7010INT Data Communications Lecture 2

Basic Concepts
Introduction to Networking Models

Dr. Ruben Gonzalez
School of Information Technology

Lecture Outline

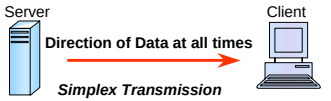
- Reference: Forouzan chapters 1, and 2.
- Types of networks: LANs – WANs - MANs
- Switching – directing traffic.
- Network Models (OSI and TCP/IP or 'Internet Model') – why we need them.

Network Connections

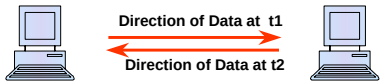
- Network devices can be connected to each other
  - *Via a cable (wired)*
  - *Over the air (wireless)*
- How many devices are connected together defines the type of network configuration. Two possibilities:
  - *Point-to-point*
  - *Multipoint* (broadcast)
- Network devices can talk to each other in different ways called Transmission Modes

Transmission Modes

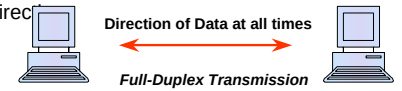
- Refers to the direction of transmission between two connected devices. Three possibilities exist:
- *Simplex*
  - One way communication only



- *Half-Duplex*
  - One way at a time

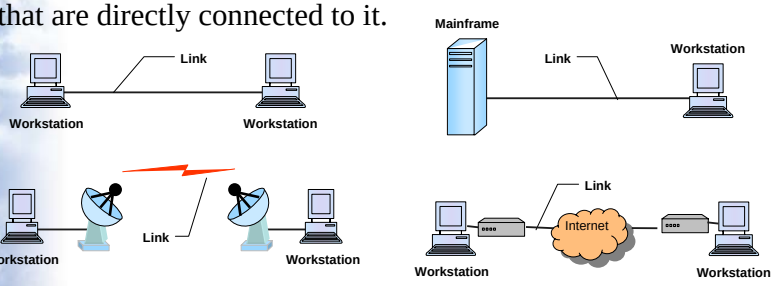


- *Full-Duplex*
  - Communication in both direc simultaneously.

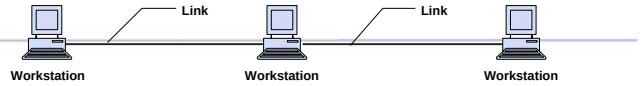


Point-to-Point Configuration

Point-to-point connections provides a dedicated link between two devices. Each device can communicate only with those that are directly connected to it.

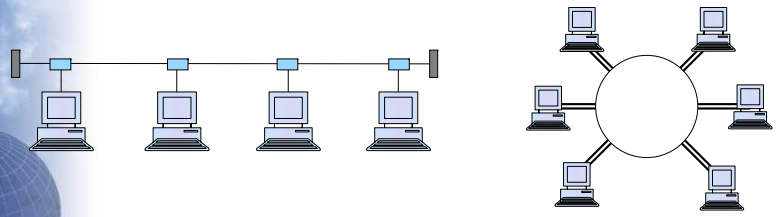


To communicate with other computers not directly connected they must do so via intermediate nodes (like the children's whispering game)



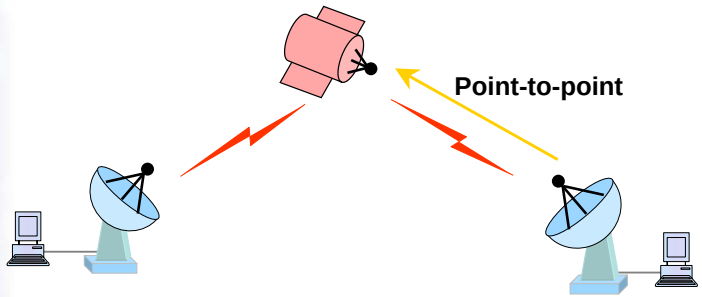
Multipoint Configuration

- In multipoint networks many devices share a single link or communication medium
- When a message is sent every device on the network "hears" it but only the intended recipient "listens" to it
- Because all nodes are attached to the same media, all must either "fight" for their turn to speak (*contention*) or wait to be granted a turn *(token passing* or *controlled access*).



Special Case: Satellite Networks

- Node to satellite: point to point
- Satellite to node: broadcast



Switched Networks

- In a large network (eg worldwide) we need to allow connection between any two arbitrary nodes, but we can't use multipoint configuration with large numbers of nodes
- The solution is to connect individual devices and multipoint networks using intermediate devices called switches or multipoint routers.
- Communication between any two nodes can involve passing through several switches
- Two main types of switching
  - circuit switching
  - packet switching

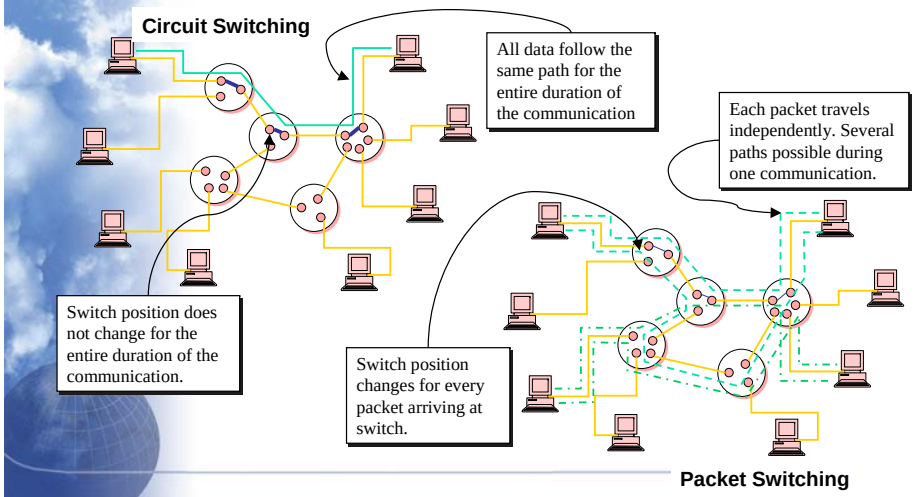
Circuit Switching

- Permits any two network devices can talk together at any one time – like telephones
- Creates a dedicated physical point-to-point connection to exist between the devices for the duration of the communication
- Data travels in a continuous stream of bits
- Advantages:
  - Secure, most suitable for continuous (streaming or real-time) data
- Disadvantages
  - Inefficient for typical (non audio-video) data

Packet Switching

- Any device can simultaneously connect to any number of other devices in the network
- Data is broken up into ***packets*** before transmission
- No dedicated physical connection is created during the transmission
  - Each packet can take a different path to reach its destination
  - Each link is shared by packets from all other devices
- Advantage:
  - More efficient for typical computer data communications
- Disadvantage:
  - Harder to secure, less suitable for continuous data

Circuit vs Packet Switching

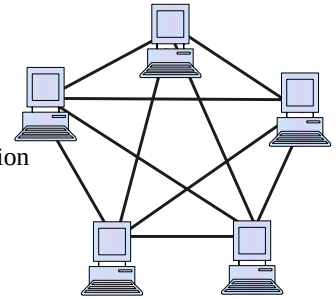


Network Topology

- The *topology* of a network is the way in which it is laid out either physically or logically.
- Five basic types of wired networks:
  - Mesh
  - Star
  - Tree
  - Bus
  - Ring
- Four basic types of wireless networks
  - Fixed Wire Replacement
  - Point-to-Point
  - Mobile-to-fixed network
  - Mobile-to-mobile networks

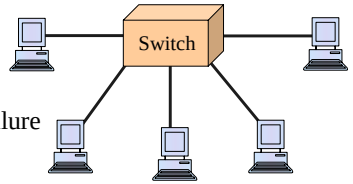
Mesh Networks

- Each device has a point-to-point link to every other device.
- A fully connected mesh network with n devices has $\frac{n(n-1)}{2}$ links.
- Each network device must have (n – 1) I/O ports
- Advantages:
  - No traffic problems
  - Robust
  - Privacy & security
  - Simple fault identification and isolation
- Disadvantages:
  - Wiring bulk
  - Hard to manage & Inflexible
  - Expensive to set up



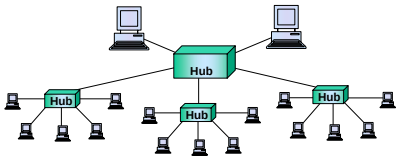
Star Networks

- Each device has a dedicated point-to-point link to a central controller or *hub* *(* called a LAN switch but not the same as a LAN hub)*.
- The hub controls all traffic by switching individual devices in or out.
- Advantages:
  - Cheaper than mesh
  - Flexible
  - Robust to single node or link failure
- Disadvantages:
  - Hub failure disables entire network
  - More cabling used than for some other topologies



Tree Networks

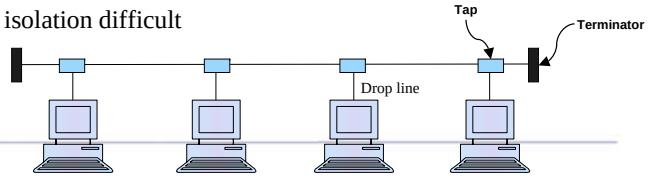
- Also use point-to-point connections but don't rely on a centralised controller but rather a network of switches.
  - If a switch can not resolve a destination then the message is transferred up to the next highest switch.
  - If the destination can be resolved the message is moved down the appropriate branch, to the next level switch, until the destination is reached.



- Advantages (as for star plus):
  - Larger networks can be built (more nodes over larger distances)
  - Can isolate/group together sections of the network
- Disadvantages (few)

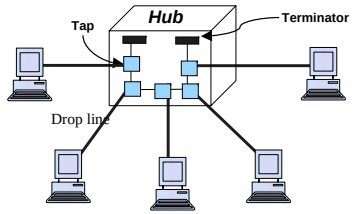
Bus Networks

- Multipoint configuration: all devices connected to a single ***backbone*** cable, there is no central controller. Instead, each node has equal access to broadcast data onto a shared channel
- Advantages:
  - Failure of any one device does not shut network down
  - Relative ease of installation & modification
  - Less cabling required
- Disadvantages:
  - Limited backbone length, number & distance between taps
  - Backbone failure causes complete network failure
  - Fault isolation difficult



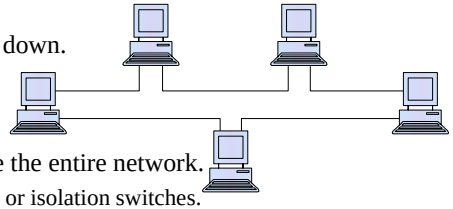
Hub Networks

- These are a variation of the bus topology, but it looks like a star because the wiring is collapsed into a central unit
- Hubs can also be connected in a hierarchical way to form a tree topology. The combined topology acts like a single bus network or an interconnected set of bus networks
- Advantages:
  - Same as bus network
  - Hubs are cheap
- Disadvantages:
  - Same as bus network
  - Hubs are slow



Ring Networks

- Each node has a dedicated point-to-point connection to only two other nodes (one either side).
- Eliminate switching altogether by routing all traffic in a circle from device to device.
- The cable is connected to form a closed loop
- Signals are passed from one node to the next in one direction.
- Advantages:
  - Fast, no hubs to slow things down.
- Disadvantages:
  - Break in the ring can disable the entire network.
    - Solution: use a double ring or isolation switches.



Token Ring?

Dear Token Ring user,

Recent changes in the Token Ring market urge the necessity to migrate from Token Ring to Ethernet. No LAN vendor actively supports Token Ring equipment anymore and the last two months, Token Ring interface cards are almost doubled in price and the delivery terms even tripled !!

It is clear that all the LAN-equipment manufacturers shifted their efforts to Ethernet and that you can no longer expect any investment and thus new development in the Token Ring technology. Staying with Token Ring becomes a serious business risk !!

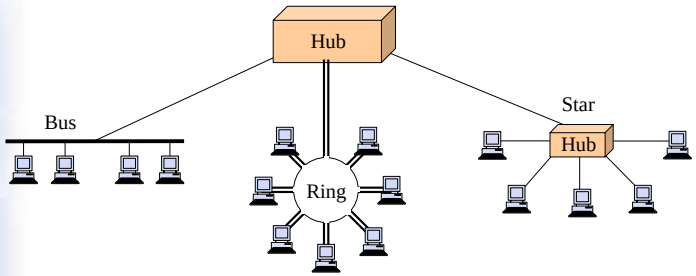
…

Yours truly,

Erwin Dirckx
Managing Director COMMswitch NV

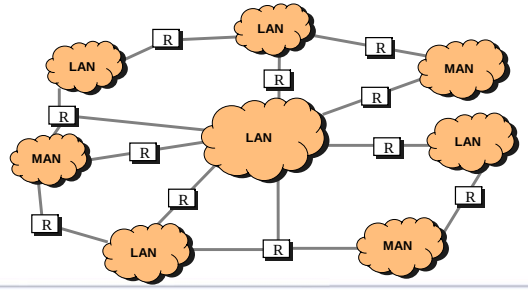
Hybrid Topologies

- Larger networks often combine several topologies connected via a central hub or backbone.



Internetworks

- Networks of networks.
- Connection via *internetworking* devices (*Routers* & *Gateways*)
- Note distinction between an *internet* and the *Internet*.



Wireless Networks

- Fixed Wire Replacements
  - Used as an extension to existing LANs
  - Limited range such as a room or building
  - Wireless base station connected to LAN cable
- Point-to-Point
  - Often used as part of a LAN backbone
  - Normally a microwave link between two buildings
- Mobile-to-fixed network (Nomadic access)
  - Used for long-range wireless data communication
  - Free roaming - not confined to particular cells
- Mobile-to-mobile networks (Adhoc)
  - These are standalone peer-to-peer networks not connected to any other network and temporarily set up for immediate needs

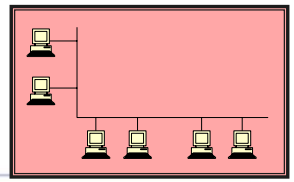
Categories of Networks

- Three categories of network:
  - *Local area network (LAN)*
  - *Metropolitan area network (MAN)*
  - *Wide area network (WAN)*
- The categories are distinguished by:
  - Dimensions (physical separation & number of nodes)
  - Ownership
  - Physical architecture.

Local Area Networks (LANs)

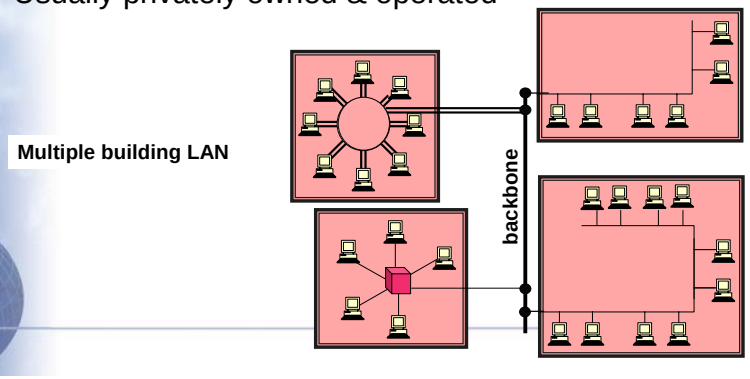
- LANs mainly designed for computers to share resources such as printers, fileservers etc.
- Links up to 100's of devices in a single office, or building.
- A LAN will generally use only a single type of transmission medium.
- Most common LAN topologies: bus, ring & star.
- Data rates range from 10Mbps to 100Mbps.
- Usually privately owned & operated

Single building LAN



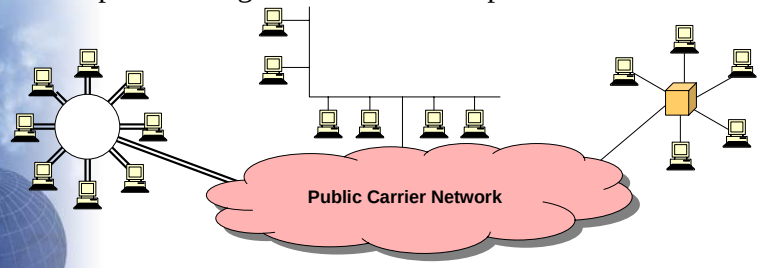
Backbone Networks

- A larger, central network connecting several LANs,
- Typically span up to several kilometers
- Typical data rates from 64 Kbps to 45 Mbps
- Usually privately owned & operated



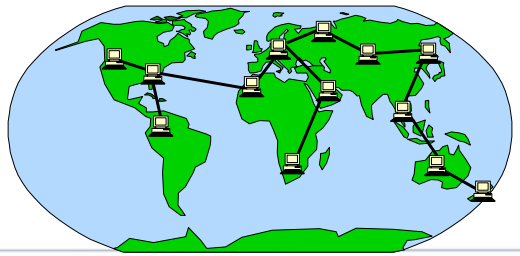
Metropolitan Area Network (MAN)

- Extend over an entire city (5 - 50 kms).
- Mainly used for interconnecting private LANs and BNs located in different areas to each others
- Supports data rates of 100 to 1000 Mbps.
- Normally owned and operated by someone else: an independent or government service provider.



Wide Area Network (WAN)

- Extends over a large geographical area (entire country, continent or globe)
- Makes use of public carrier transmission media such as
  - Leased lines
  - Public switched data network (PSDN) / ISDN
- WANs that are wholly operated by a single company sometimes referred to as an enterprise network
- Supports data rates of 28.8 Kbps to 2 Gbps.



Network Models

- During mid 70's proprietary networks were proliferating but they were largely incompatible with each other.
- A number of organisations developed a range of standard protocols to ensure network inter-operability.
  - ISO
  - ARPA
  - IEEE
- Since protocols have to define many different types of services for the network, these are broken down into layers.
- Each layer builds on the services of the layer underneath it, to provide more advanced functionality.

ISO & the OSI Reference Model

- ISO - the International Standards Organisation
- OSI – *Open Systems Interconnection* model.
- The OSI model developed in the 1978s & 1984s
- Consists of seven (7) distinct layers

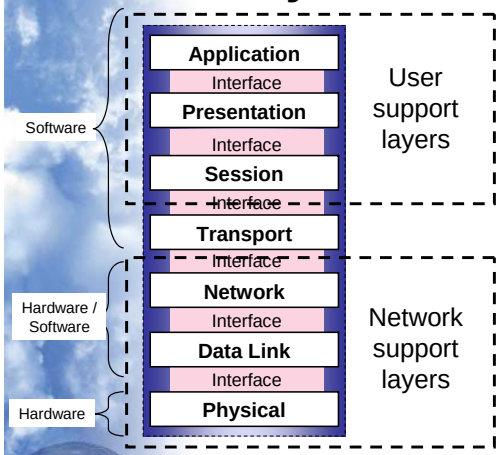
To help remember the layers and their order:

Application
Presentation
Session
Transport
Network
Data Link
Physical

Please Do Not Touch Steven's Pet Alligator

physical
DataLink
network
transport
session
presentation
application

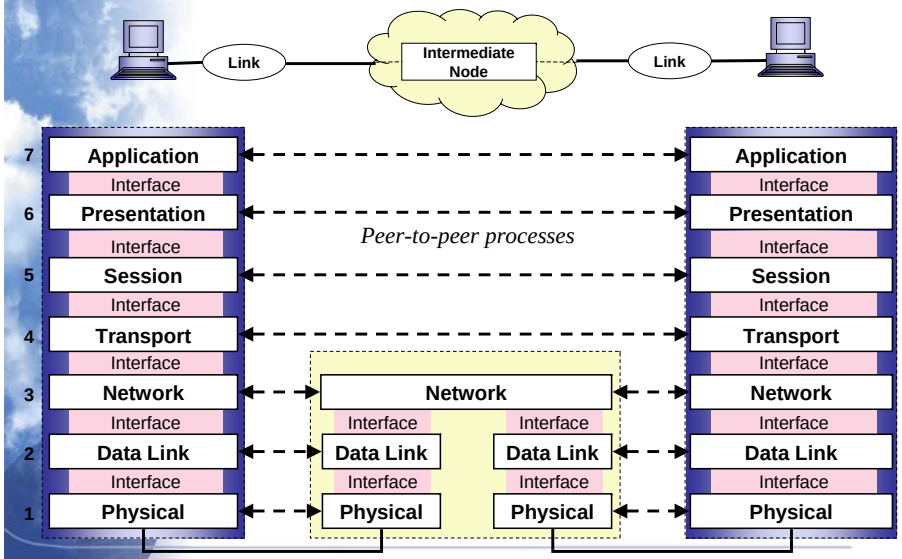
OSI Layers



- User support layers
  - Defines what messages are sent
- Transport layer
  - Ensures reliable end-to-end transmission
- Network support layers
  - Electrical specs
  - Physical connections
  - Addressing of packets
  - When to send packets
  - Error handling

- Layers communicated between each other via *interfaces*.

Communication Using the OSI Layers



The Physical Layer

The physical layer is responsible for ensuring that a stream of bits are transmitted between two nodes sharing a single link

- The physical layer coordinates all the functions required to transmit a *bit stream* over a *physical medium*.
- It defines:
  - Physical characteristics of interfaces/connectors and media.
  - Representation of bits: how raw data (0s & 1s) are *encoded* (transformed) into signals (electrical or optical).
  - Data rate: the number of bits transmitted per second.
  - Synchronisation of bits between sender & receiver.
  - Line configuration: multipoint or point-to-point.
  - Physical topology: mesh, star, tree, ring or bus.
  - Transmission mode: simplex, half-duplex or full-duplex.

Physical Layer Examples

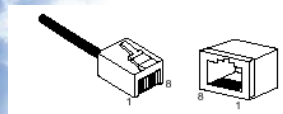
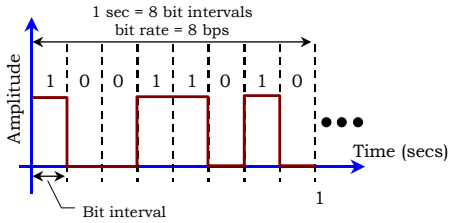


Figure A-1 Connector Pin Numbers

RJ45 Pin	Assignment*
1	Tx+
2	Tx-
3	Rx+
6	Rx-



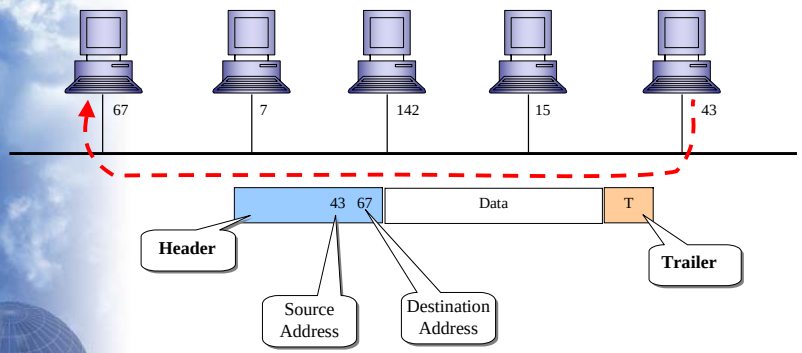
Picture Source: Fast Network User's Guide, Cabletron Systems, 1996

The Data Link Layer

The data link layer is responsible for ensuring that a packet of data is successfully transmitted between two adjacent nodes in the network

- The data link layer attempts to make the physical layer appear error free to the layers above it in the model as well as controlling *node-to-node* delivery.
- It defines:
  - ***Access control***: deciding when a device connected to the link can transmit at any given time (who gets to talk when).
  - ***Framing***: Identifies the start and end of each packet and which part of the packet is the address.
  - ***Addressing***: the address of the next node along the route to the intended final destination.
  - ***Error control***: mechanisms for detecting and recovering from transmission errors.
  - ***Flow control***: prevents the network or receiver from being swamped by controlling the release of data at the source.

Data Link Layer Example

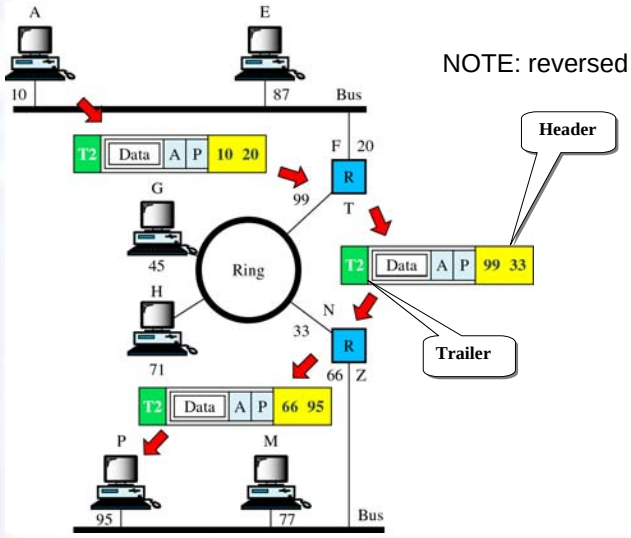


The Network Layer

The network layer is responsible for getting an individual packet of data from the source computer to the destination computer.

- The responsibilities of the network layer:
  - ***Logical addressing***: translates source and destination addresses in ones that can be understood across all connected networks.
  - ***Routing***: determining which path to take from source to destination (most important when there are multiple possible routes).

Network Layer Example



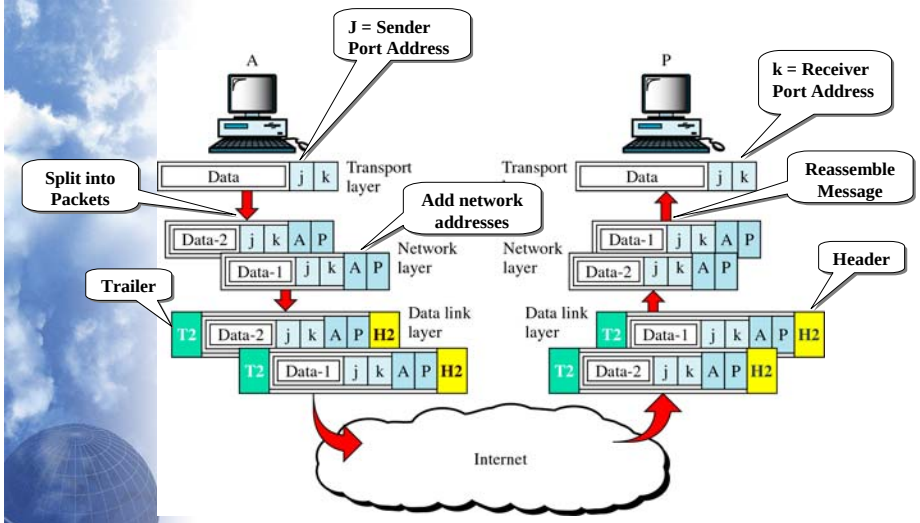
NOTE: reversed packets

The Transport Layer

The transport layer is responsible for getting the entire message from the source process to the destination process reliably.

- The transport layer manages *end-to-end* delivery between communicating software processes.
- Responsibilities of the transport layer include:
  - *Segmentation and reassembly* (*packetising*). Breaking up the message into *packets* of data at the source and reassembling them at the destination and numbering the packets.
  - *Service-point addressing*: ensuring that the message reaches the correct process (running program) at the destination by assigning *service point* (or *port*) addresses to the message.
  - *Flow control*: similar to data link layer except end-to-end.
  - *Error control*: similar to data link layer except entire message at the final destination not single packets.
  - *Connection control*: establishes end-to-end connections if required.

Transport Layer Example



The Session Layer

The session layer allows two communicating processes to co-ordinate the exchange of data.

- This establishes, maintains and synchronises the interaction between two communicating processes.
- Its responsibilities include:
  - *Dialog control*: Allows two systems to enter into a dialog defining whether communication is half-duplex or full-duplex.
  - *Synchronisation:* Allows a process to define synchronisation checkpoints in the message. This makes error/disaster recovery more efficient (eg can prevent having to resend an entire file when the link goes down).

The Presentation Layer

The presentation layer formats the data for interoperability, security and efficiency of transmission.

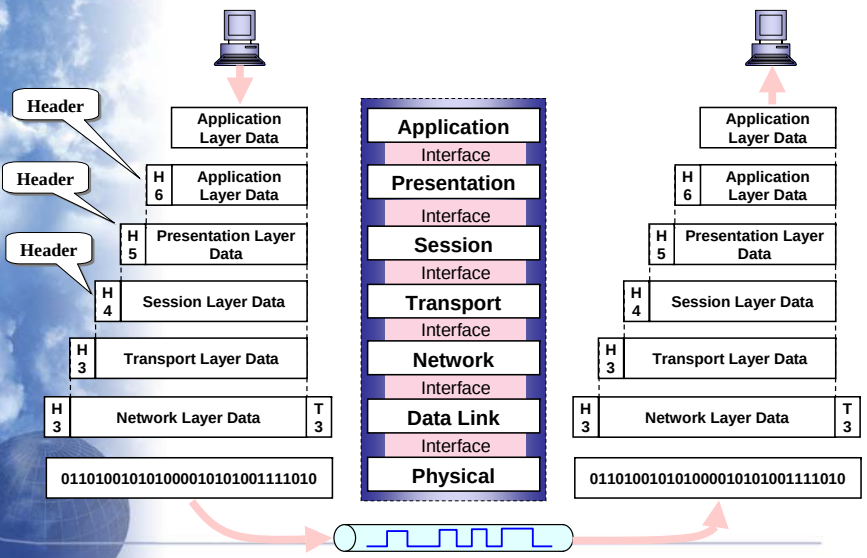
- This layer deals with the syntax and semantics of the information being exchanged between the communicating systems.
- It is responsible for:
  - ***Translation***: from machine specific character sets and data formats to generic character sets (egs unicode, ascii).
  - *Encryption*: for security purposes.
  - *Compression*: to minimise the amount of bits needing to be transmitted and so reduce delivery time.

The Application Layer

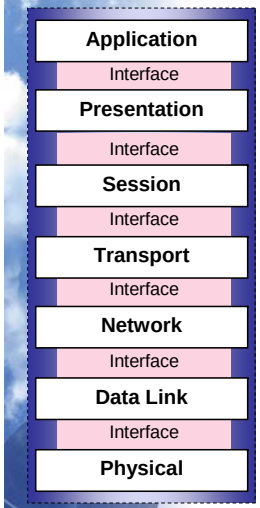
The application layer is the interface between the user and the network

- Allows the user (human or software) to access the network.
- Services provided by the application layer include but are not limited to the following:
  - *Network virtual terminal*: Remote software access to a physical terminal.
  - *Instant messaging* such as chat.
  - *File transfer, access and management (FTAM).* Allows a user to access, retrieve and manage file on a remote computer.
  - *Mail services:* control email exchange (X.400).
  - *Directory services*: distributed database sources and access to global information (X.500).

Communication Through Layers



Summary: OSI Model Layers

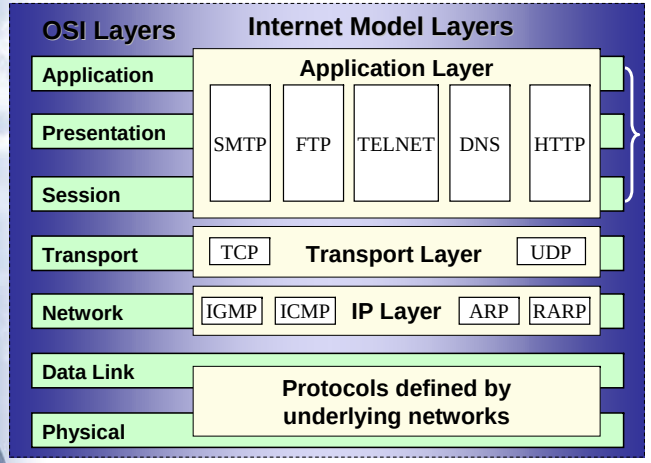


- Defines <u>what</u> message to send
- Defines the <u>format</u> of the message
- Defines <u>when</u> messages can be sent
- Sends entire message across network
- Sends a data packet across network
- Sends a data packet ⇔ connected devices
- Sends individual bits ⇔ connected devices

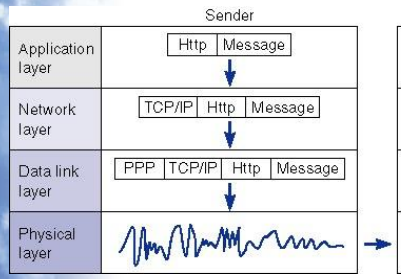
Internet Model: TCP/IP Protocol Suite

- History:
  - US DoD's *ARPA (Advanced Research Project Agency*) funded a project to investigate the possibility of creating a nuclear war proof network.
  - They connecting computers via a new technology called packet-switching and the resulting network grew to become what we now call the Internet.
  - A series of protocols were developed in conjunction with the Internet. The two most popular being *Transmission Control Protocol (TCP)* and *Internetworking Protocol (IP)*.

The TCP/IP Protocol Stack



Internet Model Layers



- Message
- Packet
- Datagram
- Frame + bits

TCP/IP vs OSI Models

OSI

- OSI is strictly a model with no implementation
- OSI is virtually unused today
- OSI is a copyrighted, de jure standard

TCP/IP

- TCP/IP is a protocol suite with an associated 'stack'
- TCP/IP is in widespread use
- TCP/IP is a de facto, free standard
- TCP/IP is the basis of the Internet

Because TCP/IP is older than OSI, the layers don't correspond exactly.

Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Logical Link Control
Physical	Medium Access Ctrl

Tutorial/Review Questions

- Chapter 1 – all review questions
- Chapter 2 – all review questions
- Also:
  - What are the two forms of switching discussed in this lecture?
  - Which form of switching uses the entire capacity of a dedicated link?
  - Which form of switching is the most appropriate for the following applications:
    - Voice conversation
    - Internet data transmission
    - Secure, fast data transmission
    - Video conferencing