Computer Networks

Topic 2:

Network Protocols and Standards

V1.0

Computer Networks

Topic 2 – Lecture 1:

Communications and Network Protocols

V1.0

Scope and Coverage

This topic will cover:

- Communications and network protocols
- Protocols and the OSI model
- Protocols in real-world networks
- The Internet

Learning Outcomes

By the end of this topic, students will be able to:

- Explain the purpose of network protocols
- Relate protocols to the OSI Reference model
- Describe the use of protocols in real-life networks
- Describe the protocols used by the Internet

Recap of Topic 1

The last topic examined:

- What a network is
- Real-world networks
- A layered architecture
- The OSI 7-layer model

Controlling a Conversation

The elements of a class discussion:

- What language is spoken?
- Whose turn it is to speak?
- Who should hear the message?
- Did all receivers get the message?
- Did all receivers get the message correctly?

Conversation Rules

- With friends, the rules are implicit.
- In more formal situations, rules may be given at the start.
- In a new situation, we may be unsure what the rules are.
- The rules depend upon the type of conversation we are having and the social context.
- Not following the rules will make a conversation difficult or impossible.

Network Conversation Rules

- The same rules apply in networks
  - Language
  - Turn to “speak”
  - Who the message is for
  - Confirming receipt
- But often the rules have to be exact, because machines cannot adapt to changes or variations from what is expected in the same way that humans can.

What is a Protocol?

- In terms of network communications, a ***protocol*** is an agreement between communicating parties on how a communication will take place.
- It is simply the rules of the conversation.
- It makes sense to have sets of rules agreed before any conversation takes place (***STANDARDS***).
- Different conversations can use different protocols.

Layers and Protocols

- We have already examined the OSI 7-layer model.
- The OSI model is a conceptual model – it does not tell us how the communication is carried out.
- Each layer has its own protocol.
- So, we have a ***protocol stack*** with protocols matching the layers of our model.
- Network communications use many protocols in one communication.

Protocol Types

- We can divide protocols into general types depending upon their purpose and how they are implemented:
  - Hardware protocols
  - Software protocols
  - Hardware-software interface

Hardware Protocols

- Define how hardware devices operate together
- Includes:
  - Voltage levels
  - Wires used
  - Pins on connectors
- Does not involve software but is controlled by electronic circuitry

Software Protocols

- Programs communicate with each other via software protocols.
- This includes the protocols required to talk to other devices and services.
- There are different protocols for different kinds of networks.

Hardware/Software Interface

- Software needs to access hardware, e.g. a message waiting in memory
- Software needs to know:
  - Where data resides
  - What order to access data in
  - What happens next

Some Common Protocols

- HTTP
- FTP
- IP
- TCP
- POP3
- SMTP
- IMAP

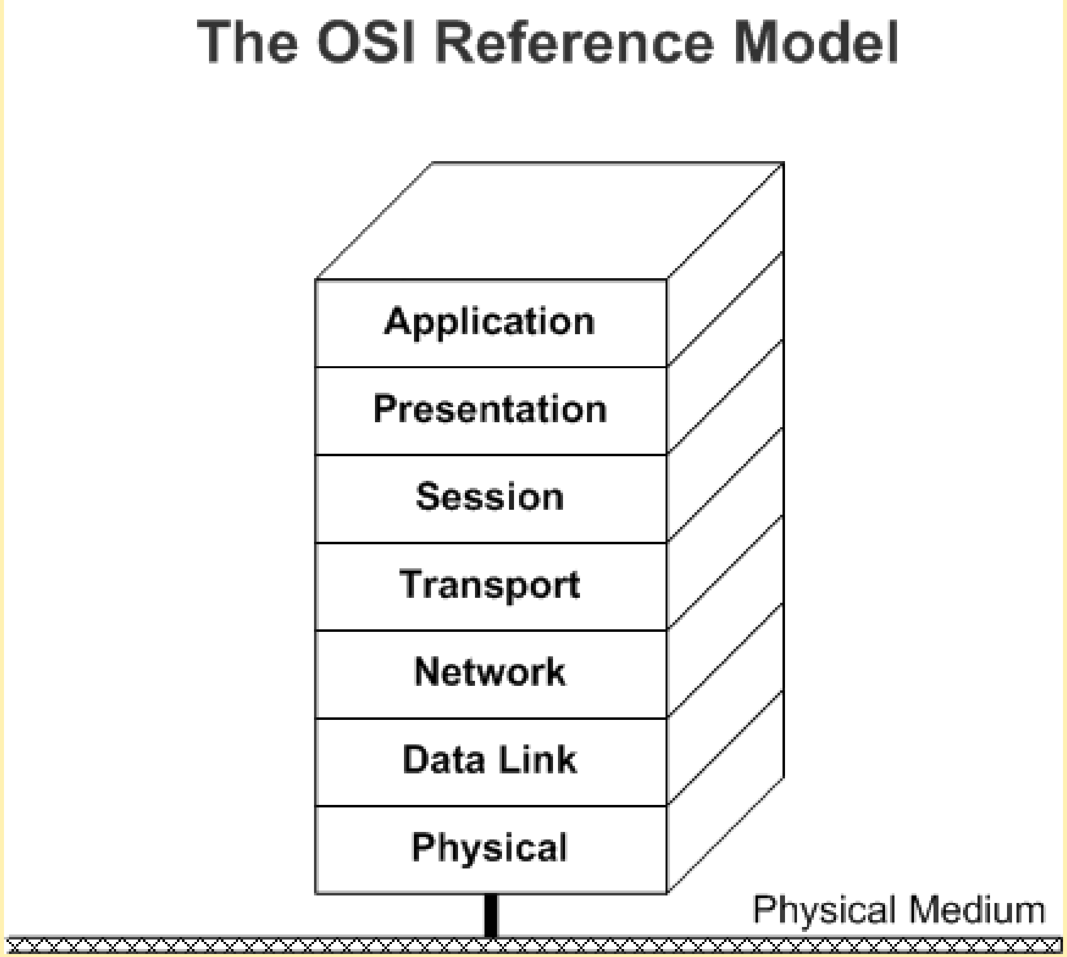
We will look at these in more detail later (after Private Study Exercise 1).

Computer Networks

Topic 2 – Lecture 2:

Protocols and the OSI Model

The OSI Seven Layer Model



Protocols and the OSI Model

- There is no single protocol that is specific to a single layer.
- The protocols are dependent upon:
  - The network type
  - The manufacturer of the hardware
- We will examine some of the common protocols that relate to specific layers of the OSI Model.

The Physical Layer

- Largely mechanical, electrical, timing issues
- The protocols associated with the physical layer are dependent upon the type of network.
- Many protocols that define communications in the physical layer are covered by the IEEE 802 series (but these overlap into the data link layer).
- Data type: bits
- Devices on this layer include the transmission media such as fibre optic cable, etc.

IEEE 802

- Standards for many kinds of ***Local Area Networks*** (LANs)
- Many have not survived with time, but there are a number of important standards, including:
  - 802.3, Ethernet
  - 802.11, Wireless LANs
  - 802.15, Personal area networks (Bluetooth)
  - 802.16, Broadband wireless

LANs

- A LAN is a privately owned network covering a small area such as:
  - An office
  - A building
  - A small geographical area (e.g. a campus)
- LANs are distinguished by:
  - Their geographical size
  - The transmission technology
  - Their topology (the layout of computer connections)

Physical Layer Standards

- The Physical Layer is controlled by electronic devices, so the standards relate to these, e.g.
  - RS232, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange
  - RS422, Electrical Characteristics of Balanced Voltage Digital Interface Circuits.

The Data Link Layer

- Responsible for communications between adjacent network nodes
- Divided into 2 sublayers:
  - ***The Media Access Control*** (MAC) sublayer
  - ***The Logical Link Control*** (LLC) sublayer
- Data type: frames
- Many protocols also covered by IEEE 802 series
- Devices: switch, bridge

The Data Link Sublayers

- The Media Access Control (MAC) sublayer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which allow multiple devices to be uniquely identified at the data link layer.
- The Logical Link Control (LCC) sublayer manages communications between devices over a single link of a network. LCC is defined in the IEEE 802.2 specification.

What is a Frame?

- Data packets are encapsulated into frames. A header with a hardware (MAC) destination and source address are added. A data frame includes:
  - Bit pattern indicating the start of a frame
  - Destination address
  - Source address
  - Data
  - Frame sequence check
  - Other elements that may be protocol specific

Data Link Layer Protocols

- Ethernet
- Token Ring
- FDDI
- IEEE 802.11 (WLAN, Wi-Fi)
- ATM
- PPP
- HDLC

The Network Layer

- Responsible for establishing paths for data transfer through the network (***routing***)
- Translates the logical address into the physical address, e.g. computer name into MAC address.
- Data type: packets
- Devices: router, frame relay device, ATM switch

Packets

- A ***packet*** is an independent, self-contained message sent over the network
- Includes:
  - A header
  - Addressing information
  - The data

Network Layer Protocols

- IP
- OSPF
- BGP
- NetBEUI
- DDP

The Transport Layer

- Responsible for delivering messages between networked hosts and the fragmentation and reassembly of messages
  - Acknowledgement of received segments
  - Retransmission of segments not acknowledged
  - Proper re-sequencing of segments
  - Flow control to manage the data so no data is lost
- Data type: segment
- Devices: bridge router (brouter), gateway

Transport Layer Protocols

- TCP
- UDP
- NetBEUI
- SPX
- ATP

The Session Layer - 1

- Responsible for establishing process-to-process communications between networked hosts
- Offers three communications modes
  - Simplex - Only one device transmits
  - Half-duplex - Each side takes turns transmitting from one side at a time
  - Full-duplex - Devices on both sides of the communications channel can talk at the same time

The Session Layer - 2

- Connection split into the following three phases:
  - Connection establishment
  - Data transfer
  - Connection termination
- Data type: session
- Devices: gateway

Session Layer Protocols

- ASP
- NetBIOS

The Presentation Layer

- Responsible for defining the syntax that two network hosts use to communicate
- Makes it possible for different systems with different data structures to communicate
- Provides a variety of encoding and encryption functions applied to application layer data
- Ensures that information sent from the application layer of one system will be readable by the application layer of another system

Encoding/Encryption Schemes

- Conversion of character representation formats – e.g. convert to ASCII characters
- Common data representation formats - standard image, sound, and video formats -

  e.g. ***JPEG***, ***MPEG***, and ***RealAudio***
- Common data compression schemes - e.g. ***WinZip*** or ***Gzip***

Presentation Layer Protocols

- AFP
- SMB
- NCP
- SSL
- MIME

The Application Layer

- Responsible for providing end-user services, such as file transfers, email, virtual terminal access, and network management
- The layer with which the user interacts
- This layer deals with application data

Application Layer Protocols

- DHCP
- FTP
- SMTP
- POP3
- IMAP
- HTTP

Research Topic

- You should research all of the protocols mentioned in this lecture to get an idea what they do.
- See Private Study, Exercise 4.

Computer Networks

Topic 2 – Lecture 3:

Protocols in Real-World Networks

Network Classifications

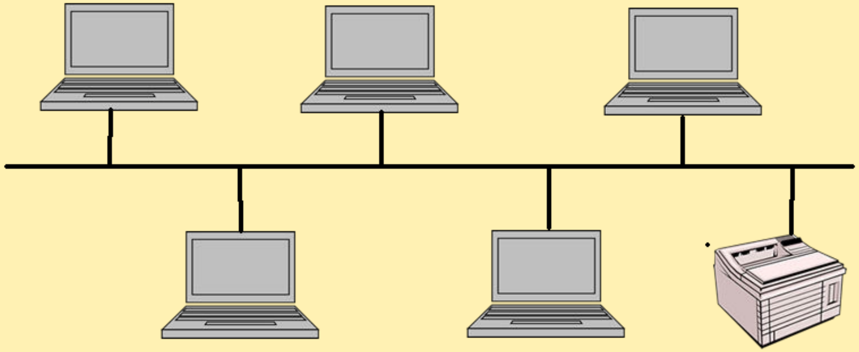
- Defined by the area covered
- ***Local Area Network*** (LAN)
  - A LAN is a privately owned network covering a small area
- ***Metropolitan Area Network*** (MAN)
  - Covers a town or city
- ***Wide Area Network*** (WAN)
  - A network that crosses regional, national and international boundaries

Networks

- Ethernet
- Fast Ethernet
- Token Ring
- Other LAN technologies
- Peer-to-Peer
- Client-Server

Ethernet

- Very common LAN standard
- ***Bus topology*** – all computers and peripherals are connected along a single cable segment
- IEEE 802.3



Broadcast Network

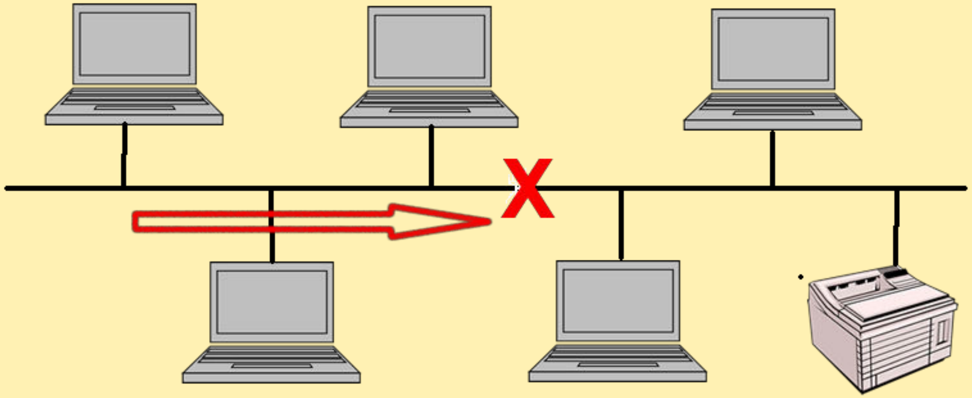
- When a node (computer) sends a message to another computer, it broadcasts the message to the entire network
- The other nodes listen and if the message is for them they keep the data, if not they ignore it
- Each node has an address
- Data is sent with the address to identify the recipient

Ethernet Issues

- Cable breaks
  - What happens if there is a break in the cable?
- Signal reflection
  - A message is an electrical signal. What happens when it reaches the end of the cable?
- Collisions
  - How does the network determine who has the right to send a message? What happens if two nodes send messages at the same time?

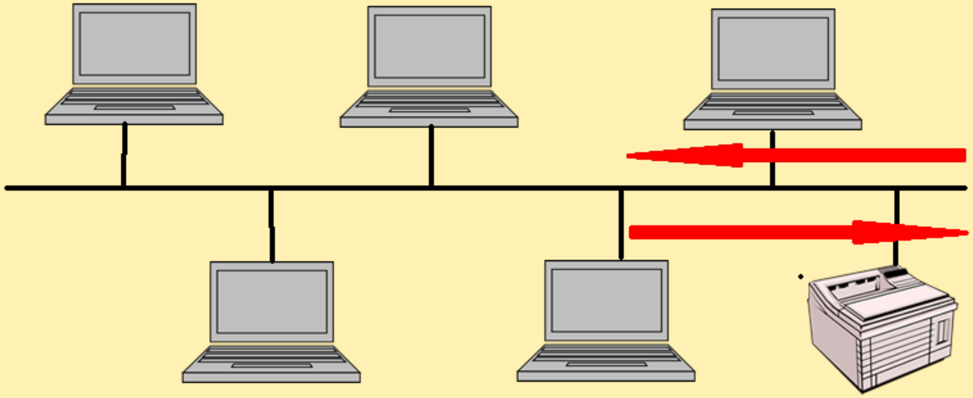
Cable Breaks

- There is a split in the network, so communication is impossible between the two sections.



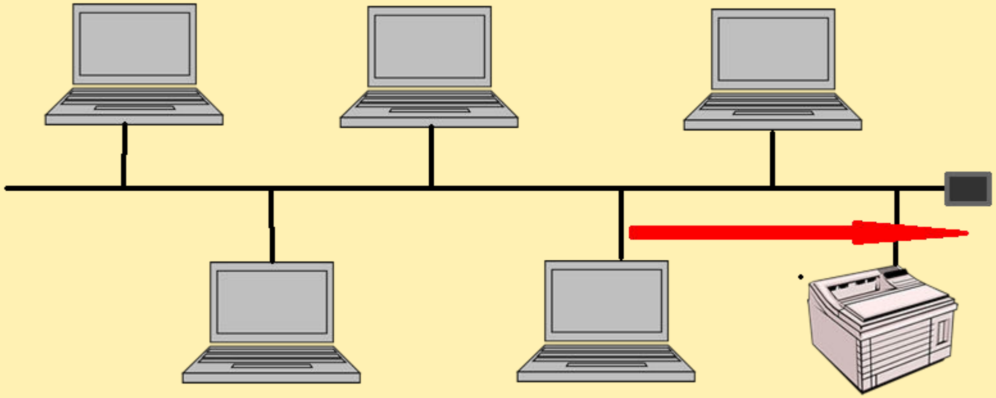
Signal Reflection

- The messages passed are simple electrical signals
- These will be reflected at cable ends and appear as a collision



Cable Termination

- Reflection is prevented by having the cable terminated with a resistor
- This dissipates the signal and prevents reflection



Collisions

- Before transmitting a signal, a node listens to the network and only transmits if there is no traffic.
- This does not prevent two nodes transmitting at the same time.
- If two or more nodes broadcast at the same time, there is a collision and the message cannot be received.
- A method is required for dealing with this.

CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- A simple protocol
- Any node can send a message when the network is free.
- If the cable is busy, it waits until it is free.
- Removes a lot of unnecessary waiting time by allowing transmission at any time.

CSMA/CD Collisions

- Two nodes may detect that the network is free at any one time and both transmit.
- The signals collide preventing either from being received.
- Energy levels on the line are increased and the collision is detected, nodes then:
  - Stop transmitting
  - Wait for a random back-off interval
  - Then attempt to retransmit

CSMA/CD Characteristics

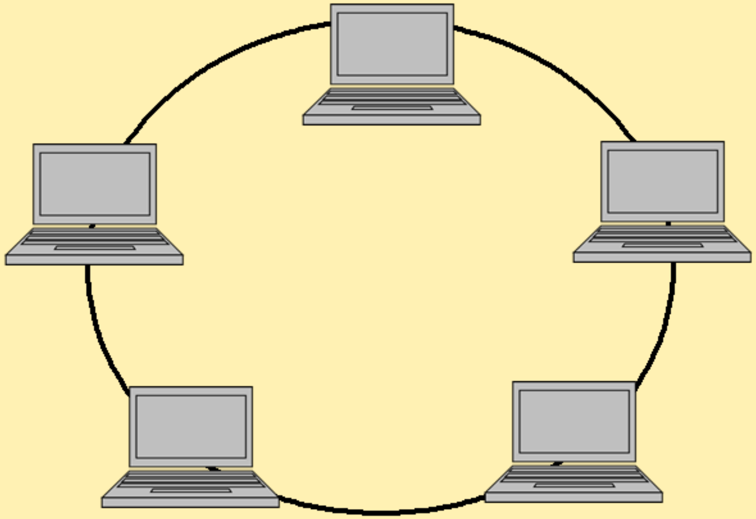
- No predetermined transmission order
- No guaranteed wait time before transmission
- Probability of collision increases as data rates increase - network saturates before theoretical limit
- Nodes transmitting at a high rate tend to take over the network

Fast Ethernet

- Ethernet originally ran at 5Mbps, then 10 Mbps
- This is too slow for many applications
- Fast Ethernet was introduced that ran CSMA/CD at speeds of 100Mbps
- This was followed by Gigabit Ethernet at speeds of 1000Mbps
- 100 Gigabit Ethernet is now a formal standard.
- It is suggested that Terabit Ethernet will be available by 2015

Token Ring

- All nodes are connected in a ring
- IEEE 802.5
- Now mainly present in legacy IBM systems



Token Passing

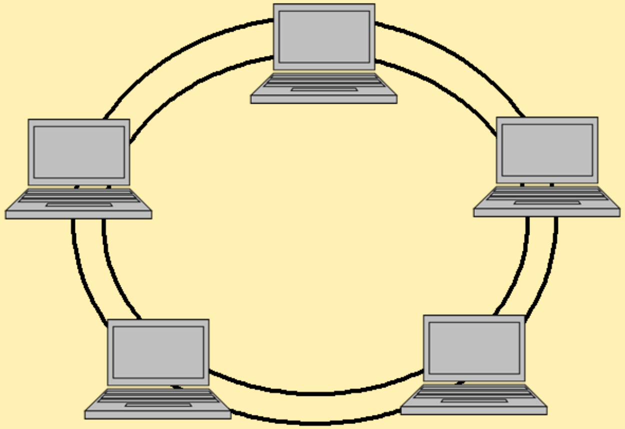
- A token is a special frame that circulates the ring, node by node.
- Only the node in possession of the token can transmit.
- Messages pass around the ring until they reach the destination node.
- The transmitting node then passes the token to the next node.
- Fairly distributes right to transmit

Problem

- Transmission is one way, a break in the ring stops transmission
- Modern rings are physically star shaped and operate through a hub that automatically removes damaged nodes thus “fixing” the ring

FDDI

- Fibre Distributed Data Interface
- Double ring transmitting in two directions, so transmission is possible if one ring is broken
- Now not a competitive technology

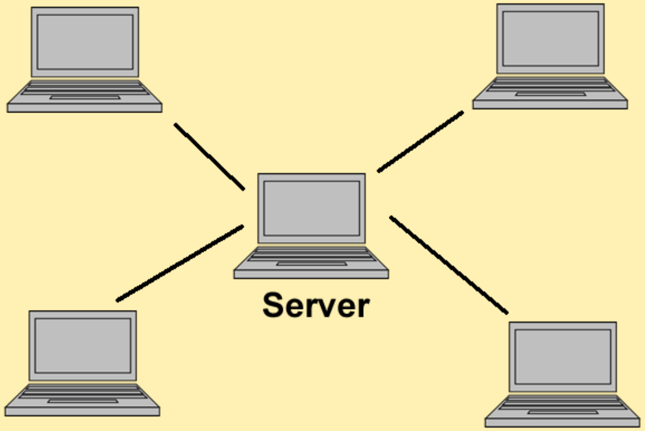


ATM

- Asynchronous Data Transfer Mode
- Intended as a replacement for telephony and data networks
- Uses a cell switching approach for high data rate transmission
- Has been widely used as a LAN backbone technology, despite requiring complicated interfaces
- Now overtaken by Gigabit Ethernet

Client-Server Networks

- Typically star-shaped networks
- Central server holds data and programs for client computers
- Clients (workstations) often have no hard drive



DHCP

- Client-server networks often allow for devices to be added and removed
- The Dynamic Host Configuration Protocol is often used to assign unique IP addresses to devices
- The address can be released when a device leaves the network
- This same address can then be allocated to another device when it joins

Peer-to-Peer (P2P) Networks

- Nodes generally have their own hard drive
- Nodes often have their own peripheral devices
- Control of a node is autonomous
- Resources are shared at the discretion of individual users
- Individual nodes can act as both clients and servers
- Gnutella is a common (P2P) protocol

Computer Networks

Topic 2 – Lecture 4:

The Internet

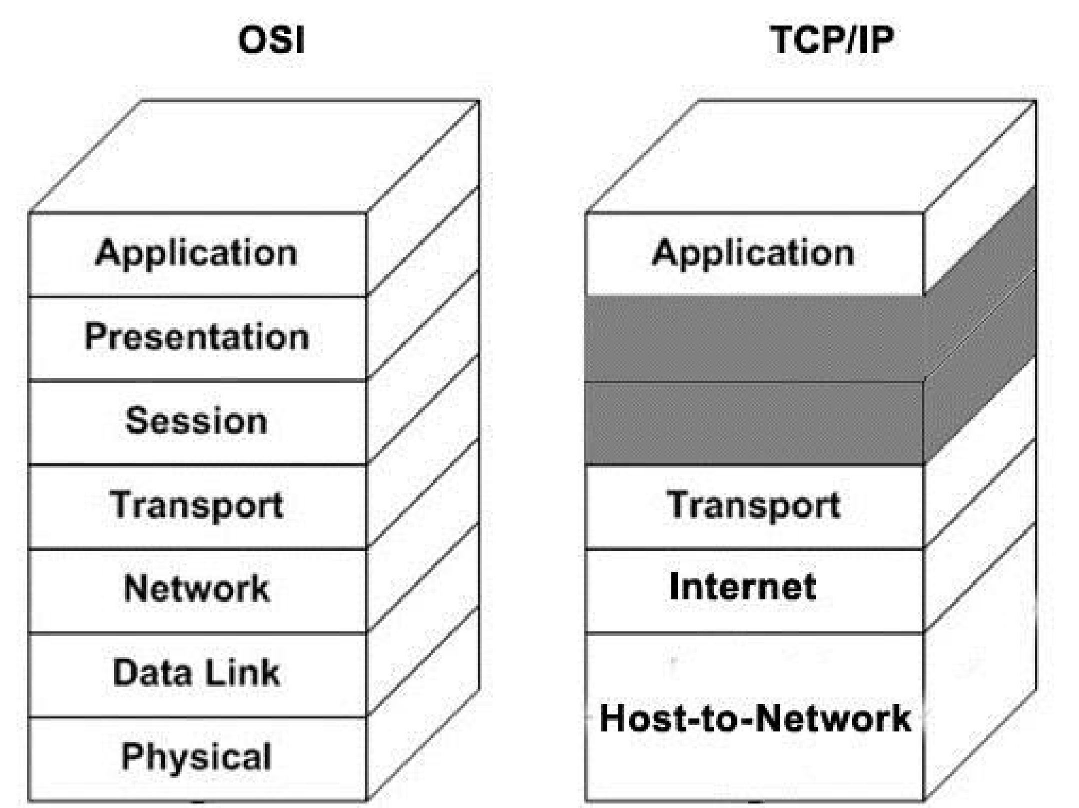
V1.0

What is the Internet?

- A collection of networks that use common protocols to provide common services.
  - Uses the TCP/IP reference model
  - Uses the TCP/IP protocol stack
- To be part of the Internet, a computer must also:
  - Have an IP address
  - Be able to send IP packets to other machines on the Internet

TCP/IP Reference Model

- Has 4 layers



Host-to-Network Layer

- Not specified in detail in the model
- The host has to connect to the network via some protocol
- The protocol must allow it to send IP packets

Internet Layer

- Permits hosts to inject packets into any network and travel independently to their destination
- Packets may be delivered in any order
- Role is to ensure packets get to the right address
- The Internet Protocol (IP) is responsible for this
- The **i**nternet layer is present in the Internet but not specific to the Internet
- Packet switching is the key function

Transport Layer

- Is designed to allow source and destination to have a conversation
- Uses one of two protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- Comparable to the OSI Transport Layer

Application Layer

- The TCP/IP model does not have session or presentation layers
- This layer consists of high level protocols such as:
  - File Transfer Protocol (FTP)
  - Simple Mail Transfer Protocol (SMTP)
  - HyperText Transfer Protocol (HTTP)

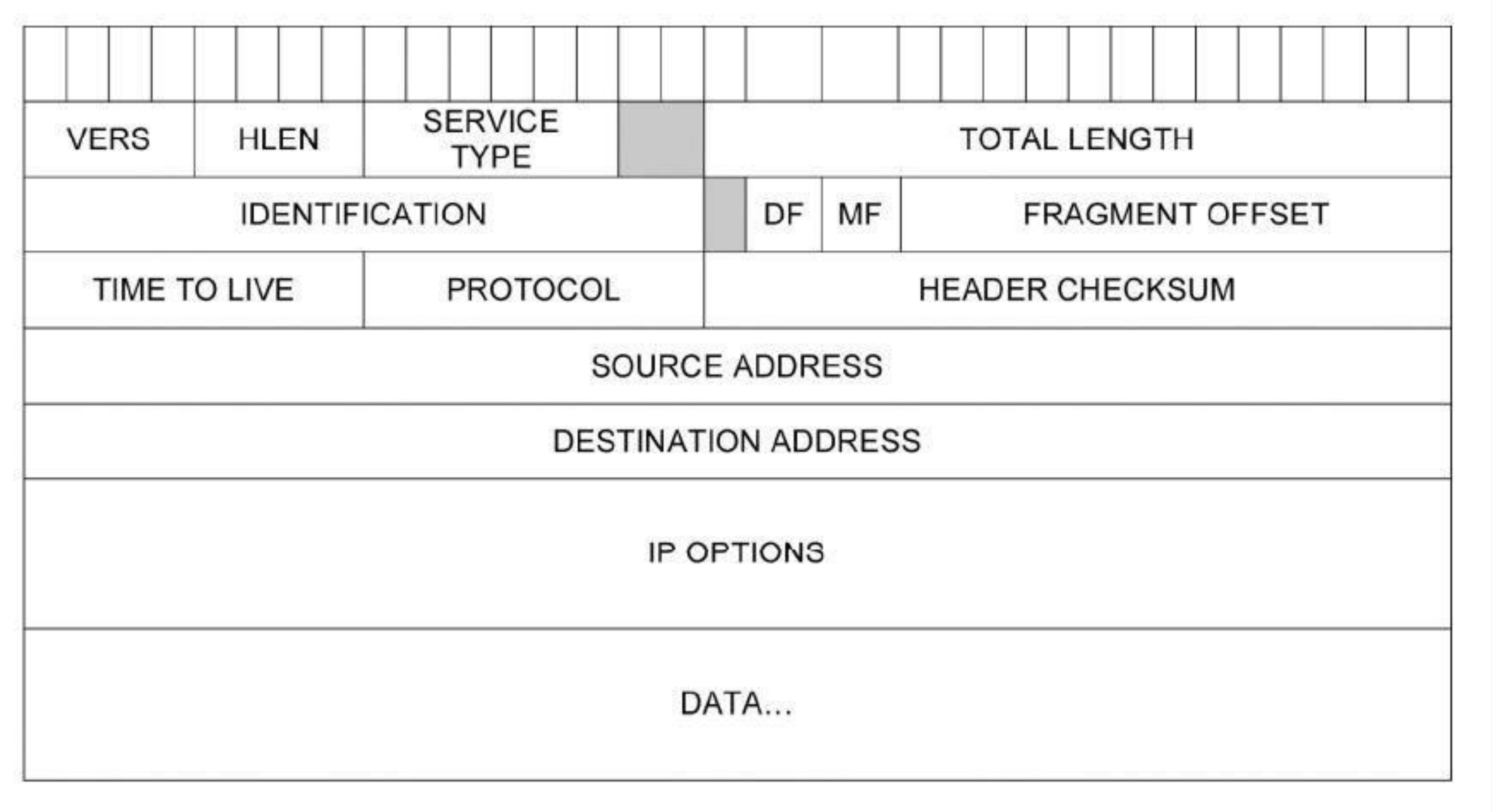
Internet Protocol

- Defines the rules that determine how packets are transferred from one host to another
- It is not a reliable protocol:
  - Packets may not be delivered
  - Packets may be delivered out of sequence
- Every host must have a unique IP address that identifies it.

IPv4 Addresses

- Internet Protocol version 4
- Each address is a dotted quad in the form 101.4.233.1
- Each address is made up of four decimal numbers between 0 and 255 separated by a dot
- Each address is 32 bits
- 2^{32}= 4 294 967 296 possible addresses

IP Datagram - 1



VERS | HLEN | SERVICE TYPE | ▨ | TOTAL LENGTH

IDENTIFICATION | ▨ | DF | MF | FRAGMENT OFFSET

TIME TO LIVE | PROTOCOL | HEADER CHECKSUM

SOURCE ADDRESS

DESTINATION ADDRESS

IP OPTIONS

DATA...

IP Datagram - 2

- The datagram is the packet sent around the network.
- Header information contains detail of where it came from, where it is going to and processing information.
- Data is the actual payload intended for the recipient.

Subnets

- A subnet is a logical subdivision of an IP network.
- Subnets are meaningless to any router outside the business.
- Internal routers can use this to route packets to the relevant subnetwork.
- By organising hosts into logical groups, subnetting can improve network security and performance.

Subnet Addressing

- The most significant part of the address is used to indicate which network is intended, e.g. 192.168.1.0.
- Devices on this subnet have addresses in the range 192.168.1.1 - 192.168.1.254.
- 192.168.1.255 cannot be assigned as it is reserved for broadcast.
- Multiple subnets can be used on one network.

Multiple Subnets

- A router could have the address 192.168.0.0.
- There could be a number of subnets within an address:
  - 192.168.1.0
  - 192.168.2.0
  - 192.168.3.0
  - Etc.

IPv6

- Problem with IPv4 - Not enough addresses
- Solution – a new version of IP
- IP version 6 addresses are made up of 128 bits.
- 2^{128}, or about 3.403×10^{38}, unique addresses
- Represented by 8 groups of 16-bit hexadecimal values separated by colons, e.g. 2001:0db8:85a3:0000:0000:8a2e:0170:4334
- Many applications do not yet support IPv6.

From IPv4 to IPv6

- Address increased from 32-bit to 128-bit
- Allows node to specify the message path
- Smaller header but addresses are longer
- Allows for more header options in the future
- Quality of service capabilities allow non-standard handling of packets
- Allow for the handling of authentication, confidentiality and data integrity

Transmission Control Protocol - 1

- Designed to provide reliable delivery for IP
- Takes care of breaking data into packets and reassembling at the destination host
- Checks if packet is corrupted and requests a resend if it is
- Checks number of packets and requests replacement if one is missing
- Handles timeouts and transmission errors

Transmission Control Protocol - 2

- A connection-oriented protocol - a connection is established and maintained until such time as the messages have been exchanged
- Establishes a full duplex virtual connection between two endpoints
- Each endpoint is defined by an IP address and a TCP port number
- Used with WWW, email and file transfer

User Datagram Protocol - 1

- A simple transmission model using headers of only 8 bytes
- Does not provide:
  - Reliability
  - Ordering
  - Data integrity
- Assumes error checking and correction is not necessary

User Datagram Protocol - 2

- Does not have the delays that can be associated with TCP
- Used with IP in time-sensitive applications:
  - Gaming
  - Voice over IP (VoIP)
  - DNS

File Transfer Protocol

- Uses TCP/IP to transmit/receive
- Works at the application layer
- Uses a generic file structure that is independent of the operating system
- Allows file transfer between dissimilar hosts

Simple Mail Transfer Protocol

- Uses TCP/IP to transmit
- Does not provide a user interface for sending and receiving messages
- Many Internet email applications do provide interfaces.
- Commonly used for sending email
- Most email clients use POP3 or IMAP for incoming mail.

Hypertext Transfer Protocol

- Used throughout the World Wide Web for sending messages and getting responses from servers
- Most common method is the GET method to request and receive a web page
- Other common methods are:
  - PUT
  - POST
  - DELETE
  - TRACE

References

- Price B. (ed) (2003). *Networking Complete,* 3rd edition. Sybex.
- Tanenbaum, A.S. & Weatherall, D.J. (2010). *Computer Networks,* 5th edition. Pearson Education.
- The IETF website: http://www.ietf.org

Topic 2 – Network Protocols and Standards

Any Questions?