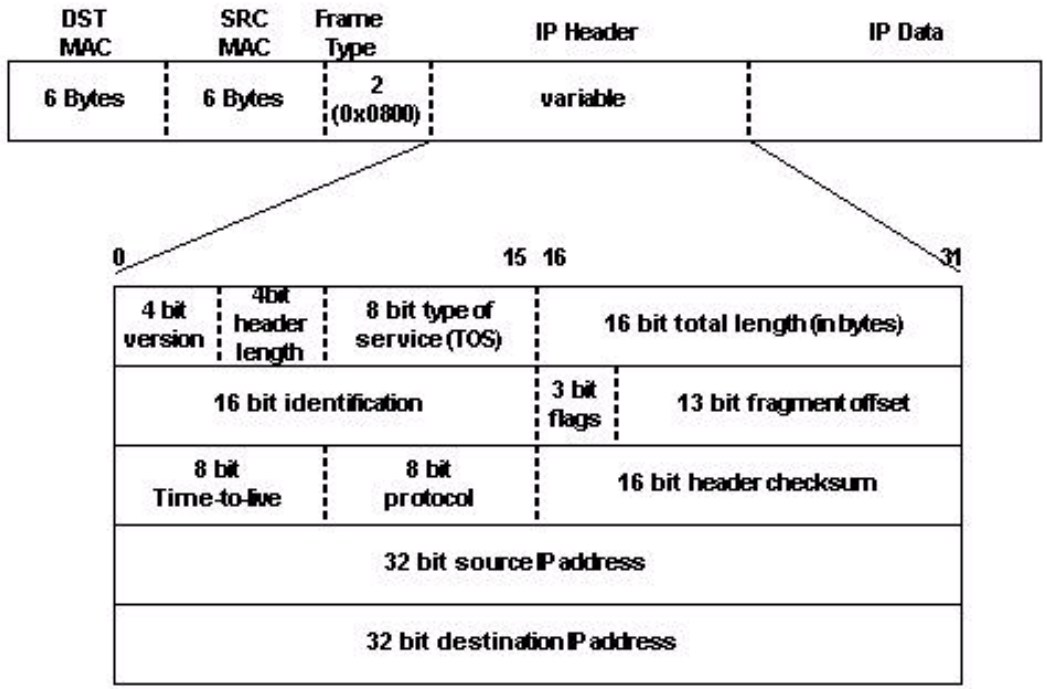
MII: Media Independent Interface PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment PMD: Physical Medium Dependent

MDI : Media Dependent Interface

Ethernet Frame





Ethernet Products

- Network Interface Card
  - Connects a computer to the network
  - PCI bus
  - 10/100 Mbps Auto negotiated , full duplex
  - Plug-n-play

- Hubs / repeaters
  Connects two or more segments together

Ethernet Products

- Switches
  Links multiple networks together
  Increases bandwidth available to each network
  Separate collision Domain
  cut-through, store-and-forward switching
  address learning
  High speed up-link (fast Ethernet, gigabit Ethernet , ATM)

Why Ethernet is Everywhere?

- About 80% of network connections are based on Ethernet.
- The most important factors that have helped Ethernet to become popular are:
  - Scalability
  - Reliability : Stable products, interoperability is proven
  - Cost : Volumes!

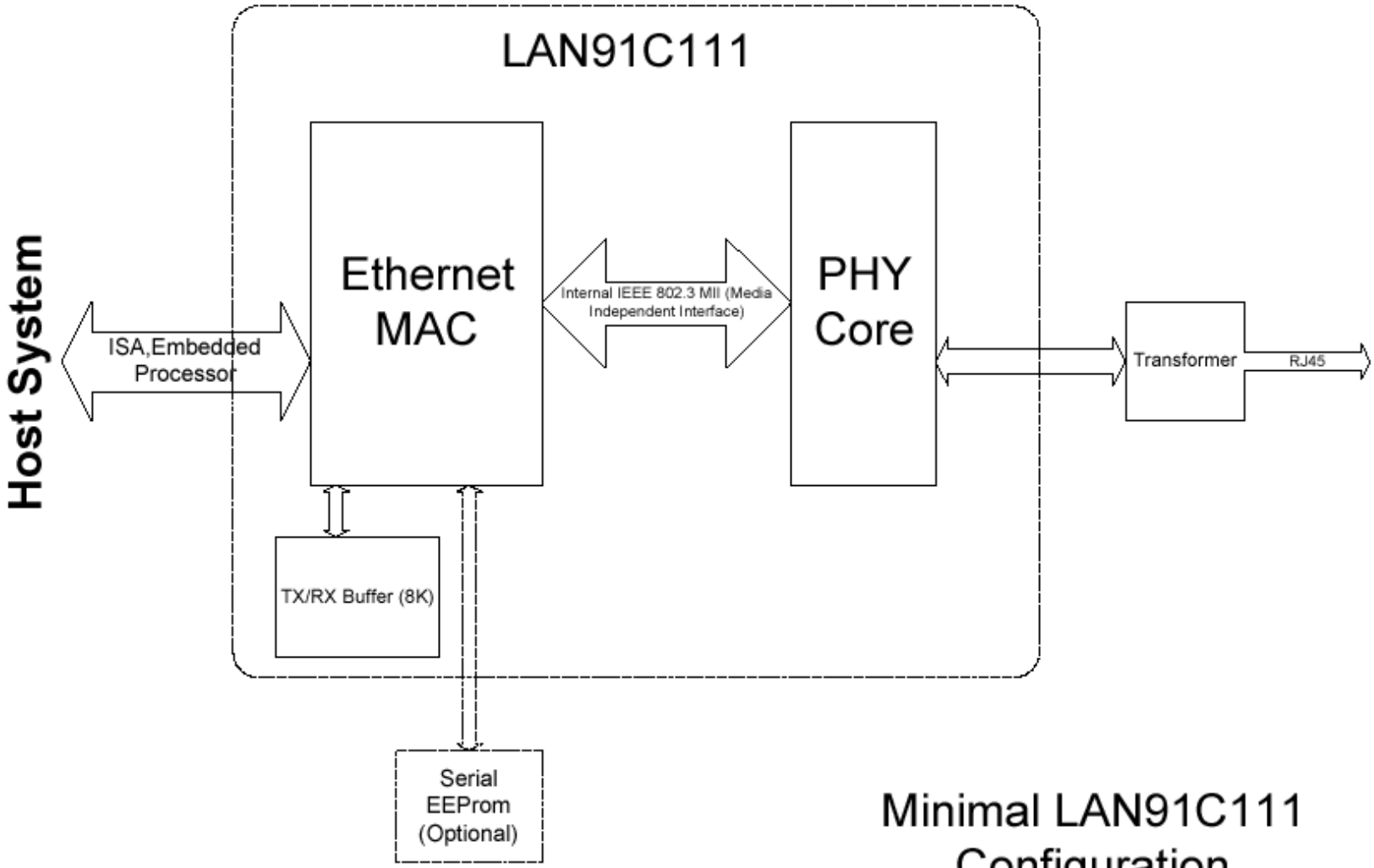
  Since Ethernet is being used for last 10-15 years, people are reluctant to shift!! And Ethernet has also evolved and provides back ward compatibility.

Ethernet Controller

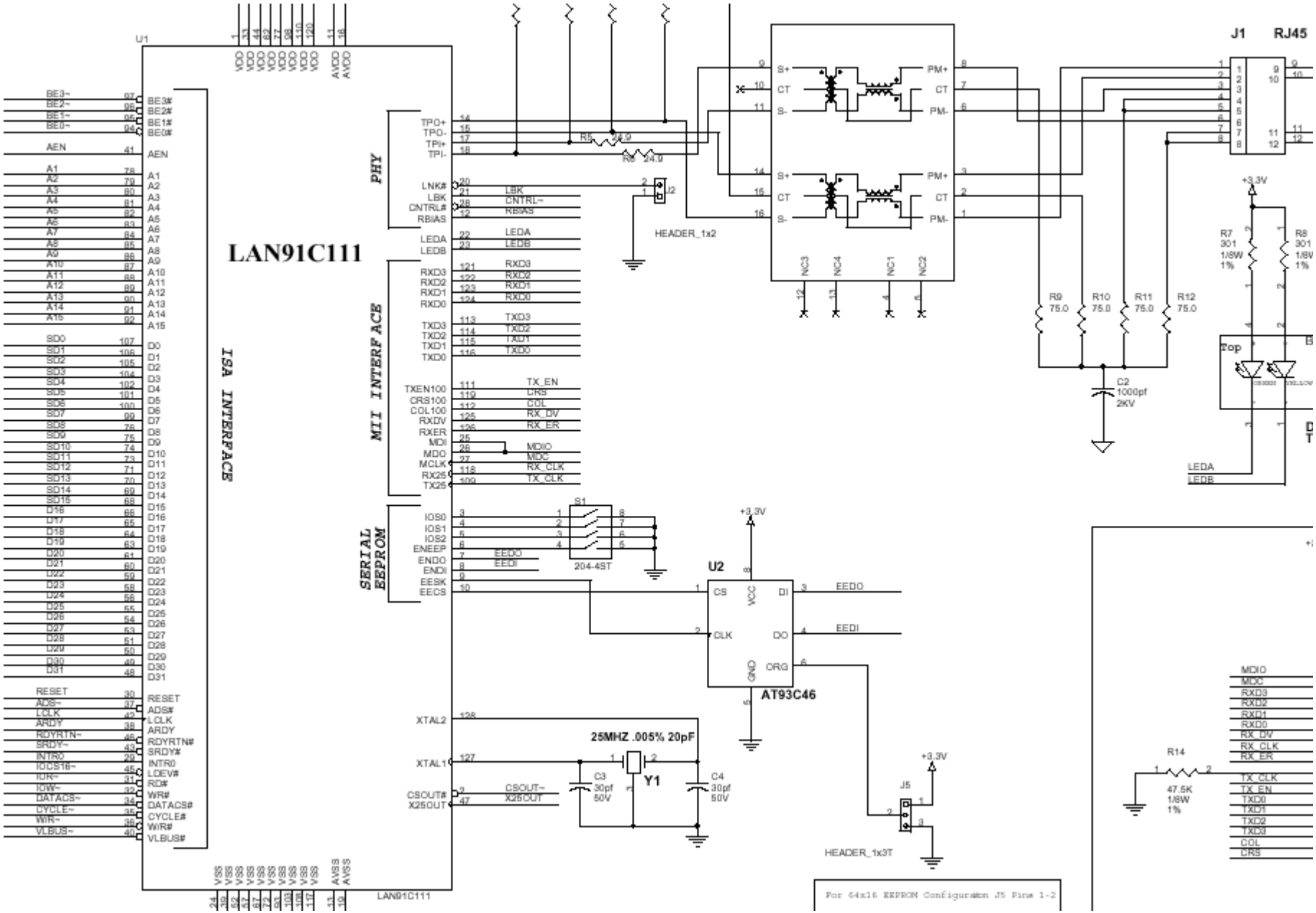
- Implements MAC and PHY in Silicon
- LLC layer is implemented as driver that interacts with Ethernet controller
- High end microcontrollers have on chip Ethernet
  - NET+ARM Ethernet-ready System-on-Chip
  - Used for developing a network-enabled application
- For smaller microcontrollers, external Ethernet controller needs to be used
- Examples: intel's 82562, Realtek's RTL8019, SMC's LAN91C111

LAN91C111

- Single chip Ethernet controller
  - Implements PHY and MAC
- Dual speed 10/100 mbps
- Supports full duplex switched Ethernet
- 8kbytes internal memory for receive and transmit FIFO buffers
- Supports 8, 16 and 32 bit CPU accesses
- Supports multiple embedded processor host interfaces
  - ARM, SH, PowerPC, Coldfire, 68XXX, MIPS R3000



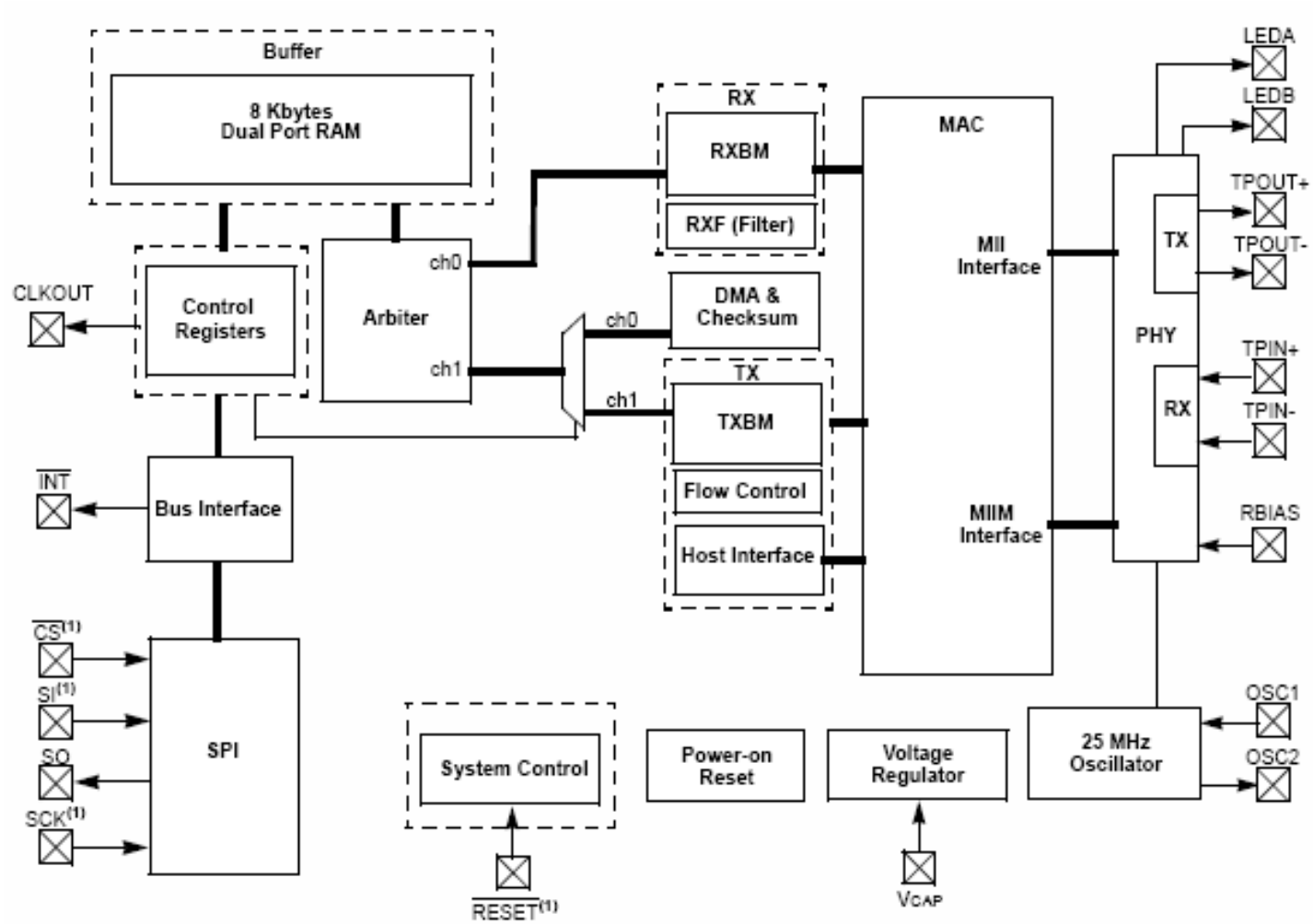
Minimal LAN91C111 Configuration


LAN91C111
ISA INTERFACE
PHY
MII INTERFACE
SERIAL EEPROM
U1
U2
AT93C46
J1
RJ45
Y1
25MHZ .005% 20pF
HEADER_1x2
HEADER_1x3T
S1
204-4ST
R5
R6
24.9
R7
301
1/8W
1%
R8
301
1/8W
1%
R9
75.0
R10
75.0
R11
75.0
R12
75.0
C2
1000pf
2KV
C3
30pf
50V
C4
30pf
50V
R14
47.5K
1/8W
1%
+3.3V
LEDA
LEDB
TX_EN
CRS
COL
RX_DV
RX_ER
RX_CLK
TX_CLK
MDIO
MDC
EEDO
EEDI
CSOUT~
X25OUT
For 64x16 EEPROM Configuration J5 Pins 1-2

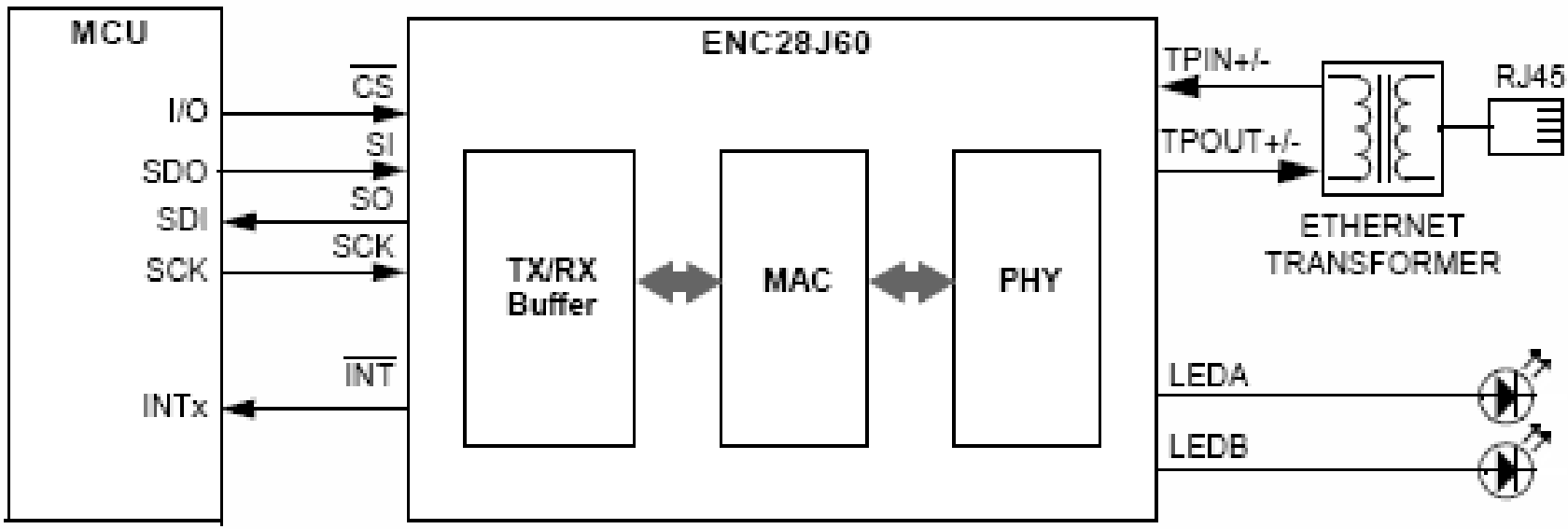
ENC28J60 – Ethernet Controller

- Standalone Ethernet controller with SPI interface
- Fully compatible with 10/100/1000Base-T networks
- Integrated MAC and 10Base-T PHY
- Supports half duplex and full duplex modes
- 8KB transmit receive dual port packet buffer
- Hardware managed circular Receive FIFO
- MAC support unicast, multicast and broadcast Packets
- MAC supports programmable packet filtering and wakeup host functions

ENC28J60 – Ethernet Controller

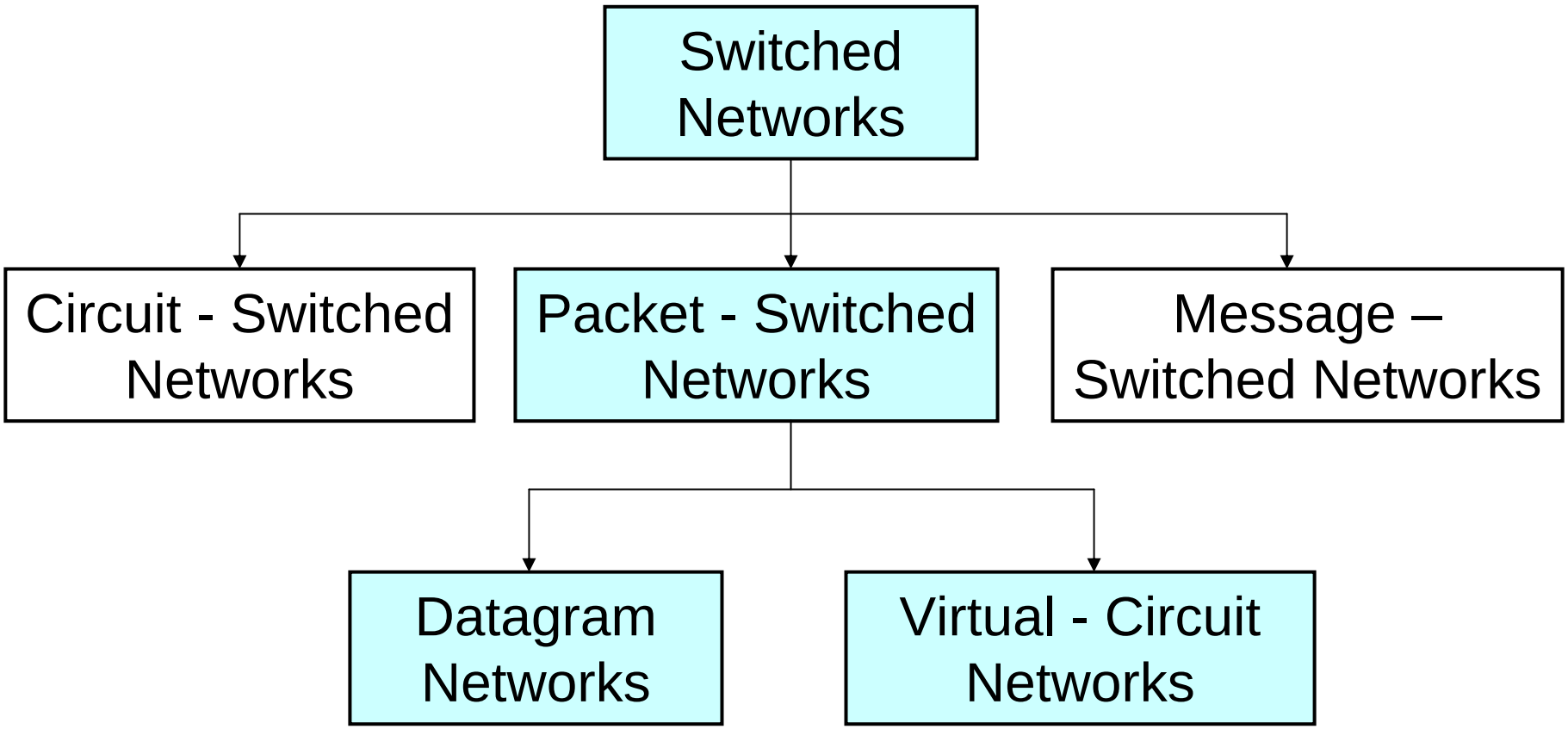


Connecting to a MCU



Building bigger Networks

- Directly connected networks suffer from two limitations
  - Number of hosts that can be attached
  - Area that a network can span
- Bigger networks are built using Data Switches, also called as packet switches
- Concept is similar to telephone network, which uses circuit switches



Packet Vs. Circuit Switching

- Packet switching was designed to provide efficient facility than circuit switching for bursty data traffic
- It can connect two stations operating at different data rates
- Routing function of packet switches attempts to dynamically find the least-cost path through the network
  - Number of hops
  - Expected delay

Packet Switching

- A switch allows to interconnect links to form a larger network
- It is a multi-input, multi-output device which transfers packet from an input to one or more outputs
- It uses star topology
- Switching or forwarding is a function of network layer
- Packet forwarding decision is based on the header
  - Datagram or connectionless approach
  - Virtual circuit or connection oriented approach

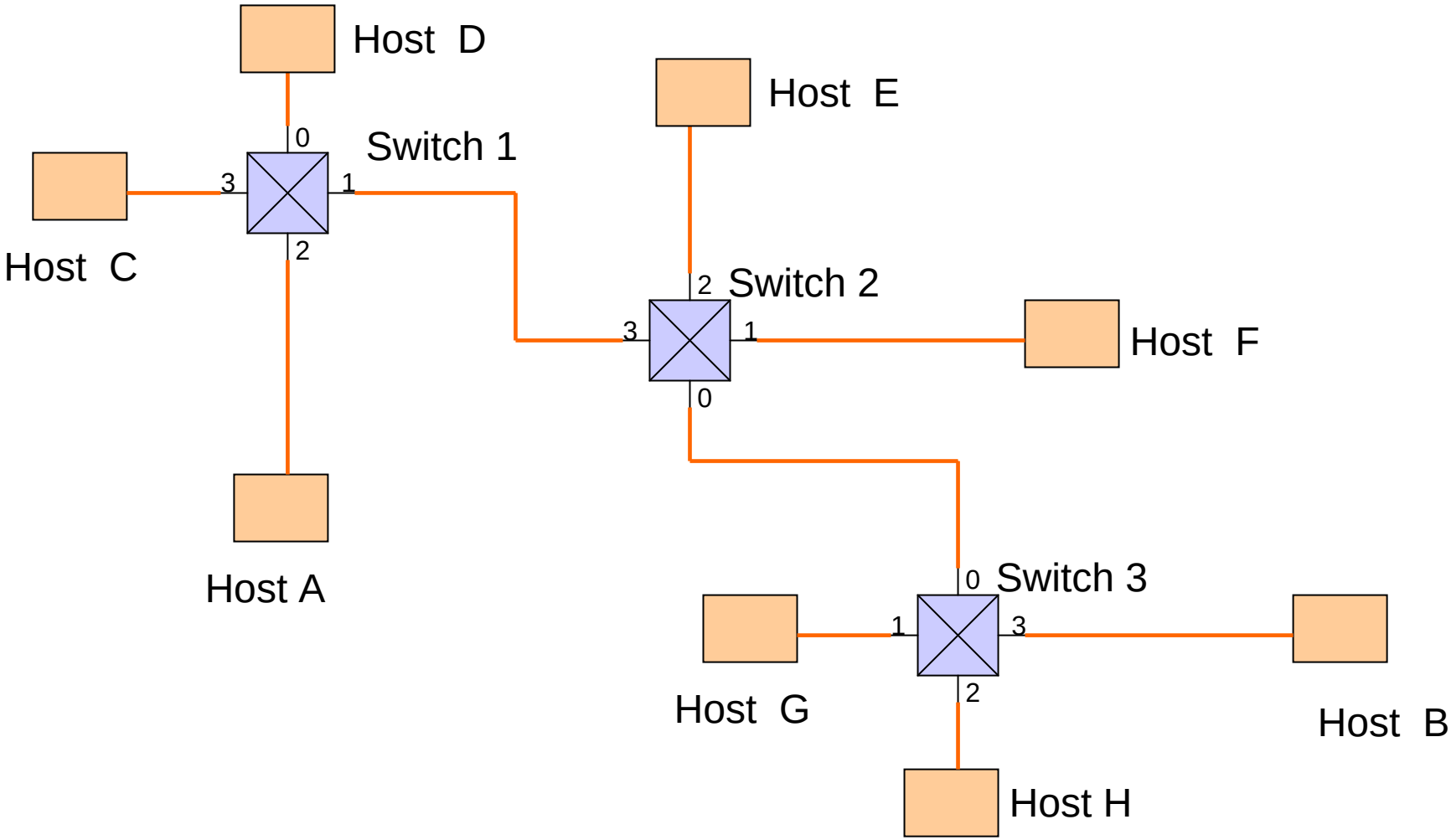
Datagram

- Every packet has complete destination address
- Each switch maintains forwarding table
  - Destination address and port number
  - Switch learns the table
- A host can send packet anywhere at any time (no setup required)
- Host has no way of knowing
  - Network is capable of delivering the packet
  - Destination exists, is up and running

Datagram (contd.)

- Each packet is forwarded independently of previous packet
  - Two packet for same destination may follow different paths
  - Could be due to forwarding table updation
- A switch or link failure may not serious effect on communication
  - Alternate routes are found, if possible
  - Forwarding tables updated accordingly

Datagram forwarding



Forwarding Table

Destination	Port
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

Forwarding table for Switch 2

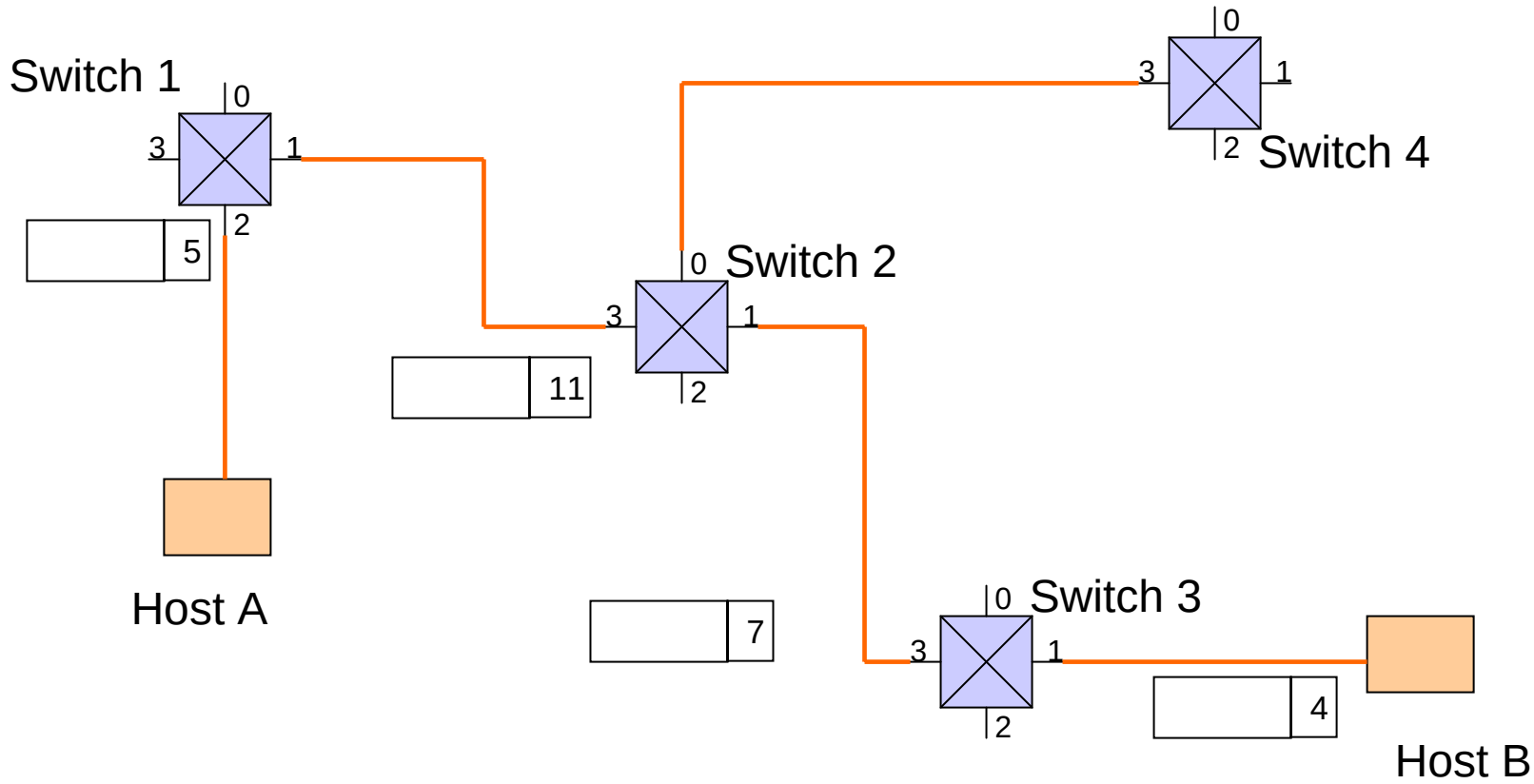
Virtual Circuit Switching

- Connection oriented model
- Virtual connection is setup from source to destination
- Data transfer is three stage process
  - Connection setup
  - Data Transfer
  - Teardown
- Establishing connection
  - Permanent Virtual Circuit(PVC)
    - Setup and deleted by the administrator
  - Switched Virtual Circuit (SVC)
    - Setup and deleted by hosts

PVC

- There is one entry in a VC table for each connection
  - Incoming interface on which packets arrive
  - A virtual circuit identifier (VCI) that will be carried in the header of arriving packets
  - Outgoing interface on which the packets will leave
  - A VCI that will be used for outgoing packets
- Incoming and outgoing VCI values are not same
- VCI is not globally significant identifier for the VC
- It has significance only for the link
- Network administrator picks unused VCI values on each link for connection

Virtual Circuit Network



Virtual Circuit table entries

VC table at Switch 1

Incoming I/F	Incoming VCI	Outgoing I/F	Outgoing VCI
2	5	1	11

VC table at Switch 2

Incoming I/F	Incoming VCI	Outgoing I/F	Outgoing VCI
3	11	0	7

VC table at Switch 3

Incoming I/F	Incoming VCI	Outgoing I/F	Outgoing VCI
0	7	3	4

SVC

- In real networks of reasonable size, configuring VC tables in large number of switches is cumbersome
- Hence VCs are setup using signaling
  - Host A sends setup message having complete destination address of host B.
  - This message needs to get all the way to B
  - Along the path it creates connection states
  - This is similar to sending a datagram to B, in that the switches know which output port to send the message so that it eventually reaches B

Setup

- When the switch receives connection request, it creates a new entry in VC table
  - In_port, out_port and picks value for incoming VCI
- This process repeats on every switch in the path
- Finally Host B receives the setup message and it assigns a incoming VCI, which identifies host A
- To complete the connection, it needs to told, what VCI the downstream neighbor is using for this connection
- This is done through acknowledgement which goes back all the way to host A
- When host A no longer wants to send data to host B, it sends a teardown message to switch 1.

Virtual Circuit Switching

- One Round Trip Delay before first data packet
- Per packet overhead caused by header is reduced
- If switch or link fails, new connection needs to be established and old one needs to be torn down
- Quality of service can be provided
  - Switches set aside resources to meet this
- Examples of Virtual Circuit Technologies
  - X.25
  - Frame Relay
  - ATM

ATM

Asynchronous Transfer Mode

- ATM is a cell-switching and multiplexing technology
- It combines the benefits of circuit switching
  - guaranteed capacity
  - constant transmission delay
- With those of packet switching
  - flexibility
  - efficiency for intermittent traffic
- International Telecommunication Union-Telecommunications Standards Section (ITU-T) standard for cell relay wherein information for multiple service types, such as voice, video, or data, is conveyed in small, fixed-size cells

ATM

- Connection Setup phase is called signalling
  - Q.2931 protocol is used
  - Discovers suitable route across an ATM network
  - Allocates resources at switches along the circuit
- QoS is one of its greatest strength
- Address format is E.164
- Packets are always of fixed length: 53 bytes
  - 5 byte header + 48 byte payload = 1 cell

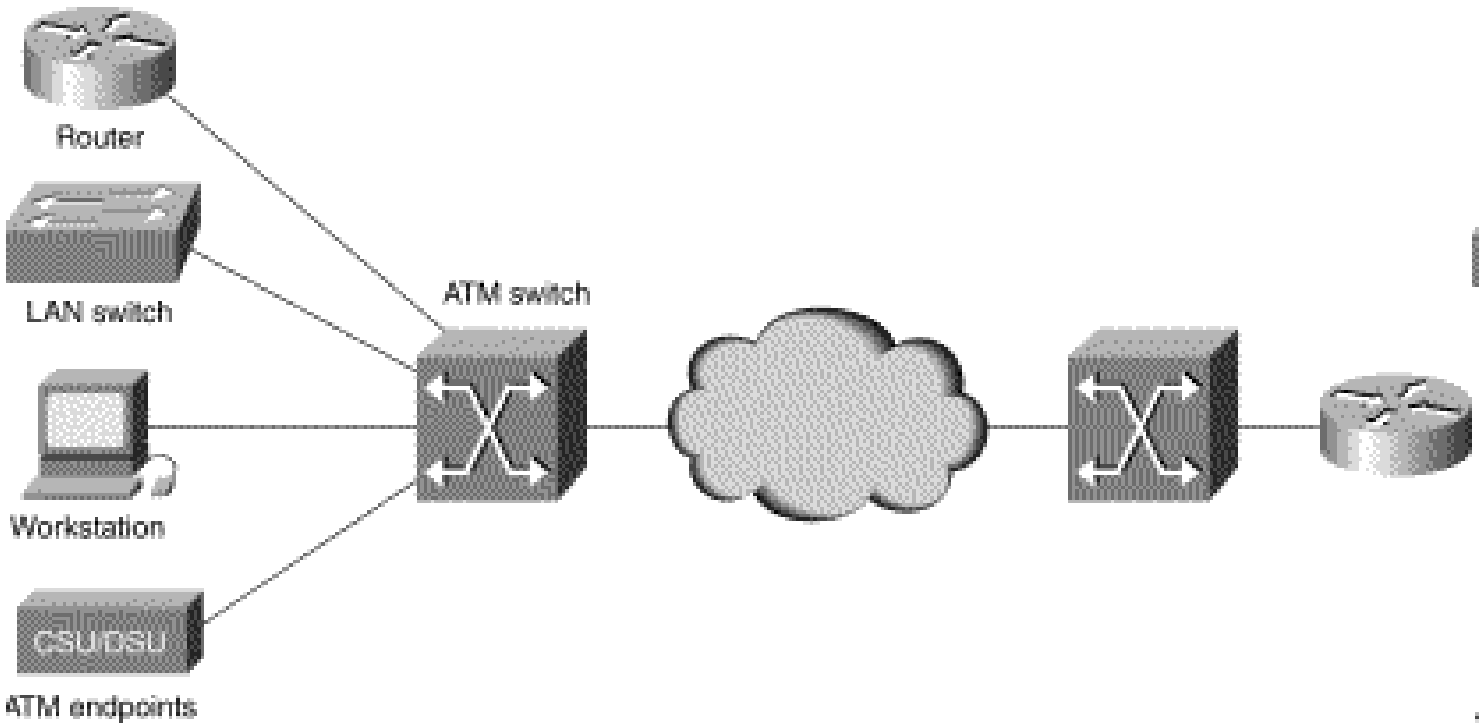
Cell

- Fixed length
  - Processing packets in switch is easier
  - Enables parallelism, improves scalability
  - Finer control over output queue management
  - Latencies are predictable
- Small size
  - Input to output queue transfers are efficient
  - Header to payload ratio
  - Filling up cell with voice samples
  - 48 is not power of 2

ATM Devices

- An ATM network is made up of an
  - ATM switch
  - ATM endpoints.
- An ATM switch
  - responsible for cell transit through an ATM network.
  - It accepts the incoming cell from an ATM endpoint or another ATM switch.
  - It then reads and updates the cell header information switches the cell to an output interface
- An ATM endpoint
  - ATM network interface adapter
  - Workstations, routers, digital service units (DSUs), LAN switches

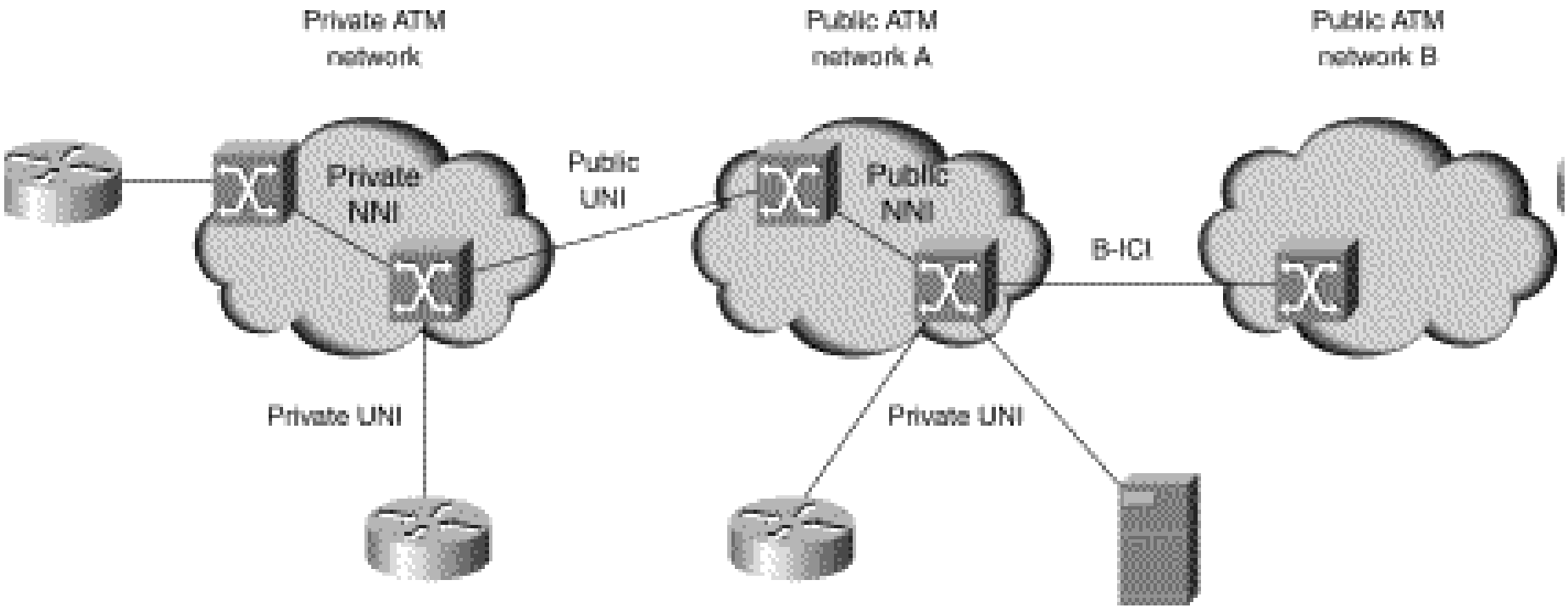
ATM Network



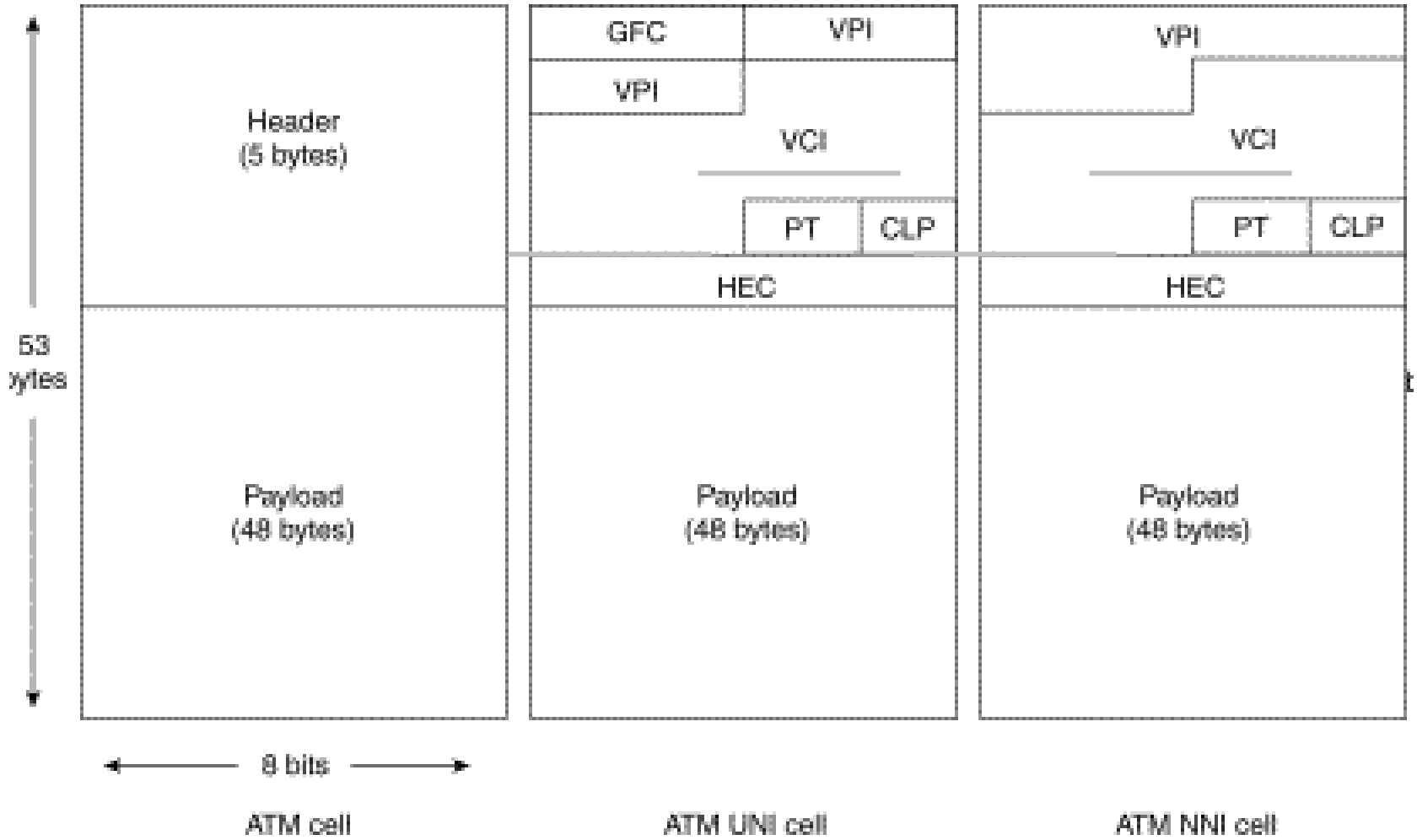
ATM Network Interfaces

- ATM switches support two primary types of interfaces
  - UNI (user- network interface)
    - connects ATM end systems (such as hosts and routers) to an ATM switch
  - NNI (network- network interface)
    - connects two ATM switches.
- UNI and NNI can be further subdivided into public and private UNIs and NNIs

ATM Network Interfaces

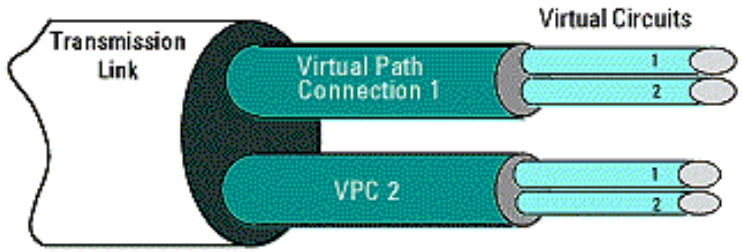


ATM Cell formats



Fields

- GFC: Generic Flow Control (4 bits)
  - Means to arbitrate access to link, if local site used some shared medium to connect to ATM
- VPI: Virtual Path Identifier (8 /12 bits)
- VCI: Virtual Circuit Identifier (16 bits)
  - Together they identify the next destination of a cell as it passes through a series of switch routers on its way to its destination.



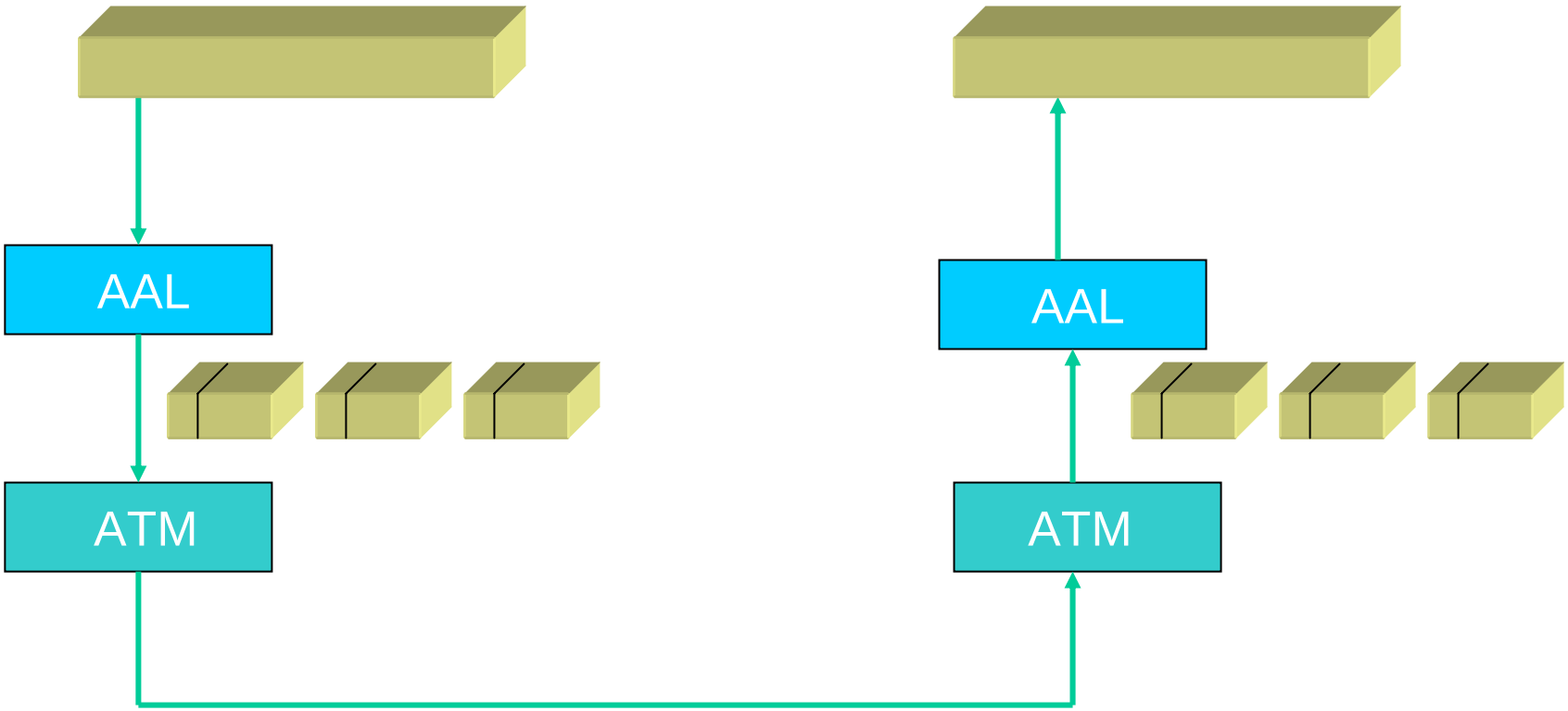
Fields (contd.)

- PT: Packet Type (3 bits)
  - First bit: cell contains user data or control data.
  - Second bit: Congestion, if the cell contains user data
  - Third bit indicates whether the cell is the last in a series of cells that represent a single AAL5 frame.
- CLP: Congestion Loss Priority (1 bit)
  - indicates whether the cell should be discarded if it encounters extreme congestion
- HEC: Header Error Control (8 bits)
  - checksum calculated only on the header itself.

Segmentation

- Packets handed down by high-level protocol are often larger than 48bytes
- Segmentation is done by sender, reassembly is done by the receiver
- This is done by a protocol layer that sits between
  - ATM
  - Variable length packet protocol like IP
  - Called ATM adaptation layer (AAL)
- AAL is designed to support all types of services
  - Voice, Video, Data

Segmentation & Reassembly

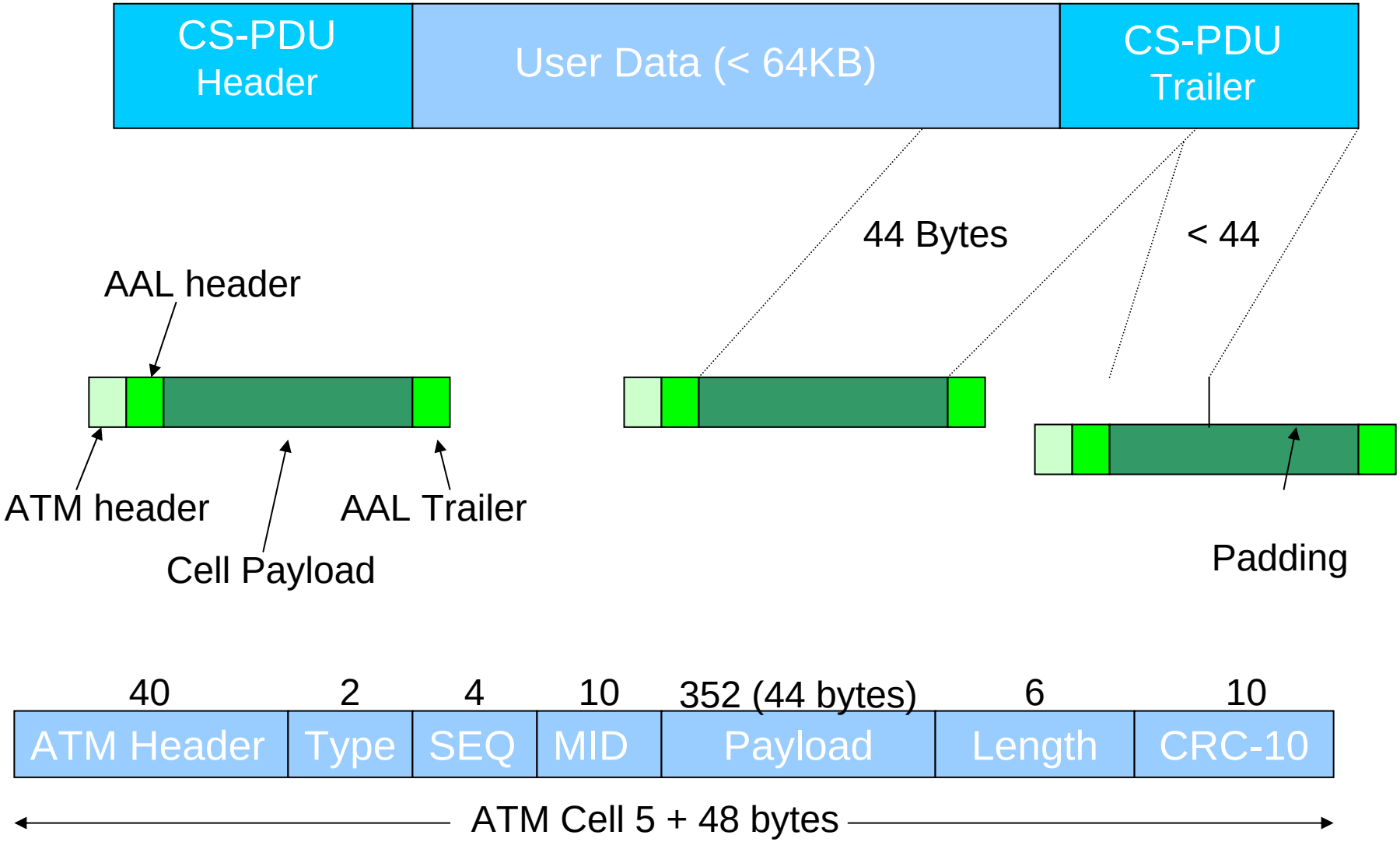


AAL

- Four adaptations layers were originally defined
  - 1 and 2 to support guaranteed bit rates (eg. Voice)
  - 3 and 4 for packet data
    - AAL3 for connection oriented (e.g. X.25)
    - AAL4 for connectionless (eg. IP)
    - Merged to form AAL3/4
  - Later AAL5 was proposed

AAL 3/4

- Provides information to allow variable length packets to be transported across ATM network
  - Series of fixed length cells
- Segmentation and Reassembly involves 2 steps
  - Convergence Sublayer – Protocol Data Unit (CS-PDU) for encapsulating variable length PDU
  - PDU passed on by AAL is encapsulated by adding header and trailer into the cell
- With 44 bytes of data for 9 bytes of header, the best possible efficiency is 83% (further degraded by CS-PDU encapsulation and partial filling of last cell)



WAN Protocols

Wide Area Networks

- A computer network that covers a broad area
  - Network whose communications links cross metropolitan, regional, or national boundaries
- WANs are used to connect LANs and other types of networks together
  - Allows users and computers in one location to communicate with users and computers in other locations.
- WANs built for one particular organization and are private.
- WANs built by Internet service providers, provide connections from an organization's LAN to the Internet.

WAN connections

- Leased line
  - Expensive but secure
- Circuit switching
  - Cheaper but low speed
- Packet switching
  - Uses shared medium
- Cell switching
  - Useful for voice and data

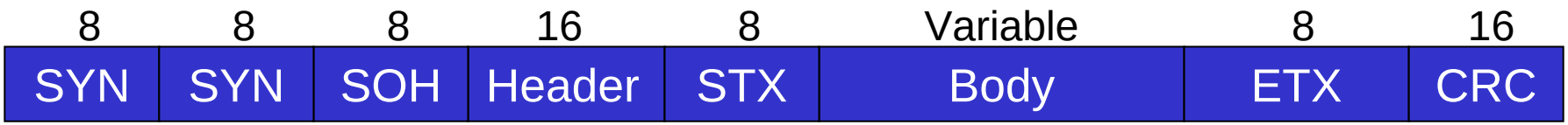
Framing

- Data encoding techniques specify how a sequence of bits can be transmitted
- Protocol layers are concerned about moving a block of data across the network
- The physical layer (network adapter) facilitates the exchange
  - Interpreting the series of bits
    - Where does a frame begins and ends
    - Which bits constitute a frame

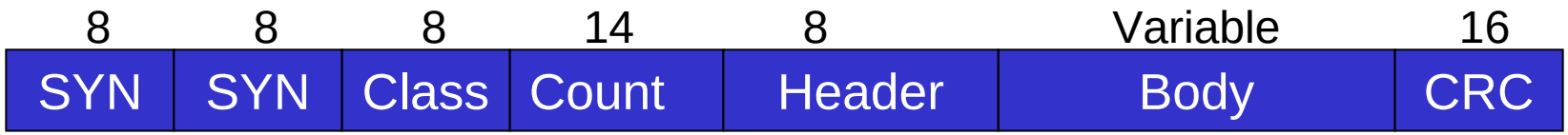
Framing Methods

- Byte oriented protocols
  - Sentinel method
    - Puts guarding characters at either end
    - eg. IBM's BISYNC, PPP
  - Byte counting method
    - Count of characters are sent in the header
    - eg. DECNET's DDCMP

BISYNC



DDCMP



Bit oriented protocols

- Bit oriented protocols
  - Not concerned with byte boundaries
  - Series of bits can be from a character set like ASCII or pixel values of image or a .exe file
- A frame is wrapped between a beginning sequence and ending sequence
- The sequence is also transmitted during idle period
  - Helps to keep receiver clock in sync.
- If the sequence appears in bit stream, bit stuffing is done
- IBM developed SDLC (synchronous data link control) which was standardized by ISO as HDLC (High-level data link control)

HDLC

HDLC

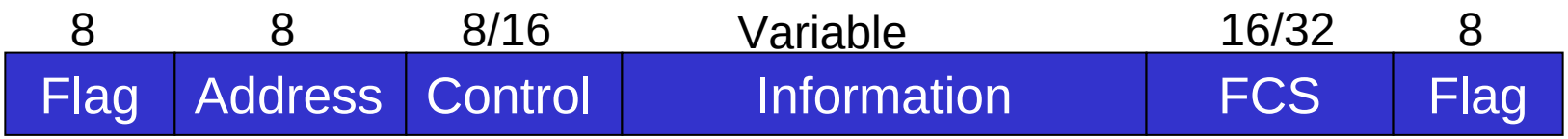
- Operates at Data Link Layer, of the OSI model
- Supports
  - half duplex and full duplex communication lines
  - point to point(peer to peer) and multi-point networks
- Specified by ISO 3009, ISO4335
- Widely used and is basis for many other important data link control protocols

Types of Stations

- Primary Station
  - Controls the operation of the link
  - Frames issued by primary are called commands
  - Separate logical link with every secondary station
- Secondary Station
  - Operates under control of Primary
  - Frames issued by secondary are called responses
- Combined
  - Combines features of Primary and Secondary
  - May issue both command and responses

Frame Structure

- Synchronous transmission
- Single frame format suffices all types of data and control exchanges
- Flag, address and control are headers
- FCS and flag are trailers



Frame Structure(contd.)

- Address field
  - Indicates the secondary station
  - Included even in point-point link for sake of uniformity
  - 1111 1111 is interpreted as all station address
- Control field
  - Information frames (I-frames) carry data to be transmitted for the user
  - Supervisory frame(s-frames) used for Automatic Recovery Request(ARQ) mechanisms
  - Unnumbered frames(U-frames) provide supplementary link control functions

Frame Structure(contd.)

- Information field
  - Present only in I-frames and some U frames
  - Must contain integral number of octets
  - Length is variable and up to some system-defined maximum
- FCS
  - Error detecting code calculated from remaining bits of the frame, excluding the flags.
  - Code is 16 bit CRC-CCITT

HDLC Operation

- Three phases
- Initialization
  - Options to be used are agreed upon
    - Modes, sequence numbers,
- Data Transfer
  - Both sides may send data in I-frames
  - S-frames are used for flow control and error control
- Disconnect
  - Due to fault or on request of upper layer

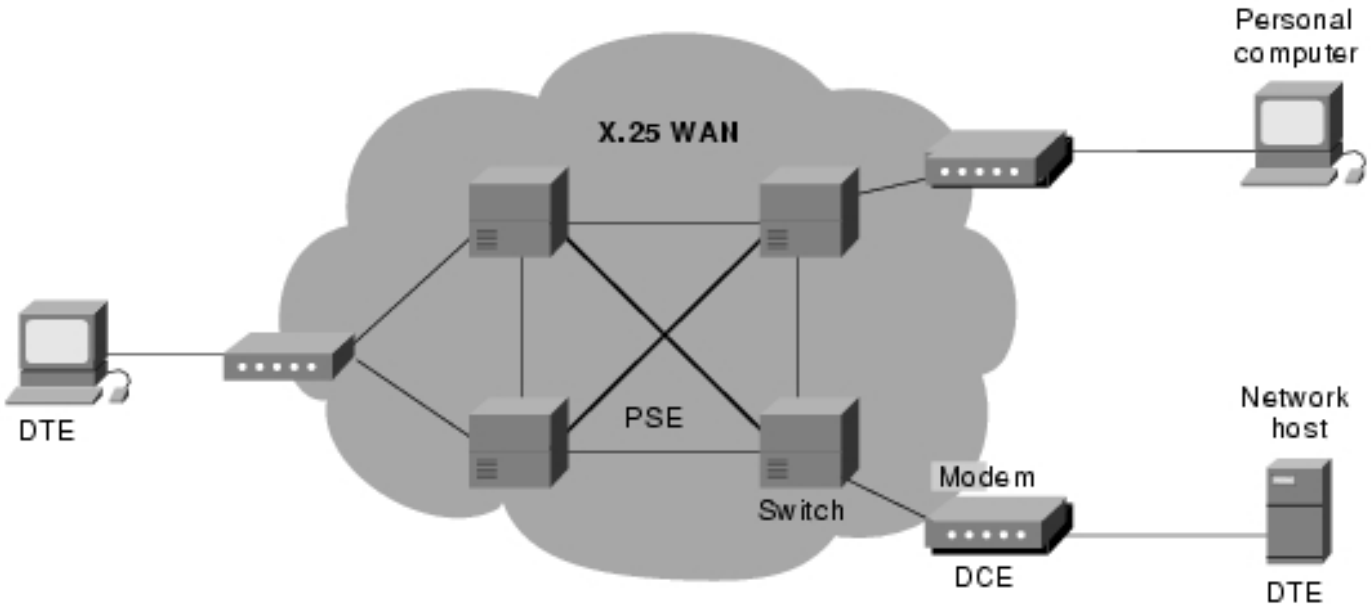
X.25

- *X.25* is an (ITU-T) protocol standard for WAN communications that defines how connections between user devices and network devices are established and maintained.
- Originally approved in 1976, went through numerous revisions.
- Standard specifies three levels: Physical,Data Link & Network, which corresponds to lowest three layers of OSI model

X.25

- Standard was made before OSI model was proposed
- Standard specifies three levels: Physical,Data Link & Network, which corresponds to lowest three layers of OSI model
- Physical
  - End systems are DTE (Data Terminal Equipment)
  - Switching nodes are DCE (Data Communication Equipment)
  - PSE (packet switching exchange)s are switches that compose the bulk of the carrier's network

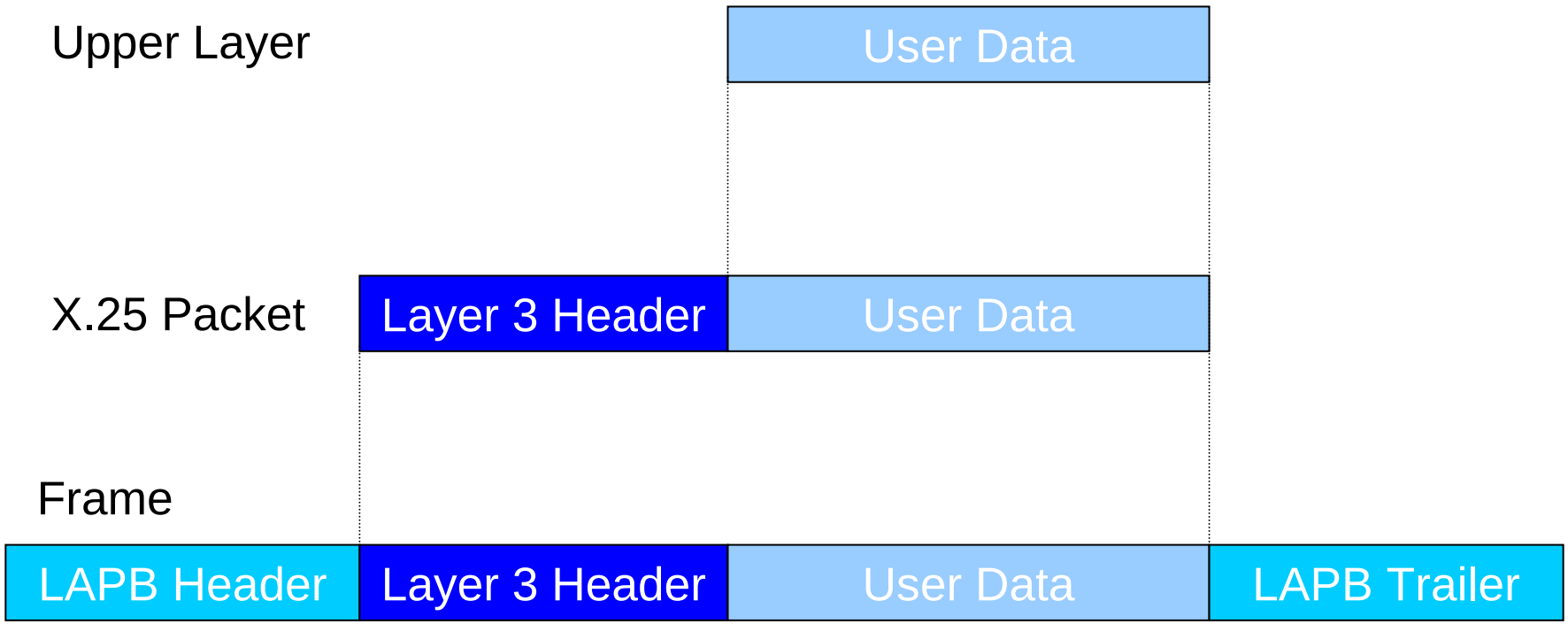
DTE, DSE & PSE



X.25

- Data Link
  - Reliable transfer of data as a sequence of frames
  - LAPB (Link Access Protocol Balanced), which is subset of HDLC is used
- Network Layer
  - Packet Layer Protocol (PLP)
  - Also called packet layer
  - Provides virtual circuit functionality
    - PVCs and SVCs
  - Multiplexing is supported. 4096 circuits can be established by one host

X.25 Protocol Control Information



Current Usage

- With the widespread introduction of "perfect" quality digital phone services and error correction in modems, the overhead of X.25 is no longer found to be worthwhile.
- X.25 networks are still in use throughout the world, although in dramatic decline,
  - largely supplanted by newer layer 2 technologies such as frame relay, ISDN, ATM, ADSL,
  - the ubiquitous layer 3 Internet Protocol.
- X.25 however remains one of the only available reliable links in many portions of the developing world, where access to a PDN may be the most reliable and low cost way to access the Internet

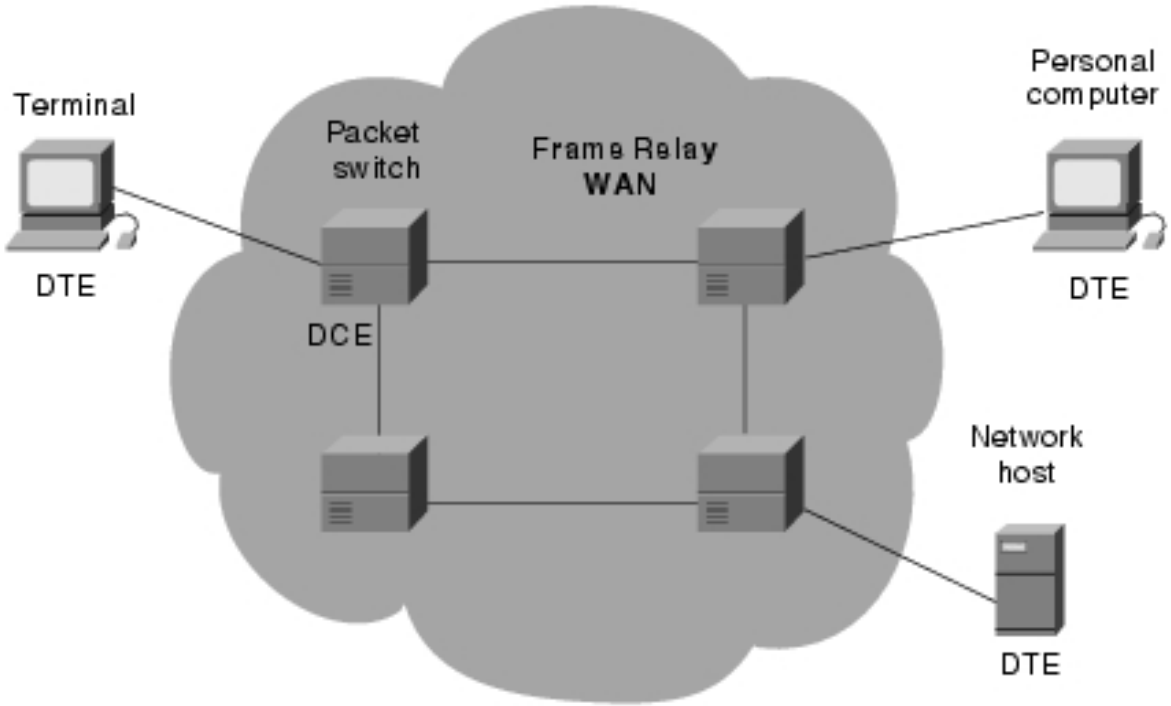
Frame Relay

- Provides fast switching of packets by reducing protocol overhead
- Evolved from X.25
  - Control and data packets use the same channel
  - Multiplexing of virtual circuits is done at layer 3
  - Both layer 3 and 2 have flow control and error control mechanisms
  - This results in considerable overhead
  - Each hop provides acknowledgement for data
  - At each intermediate node, state tables have to be maintained for flow and error control

Frame Relay

- As networks evolved they become more reliable
- Speed up is achieved by reducing overheads
  - Call control signaling is carried on separate logical connection
  - Multiplexing and switching of logical connection takes place at layer 2 (instead of layer 3)
  - There is no hop-by-hop flow and error controls. End-to-End flow and error controls are delegated to higher layers.

Frame Relay



Data Security

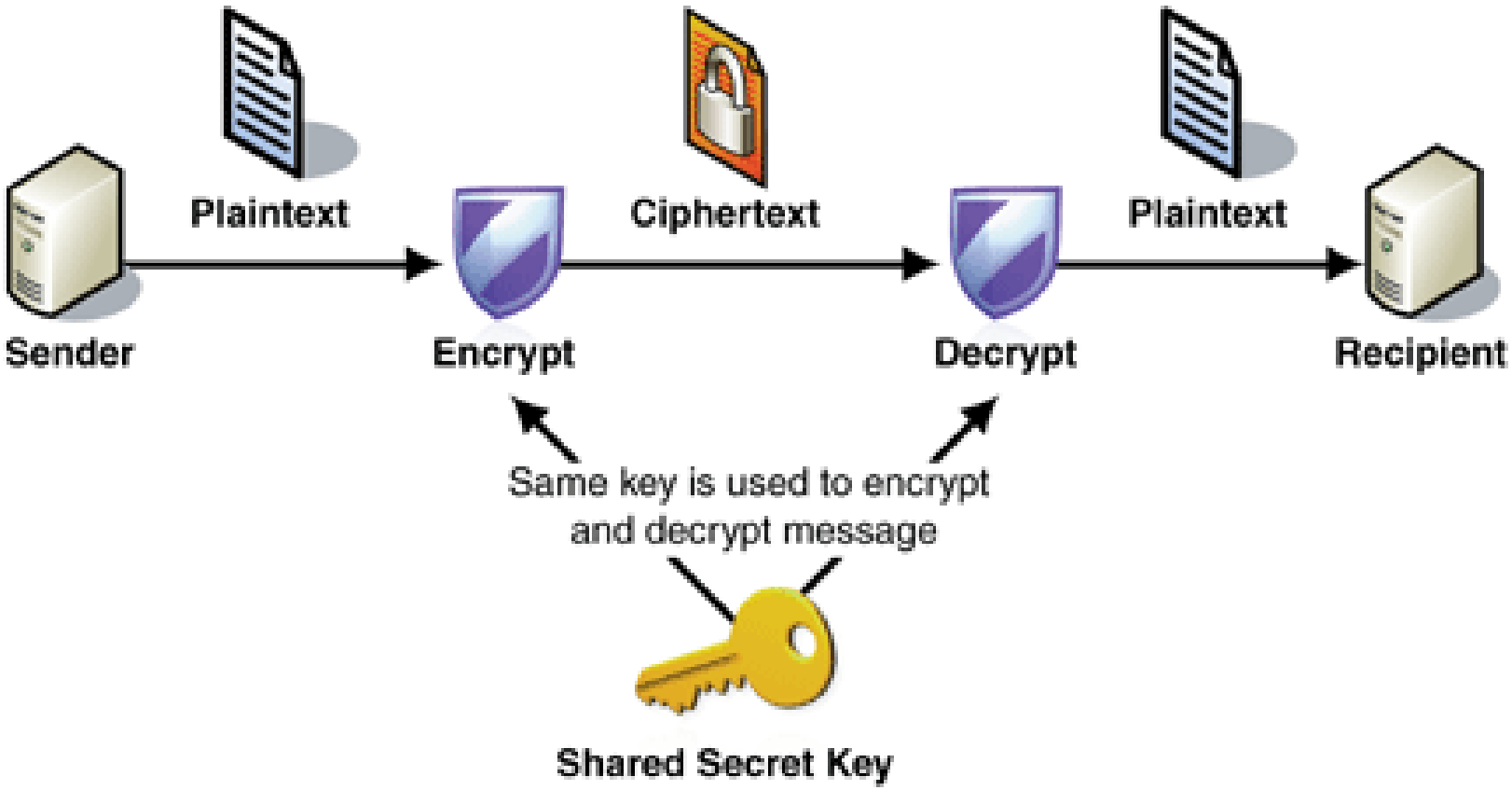
Network Security Requirements

- Confidentiality
  - data should be unavailable to the unauthorized
- Integrity
  - data should not be modified
- Authentication
  - assurance of identity of originator of data
- Non-repudiation
  - protect recipient from false denial by sender
- Entity Authentication
  - Verification of user prior to access to system

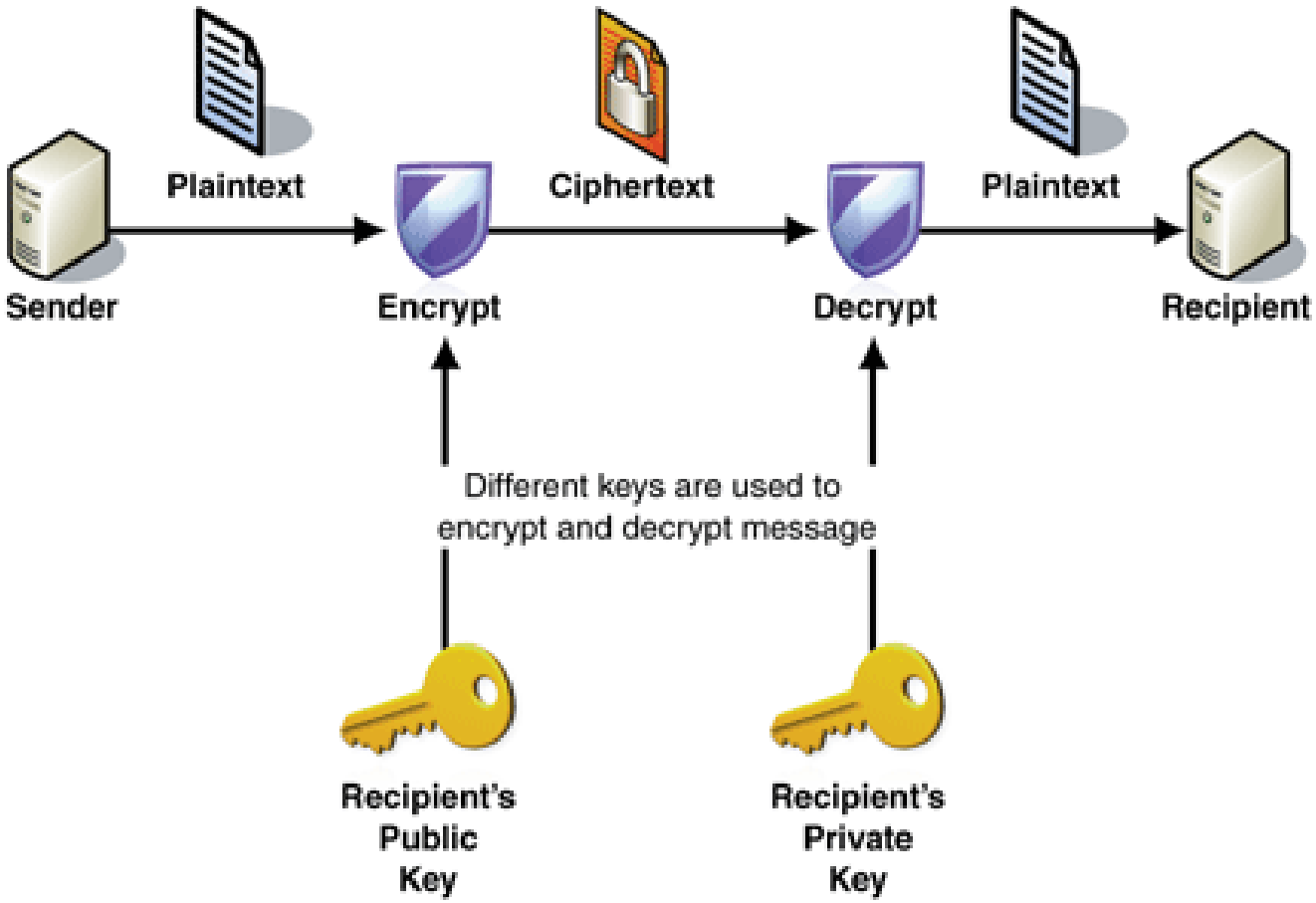
Cryptography

- A word with Greek origins meaning “secret writing”
- Technique of using secret code to disguise the message contents
- Very hard to mimic or reverse
- How is it done
  - Take Plain text
  - Encrypt it using a secret key
  - Send encrypted text
  - Decrypt it using the same/another secret key
  - Receiver gets the same plain text !

Symmetric Key Cryptography



Asymmetric Key Cryptography



Risks!

- Cryptanalysis
  - systematic breaking of encrypted messages
- Brute force cracking of keys

Key	Combination	time/test	Avg Search
3 digit lock	1,000	2sec	17 minutes
4 digit PIN	10,000	60sec	3.5 days
Passwd	.8 mill	50usec	34 minutes
N’pe crypt	1billion	50usec	10months

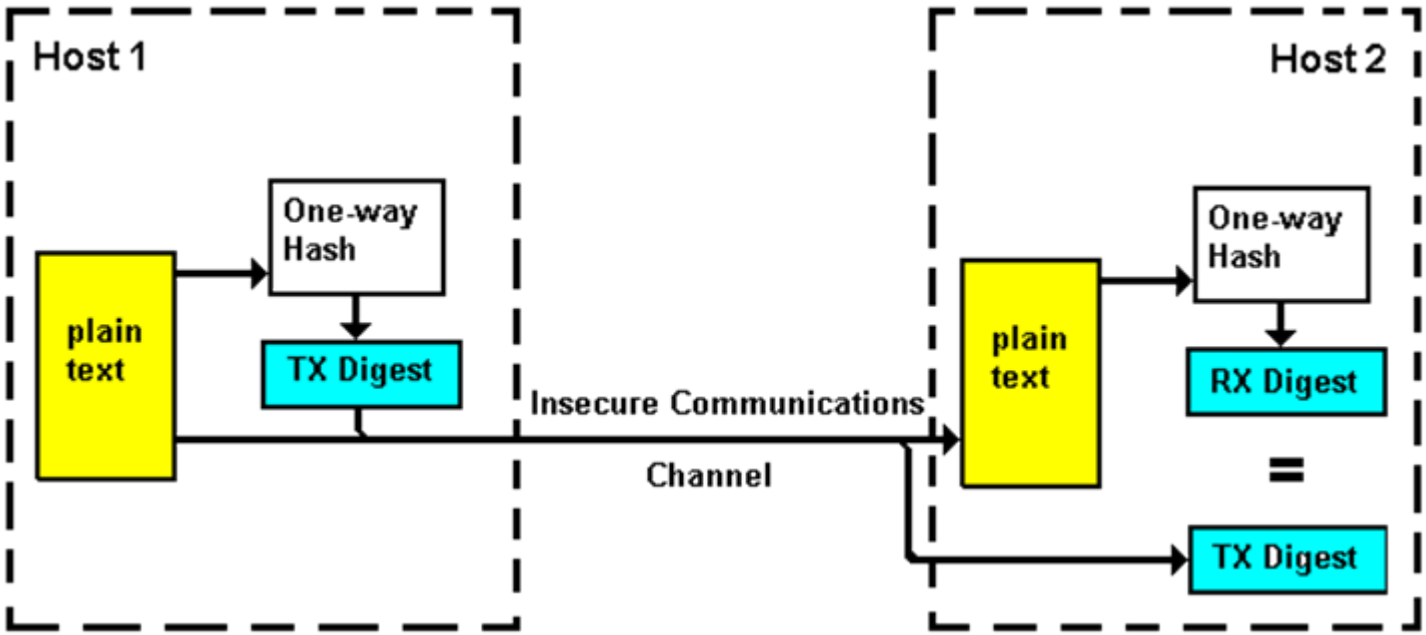
Confidentiality

- The transmitted message should make sense only to the intended receiver.
  - For others, it should look like garbage
- Achieved using
  - Symmetric key or
  - Asymmetric key cryptography

Integrity

- Data must arrive at the receiver exactly as it was sent
- Achieved using fingerprinting
  - Electronic equivalent is message digest
  - Generated using hash function
- The ideal hash function has four significant properties:
  - Easy computation of the hash value
  - Not possible to find a message that has a given hash,
  - Not possible to modify a message without hash being changed,
  - Not possible to find two different messages with the same hash.

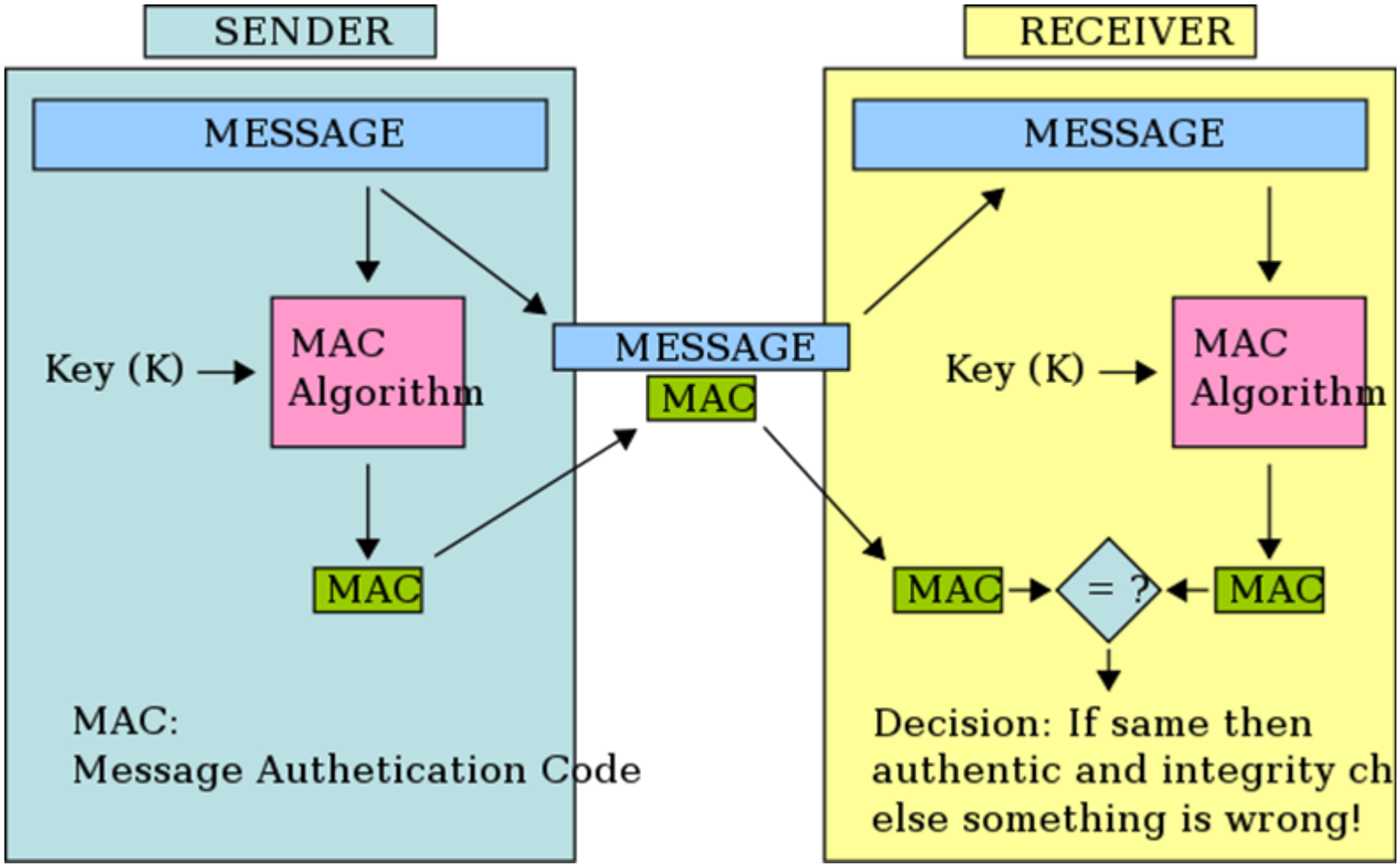
Message Digest



Authentication

- Receiver needs to be sure of sender's identity
- Achieved using MAC
  - Message Authentication Code also called a keyed (cryptographic) hash function
- Similar to hash function, but uses symmetric key while hashing

Authentication



Implementing Security

- Data link encryption
  - fully isolated connection between pair of computer
- IP link encryption
  - encryption between trusted hosts forming VPN
- WWW service with SSL
  - security at application layer

Data Link Encryption

- Works over point to point links
- Uses pair in-line encrypter device
- Simple to deploy
- Effectively decreases the speed of the link
- Scalability is not good

Internet Protocol (IP) Security Issues

- No guarantee that the received IP packets:
  - Are from the claimed sender
  - Contain the original data that the sender placed in them
  - Have not been inspected by a third party while in transit

IP security weakness and exploits

- Password Sniffing
- IP Snooping
- IP Hijacking
- SYN flooding (denial of service)

Password Sniffing

- Done by running a program on a server
  (eg. That of an Internet Service Provider)
- It collects about first 100 bytes of each connection
- Manages to intercept login names and passwords

IP Spoofing

- Making a vulnerable host feel that packets are coming from a trusted host
- Attacker exploits the misplaced trust
- Attacker gets into the server

IP Hijacking

- Active authenticated connection between two hosts is disrupted
- Attacker takes place of one host
- Attacker masquerades as host that was cut off
- Host does not now know that the commands are now coming from an attacker

SYN Flooding

- Attacker sends TCP “SYN” message to request a connection
- Never responds with final message to establish the connection
- Hosts waits with “half-open connection”
- More “SYN” are sent with forged addresses
- Available connections dry up faster than the host can recover
- Connections to legitimate users are denied

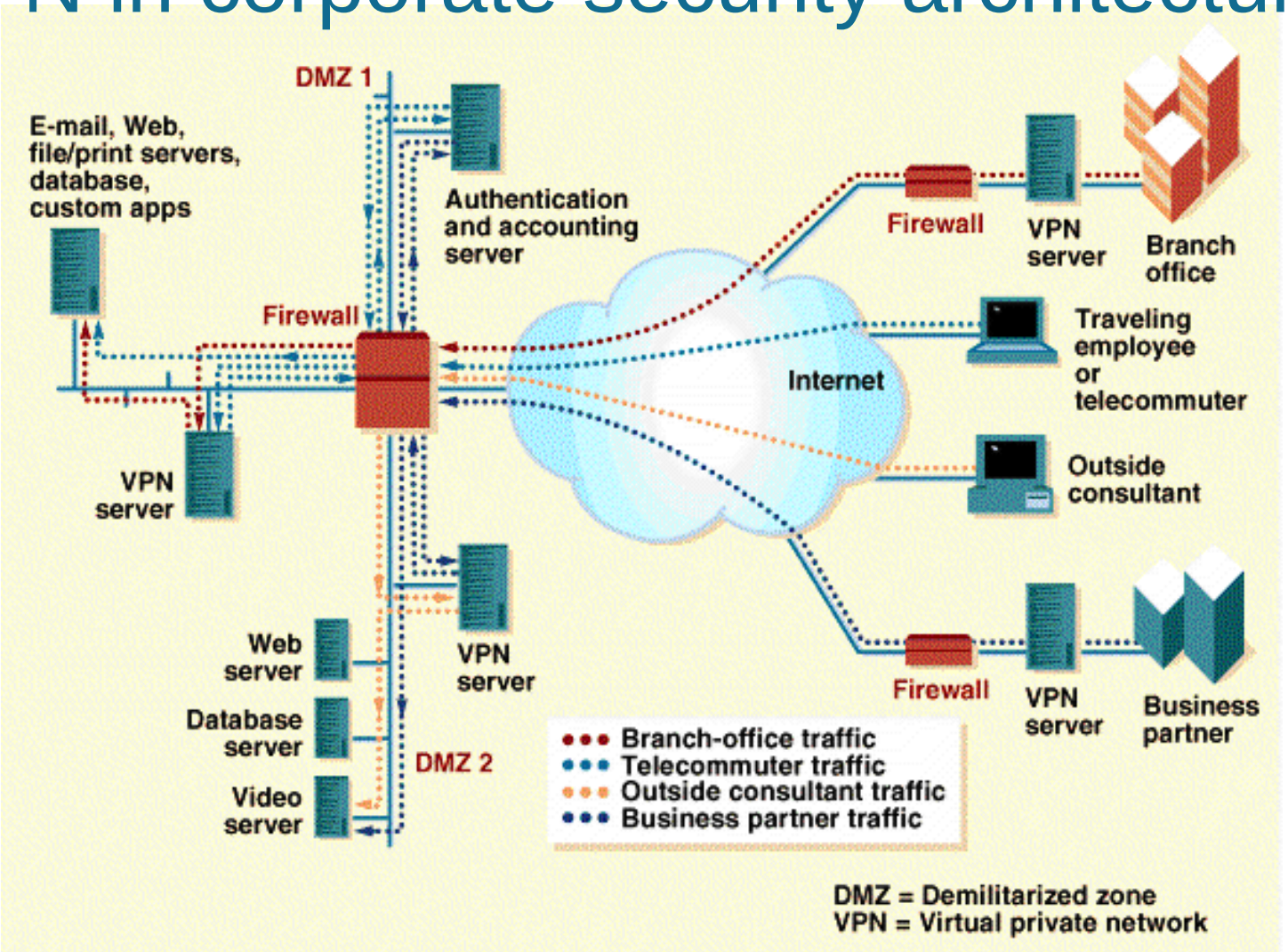
IP Link Encryption

- Uses IPSec protocol
- Transparent to internet software currently in use
- Carries encrypted data over untrusted network
- Cheaper to deploy
- Building block for VPNs

Virtual Private Network

- Private Network over public internet infrastructure
  - Privacy through tunneling and encryption
  - Restrict network access to trusted parties
- Reduces need for costly private networking equipment
- “Tunnels” establish connectivity between physical networks
  - Create one logical network out of multiple separated networks
  - Connect remote users to “home” network
  - No need for expensive long distance dial-ups
- Support multiple(incl. Non-IP) protocols over IP
- Security Risk: exposes network data/internal services to public

VPN in corporate security architecture



Firewalls

- Restrict unauthorised external network traffic from entering a controlled network
- Restrict internal network users from leaving a controlled network
- First line of network defense
  - Prevents attackers from getting close to other network defenses
- Types of Firewall filtering:
  - Static filtering based on IP-header field information
  - Dynamic filtering based on connection states(stateful inspection)
  - Content and application filtering
  - Proxy servers

Intrusion Detection Systems

- Designed to catch break-in attempts
- Give a real time view of what is transpiring in the network
- Maintain a database of possible attacks and keep sniffing network for a possible match
- Minimize the time between attack and detection
- Examples: Stalker, CMDS(Computer Misuse Detection System)

Some Famous Hackings

- 1973 Employee of NYT Savings Bank defrauds employer of $1M by computer
- 1982 Kevin Mitnick(18) breaks into US Air Force's supreme command Computer
- 1987 IBM Christmas Card worm virus infects IBM mainframes worldwide
- 1988 Student Robert Morris lets an experimental virus affecting 6000 servers
- 1995 Vladmir Levin manages to siphon off $7M from Citibank, New York

Thank You