CSIT985
Strategic Network Design

Spring 2023

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Lecture week 2:

Networking Fundamentals

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Presented by: Dr. Chau Nguyen

Lecturer, School of Computing and Information Technology, UOW

Outline

- ❑ Network Elements
- ❑ Network Categories
- ❑ Network Models
- ❑ Network Topology
- ❑ Network Addressing
- ❑ Network Performance
- ❑ Network Protocols

Network Elements

What is a network?

Two or more end devices connected to each other via wired or wireless connection form a computer network.

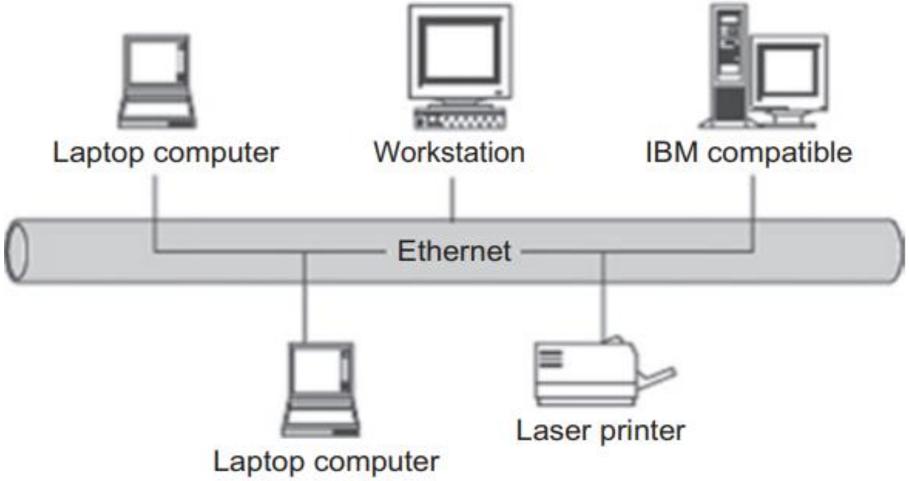


Figure. A Computer Network (Kizza, 2020, p.4)

Network elements: Hosts or End Devices

- On a network, each computer is called an end device or a host
- “An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device”

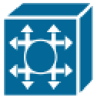
Network elements: Networking Devices

- Networking devices are intermediate devices in a computer network. They enable the communication and interaction between connected device within the network.
- Types of networking devices: hub, switch, router, bridge, gateway, modem, repeater, or access point

Workgroup switch

Small Hub

Router



Programmable Switch

Wireless Router

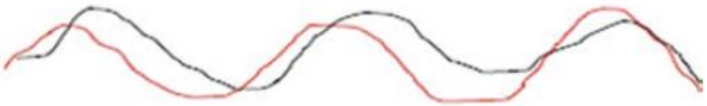
Network elements: Transmission Media

- Transmission media play a vital role in the performance of a network.
- Without it, the communication between network elements can not happen and there will no connection between the elements.
- Media types
  - Wired transmission media
  - Wireless transmission media

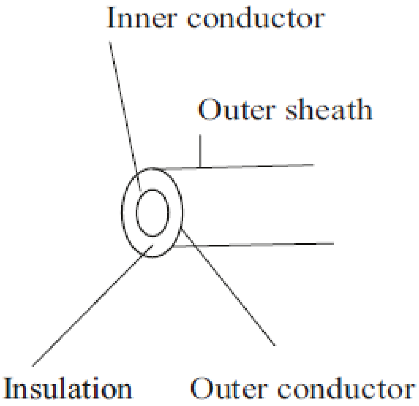
Network elements: Transmission Media

Wired transmission media

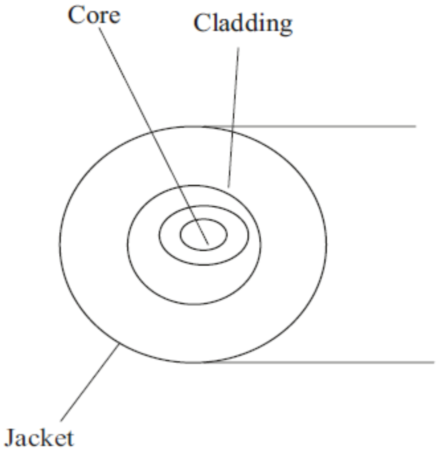
- Copper wires:
- Twisted pair



- Coaxial cables



- Optical fiber



Network elements: Transmission Media

Wireless transmission media results in the three wireless network categories depending on distances:

- Restricted Proximity Network: it involves LANs with a combination of wireless and fixed devices.
- Intermediate/Extended Network: it is made of two fixed LAN joining together by a wireless element.
- Mobile Network: the network uses a base station to provide a radio network over land areas.

Network elements: Transmission Media

Wireless transmission media

- **Infrared wave** is the electromagnetic wave that carries coded instructions exchanged between network elements. It uses line-of-sight propagation.
- **High-Frequency Radio (RF)** wave is the high-frequency electromagnetic radio wave. Its range is greater than that of infrared wave. The RF transmission is good for long distances, but it is affected by interferences and rains.
- **Microwave** is a higher version of radio wave. It uses a pair of parabolic antennas. It is unidirectional and do not go through buildings.
- **Laser light** is used for transmitting data for several thousand yards via the air and optical fibers. The restriction is that it works in the context of no obstacles in the line of sight.

Network Categories

Network categories

- The network is categorized based on
  - Network size
  - Network ownership
  - Number of connected users
  - The distance it covers and physical architecture
  - Available services in the area

- Examples:
  - Small home
  - Small Office/Home Office
  - Medium/Large
  - World Wide

Local Area Network (LAN)

- LAN covers a small geographical area (few kilometers).
- It is designed mainly for sharing resources such as printers, programs, disks, and data.
- It is managed and administered by an individual or a single organization
- It enables a high-speed bandwidth communication within the internal network
- The common LAN types are star, bus, ring, or tree topologies.

Metropolitan Area Network (MAN)

- The MAN is design for covering an entire city.
- It has a larger geographical scope in comparison with a LAN and can range from 10km to a few hundreds km in length.
- It may be operated and owned by a private company or a public service provider.

Wide Area Network (WAN)

- A WAN interconnect LANs that span a wide geographical area.
- It is designed for the interconnection of computer systems over a large area like a continent, a country or even over the world
- It possibly uses the public, leased or private communication devices, usually in combinations, and thus can span an unlimited number of miles.
- The Internet is a good example of WAN. The Internet has a connection to similar networks in other regions.
- The WAN typically has slower speed connections between LANs.

The Internet

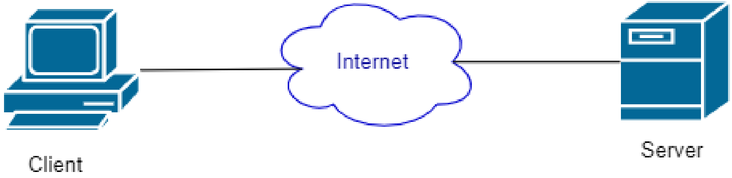
- LAN are connected to each other using WANs
- WANs may use copper wires, fiber optic cables, and wireless transmissions.
- The Internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:
  - IETF (Internet Engineering Task Force) develops Internet standards.
  - ICANN (Internet Corporation For Assigned Names and Numbers) for managing domain name system and allocating IP addresses.
  - IAB (Internet Architecture Board) oversees the evolution of the Internet standards and protocols.
- To connect users and organization to the Internet uses broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services, business DSL, leased lines, and Metro Ethernet.

Network Model

Network Model: Client-Server network

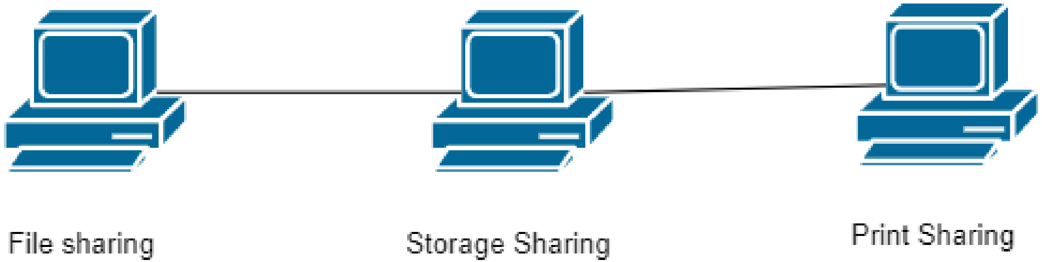
- A server is a computer which give information to the hosts or ends devices, e.g. file server, web server, or email server, etc.

- A client is a computer which sends requests to the server to get information
  - Retrieving emails from an email server
  - Retrieving web pages from a web server



Network Model: Peer-to-peer network

- In a peer-to-peer network, a device can be a server or a client.
- The peer-to-peer network design is suitable for small networks



Network Model: Centralized network

A centralized network model includes:

- One central computer called master
- Dependent computers called surrogates

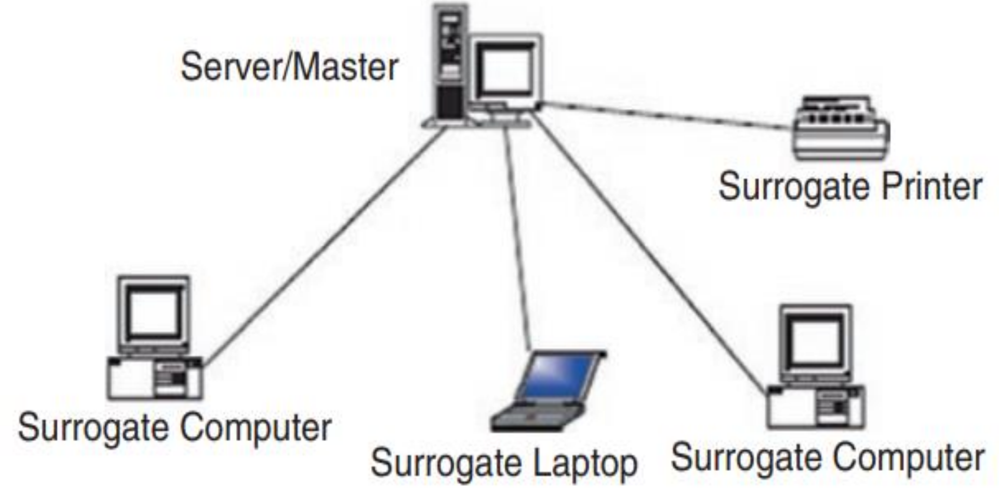


Figure. A centralized network model (Kizza, 2020, p.5)

Network Model: Distributed network

- Computers may own their local resources
- Computers in the network can work as stand alone

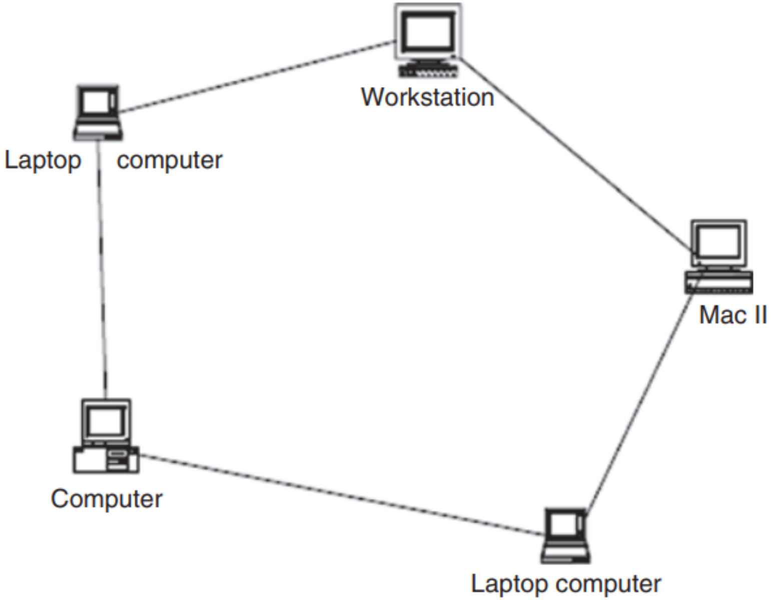


Figure. A distributed network model (Kizza, 2020, p.5)

Network Topology

Network Topology

The term “topology” refers to the approach in which network elements are interconnected. The common LAN topologies are as below.

- Mesh network
- Tree network
- Bus network
- Star network
- Ring network

Network Topology: Mesh Network

- Multiple access links between network devices
- Most often applied in MAN
- Advantages:
  - High reliability
  - Easy fault identification and fault isolation
  - Robust
- Disadvantages:
  - High cost with high demand for cabling
  - High demands for the number of I/O ports

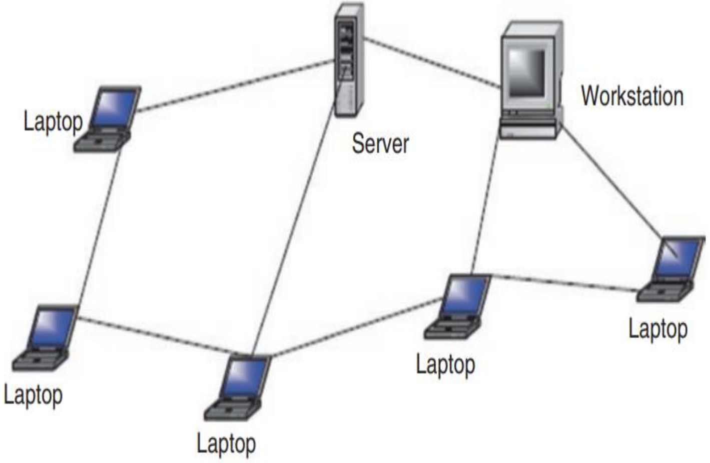


Figure. A distributed network model (Kizza, 2020, p.14)

Network Topology: Tree Network

- Hierarchical structure
- The most predominant element is the root of the tree and all other elements in the same network sharing a child-parent relationship.
- Advantages:
  - High reliability
  - Easy fault identification and fault isolation
  - Robust
- Disadvantages:
  - High cost with high demand for cabling
  - High demands for the number of I/O ports

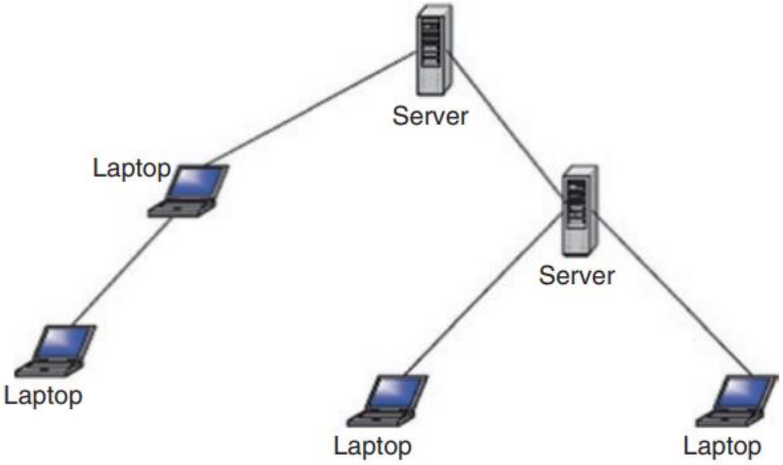


Figure. A distributed network model (Kizza, 2020, p.14)

Network topology: Bus Network

- A bus network is multipoint.
- One long cable acts a backbone connecting all devices in a network
- Advantages:
  - Simple, reliable and easy to use
  - Less cabling
- Disadvantages:
  - Can be used in relative small networks
  - Difficult to add new nodes
  - All network devices share the same bus
  - Reconfiguration is difficult

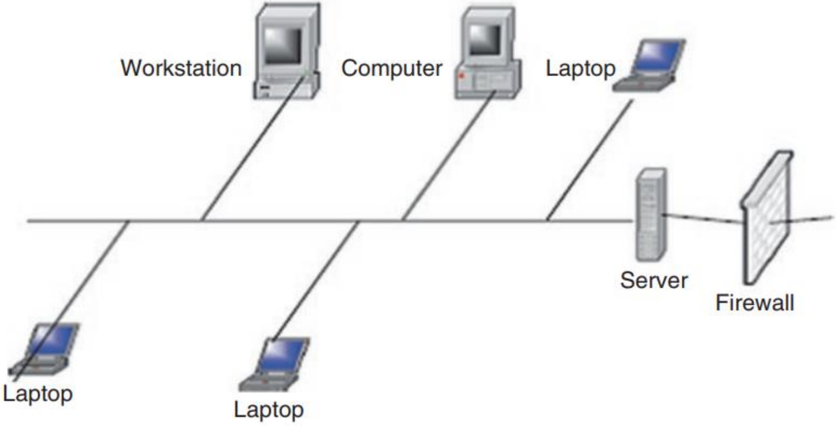


Figure. A distributed network model (Kizza, 2020, p.15)

Network Topology: Star Network

- It needs a central node connects with other devices in the network

- The central point is referred as a hub.

- Advantages:
  - Easy to diagnose network faults
  - Single device failure does not affect the network
  - Easy to add new device
  - Ordinary telephone cables can be used

- Disadvantages:
  - The central hub failure causes the failure of the entire network

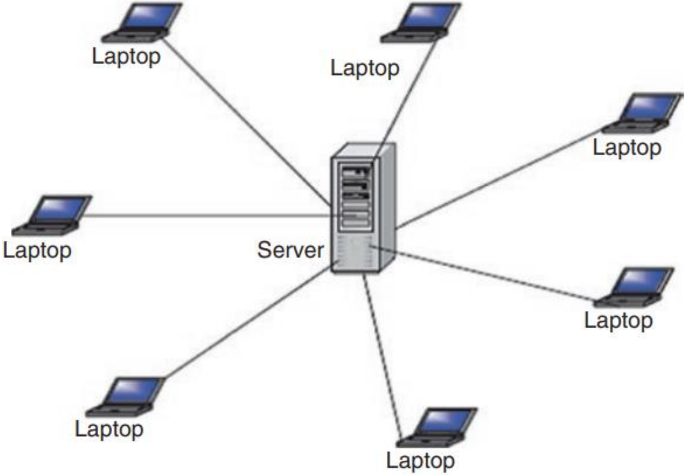


Figure. A distributed network model (Kizza, 2020, p.16)

Network Topology: Ring Network

- In the ring network, each device has a repeater
- Advantages:
  - No terminators is required
  - Fault isolation is simple
- Disadvantages:
  - A break in the ring will stop the transmission of the entire network
  - Adding/removing a device disrupts the whole network

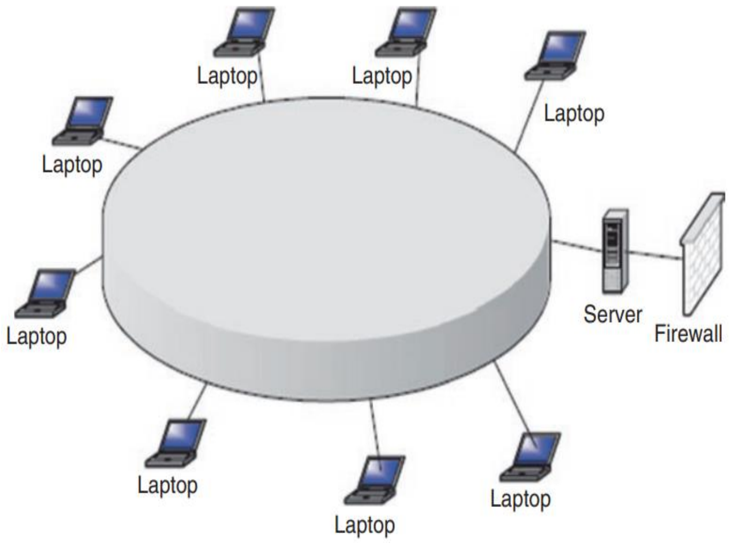


Figure. A distributed network model (Kizza, 2020, p.16)

Network Topology

- Ring and mesh topologies are suitable for peer-to-peer network
- Star and tree network are more convenient for client server
- Bus network can be used for either of them.

- Different from other types of network topologies, mesh network enables multiple connections between network elements.
- The choice of network topologies is dependent on transmission medium, reliability of the network, the network size, and prediction of the future growth.

Network Addressing

Network Addressing Types

There are two IP (Internet Protocol) address types:

- IPv4: 10.10.10.1
- IPv6: 2345:0425:2CA1:0000:0000:0567:5673:23b5

Network Performance

Network Performance Metrics

- **Fault Tolerance:** limits the failures in the network connections
- **Scalability:** enable future expanding the network capacity
- **Quality of Service (QoS):** ensure the quality to services like voice or video transmissions
- **Security:** secure the network connections with three goals as confidentiality, integrity, and availability

Network Protocol

What is a computer networking protocols?

"A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event." (Kurose, 2017, p.37)

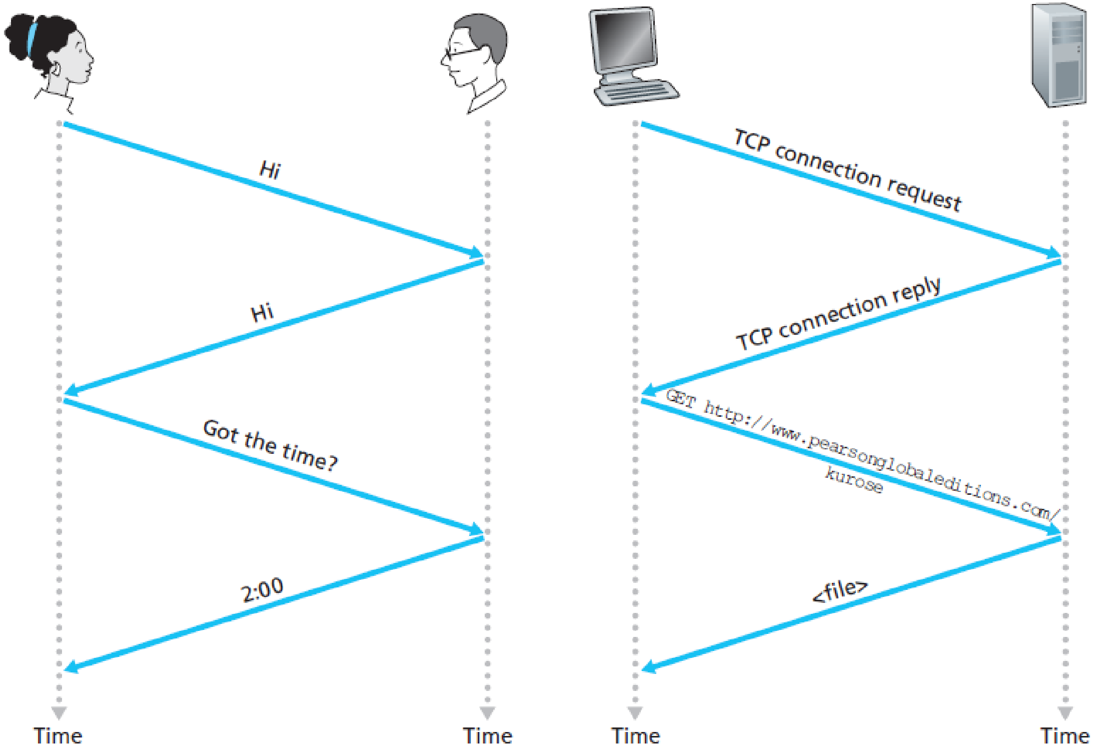


Figure. A human protocol and a computer network protocol (Kurose, 2017, p.35)

Network Protocol

- The Network protocol defines a common set of communication rules between networking devices.
- It can be implemented in hardware or software or both
- It has its own format, rules, and functions
- Protocol types:
  - Network communications
  - Network security
  - Routing
  - Service discovery

Network Protocol

- The Network protocol must be suitable with other protocols in the same communication channel.

- The protocol is viewed in terms of layer

  - Higher layers

  - Lower layers

Network Protocol Models

- **Internet Protocol Suite or TCP/IP**
- **Open Systems Interconnection (OSI) protocols**
- **AppleTalk**
- **Novell NetWare**

Network Protocol Models

- **Internet Protocol Suite or TCP/IP**

TCP/IP Model Layer	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

Network Protocol Models

- **Open Systems Interconnection (OSI) protocols**

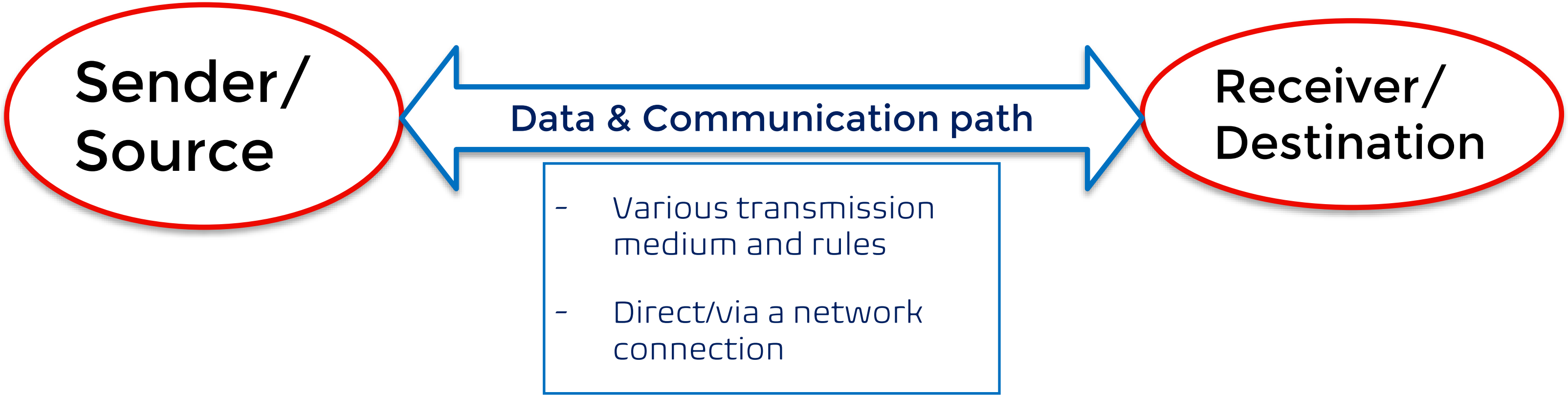
OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network.
2 - Data Link	Describes methods for exchanging data frames over a common media.
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.

Network Protocol Models

- **Comparison of the two models**
  - The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
  - The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
  - OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

Network Protocol: Background

- Fundamental Communication



Sender/ Source

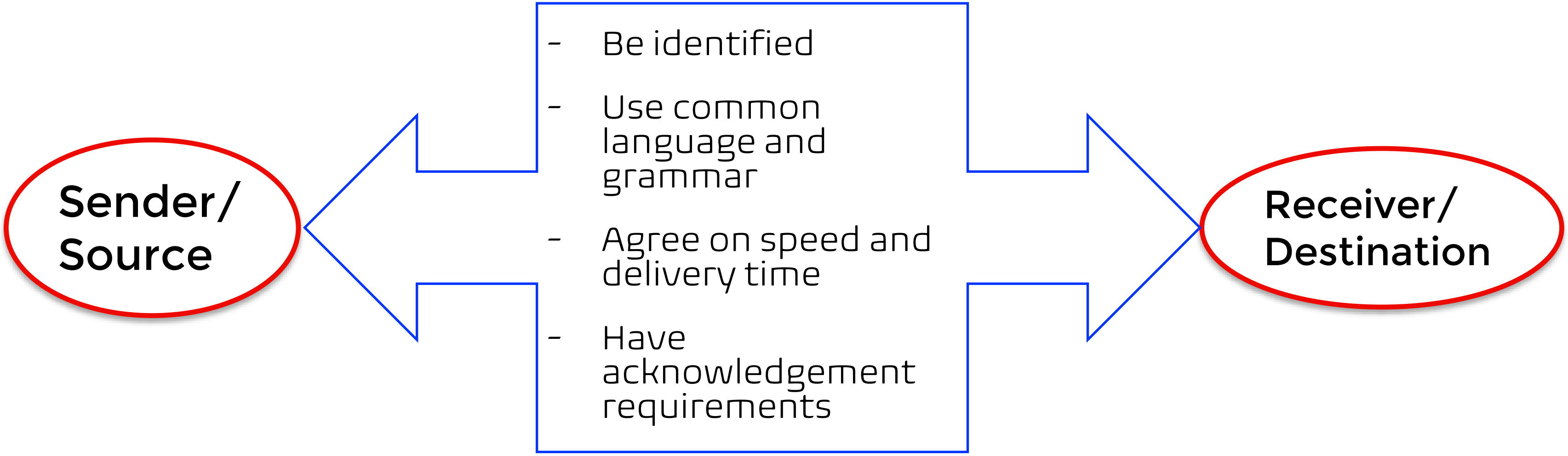
Data & Communication path

- Various transmission medium and rules
- Direct/via a network connection

Receiver/ Destination

Network Protocol: Background

- Rule establishment



Sender/ Source

- Be identified
- Use common language and grammar
- Agree on speed and delivery time
- Have acknowledgement requirements

Receiver/ Destination

Network Protocol: Background

- Network Protocol Requirements
  - Message encoding
  - Message formatting and encapsulation
  - Message size
  - Message timing
  - Message delivery options

Network Protocol: Background

- Network Protocol Requirements
  - Message encoding
    - Encoding is to covert information into another acceptable form for transmission
    - Decoding is to reverse this process to interpret the information

Network Protocol: Background

- Network Protocol Requirements
  - Message formatting and encapsulation
    - When a message is sent, it must use a specific format or structure.
    - Message formats are dependent on the type of message and the channel that is used to transmit the message.

Network Protocol: Background

- Network Protocol Requirements
  - Message size
    - Encoding between hosts must be in an appropriate format for the medium.
      - Messages sent across the network are converted to bits
      - The bits are encoded into a pattern of light, sound, or electrical impulses.
      - The destination host must decode the signals to interpret the message.

Network Protocol: Background

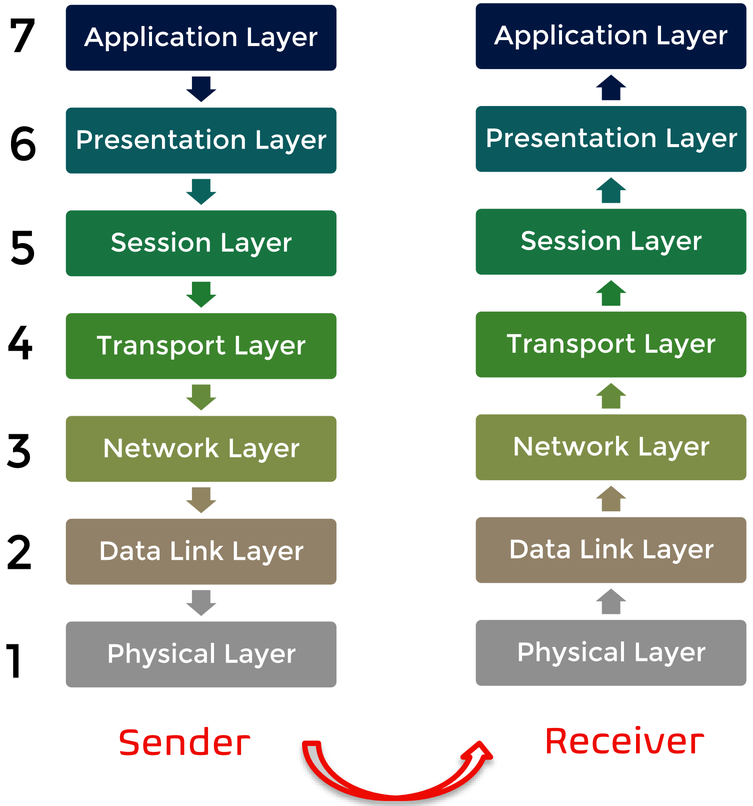
- Network Protocol Requirements
  - Message timing includes:
    - Flow Control – to manage the rate of data transmission and define how much information could be sent and the speed at which it could be delivered.
    - Response Timeout – to manage how long a device need to wait when it does not hear a response from the destination.
    - Access method – to determine when someone can send a message.
      - There may be various rules governing issues like "collisions". This is when more than one device sends traffic at the same time and the messages become corrupt.
      - Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

Network Protocol: Background

- Network Protocol Requirements
  - Message delivery options
    - Unicast – one to one communication
    - Multicast – one to many, typically not all
    - Broadcast – one to all

Protocol stack/model/suite

OSI Model



7 Application Layer

6 Presentation Layer

5 Session Layer

4 Transport Layer

3 Network Layer

2 Data Link Layer

1 Physical Layer

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

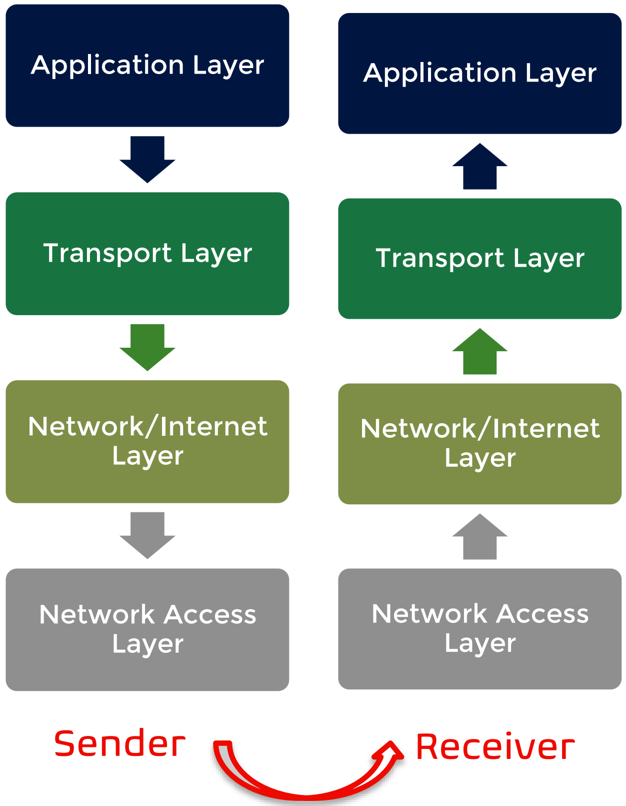
Data Link Layer

Physical Layer

Sender

Receiver

TCP/IP Model



Application Layer

Transport Layer

Network/Internet Layer

Network Access Layer

Application Layer

Transport Layer

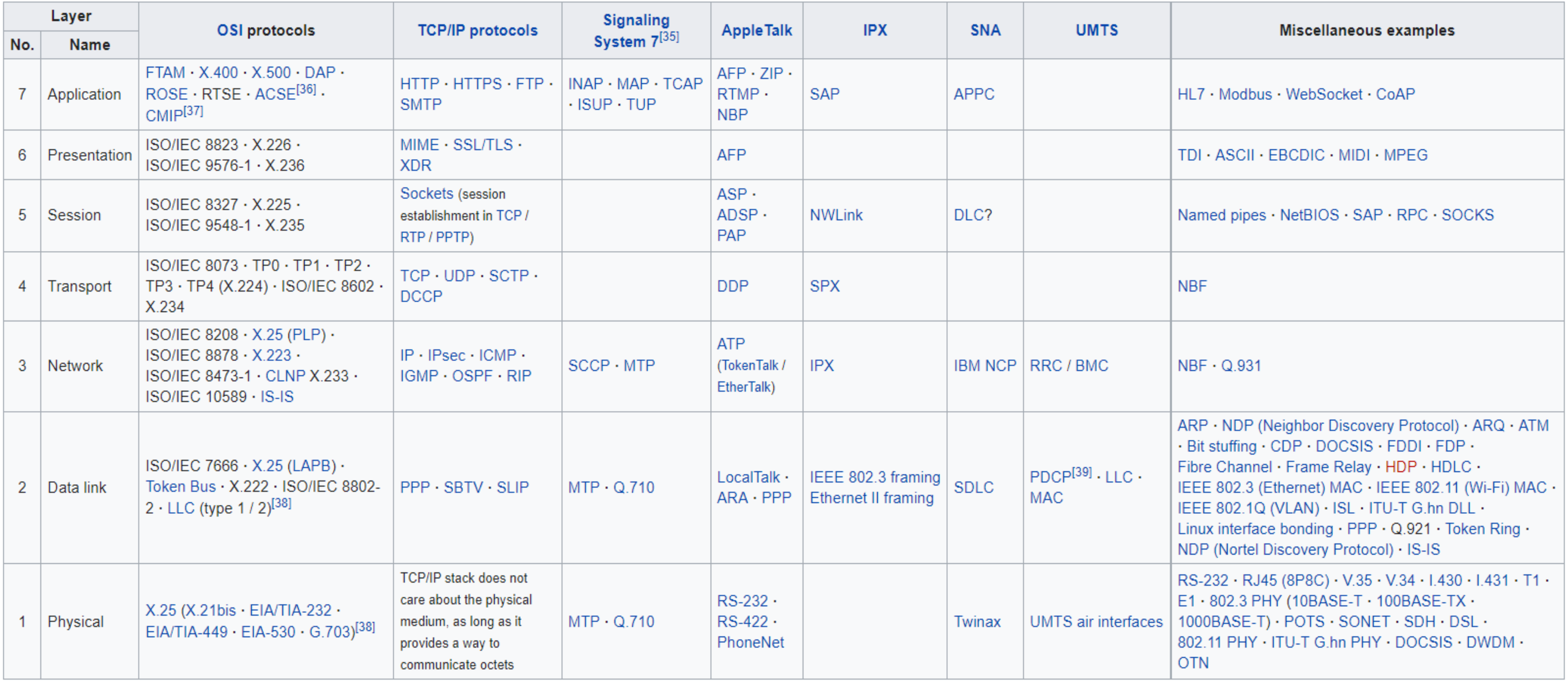
Network/Internet Layer

Network Access Layer

Sender

Receiver

Background – OSI Protocol and other networking suites



Layer		OSI protocols	TCP/IP protocols	Signaling System 7[35]	AppleTalk	IPX	SNA	UMTS	Miscellaneous examples
No.	Name								
7	Application	FTAM · X.400 · X.500 · DAP · ROSE · RTSE · ACSE[36] · CMIP[37]	HTTP · HTTPS · FTP · SMTP	INAP · MAP · TCAP · ISUP · TUP	AFP · ZIP · RTMP · NBP	SAP	APPC		HL7 · Modbus · WebSocket · CoAP
6	Presentation	ISO/IEC 8823 · X.226 · ISO/IEC 9576-1 · X.236	MIME · SSL/TLS · XDR		AFP				TDI · ASCII · EBCDIC · MIDI · MPEG
5	Session	ISO/IEC 8327 · X.225 · ISO/IEC 9548-1 · X.235	Sockets (session establishment in TCP / RTP / PPTP)		ASP · ADSP · PAP	NWLink	DLC?		Named pipes · NetBIOS · SAP · RPC · SOCKS
4	Transport	ISO/IEC 8073 · TP0 · TP1 · TP2 · TP3 · TP4 (X.224) · ISO/IEC 8602 · X.234	TCP · UDP · SCTP · DCCP		DDP	SPX			NBF
3	Network	ISO/IEC 8208 · X.25 (PLP) · ISO/IEC 8878 · X.223 · ISO/IEC 8473-1 · CLNP X.233 · ISO/IEC 10589 · IS-IS	IP · IPsec · ICMP · IGMP · OSPF · RIP	SCCP · MTP	ATP (TokenTalk / EtherTalk)	IPX	IBM NCP	RRC / BMC	NBF · Q.931
2	Data link	ISO/IEC 7666 · X.25 (LAPB) · Token Bus · X.222 · ISO/IEC 8802-2 · LLC (type 1 / 2)[38]	PPP · SBTV · SLIP	MTP · Q.710	LocalTalk · ARA · PPP	IEEE 802.3 framing Ethernet II framing	SDLC	PDCP[39] · LLC · MAC	ARP · NDP (Neighbor Discovery Protocol) · ARQ · ATM · Bit stuffing · CDP · DOCSIS · FDDI · FDP · Fibre Channel · Frame Relay · HDP · HDLC · IEEE 802.3 (Ethernet) MAC · IEEE 802.11 (Wi-Fi) MAC · IEEE 802.1Q (VLAN) · ISL · ITU-T G.hn DLL · Linux interface bonding · PPP · Q.921 · Token Ring · NDP (Nortel Discovery Protocol) · IS-IS
1	Physical	X.25 (X.21bis · EIA/TIA-232 · EIA/TIA-449 · EIA-530 · G.703)[38]	TCP/IP stack does not care about the physical medium, as long as it provides a way to communicate octets	MTP · Q.710	RS-232 · RS-422 · PhoneNet		Twinax	UMTS air interfaces	RS-232 · RJ45 (8P8C) · V.35 · V.34 · I.430 · I.431 · T1 · E1 · 802.3 PHY (10BASE-T · 100BASE-TX · 1000BASE-T) · POTS · SONET · SDH · DSL · 802.11 PHY · ITU-T G.hn PHY · DOCSIS · DWDM · OTN

https://en.wikipedia.org/wiki/OSI_model

Background – Protocol Suite and PDU

OSI Model

Layer		Protocol Data Unit (PDU)
7	Application	Data
6	Presentation	
5	Session	
4	Transport	Segment, Datagram
3	Network	Packet
2	Data Link	Frame
1	Physical	Bit, Symbol

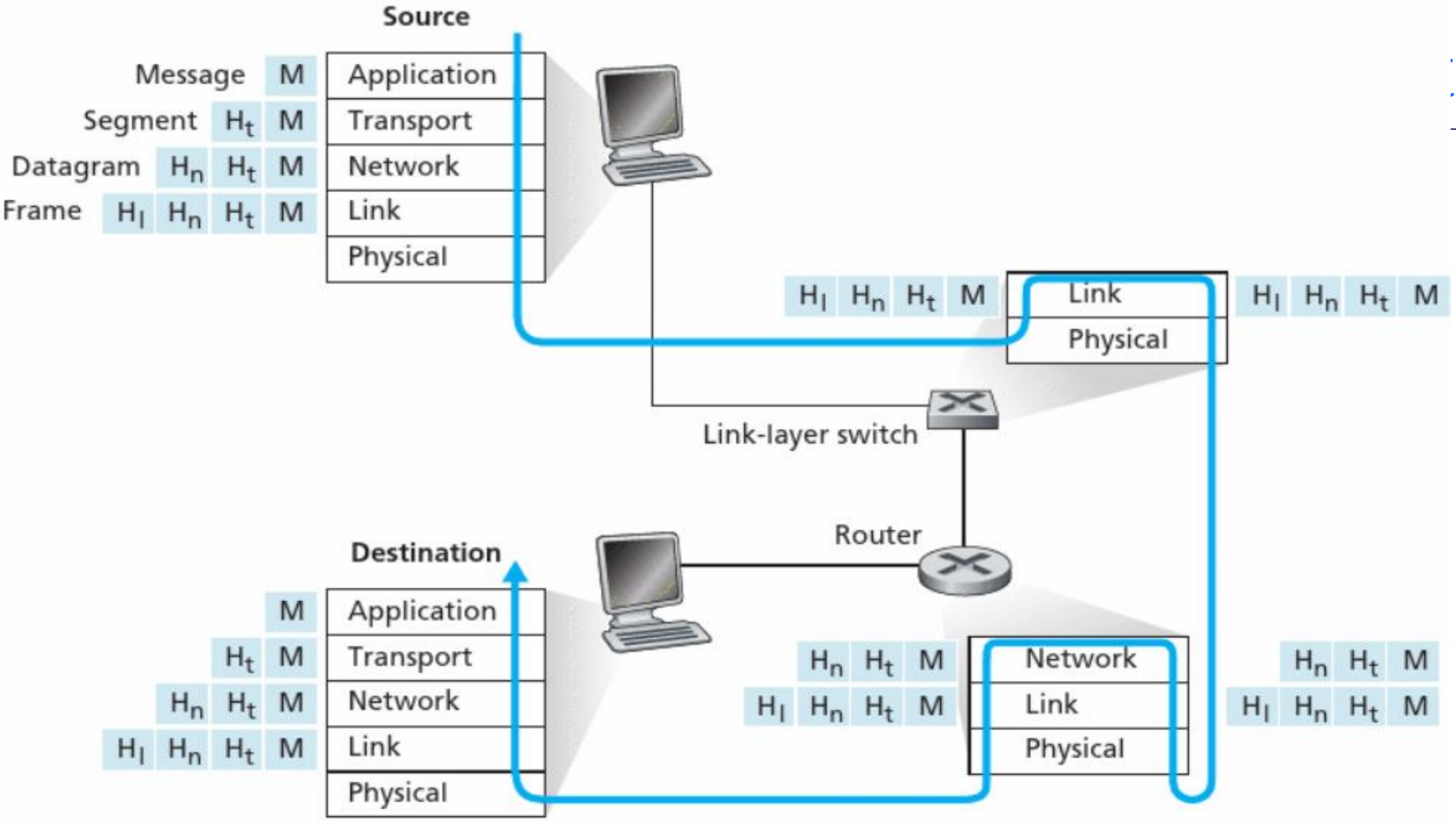
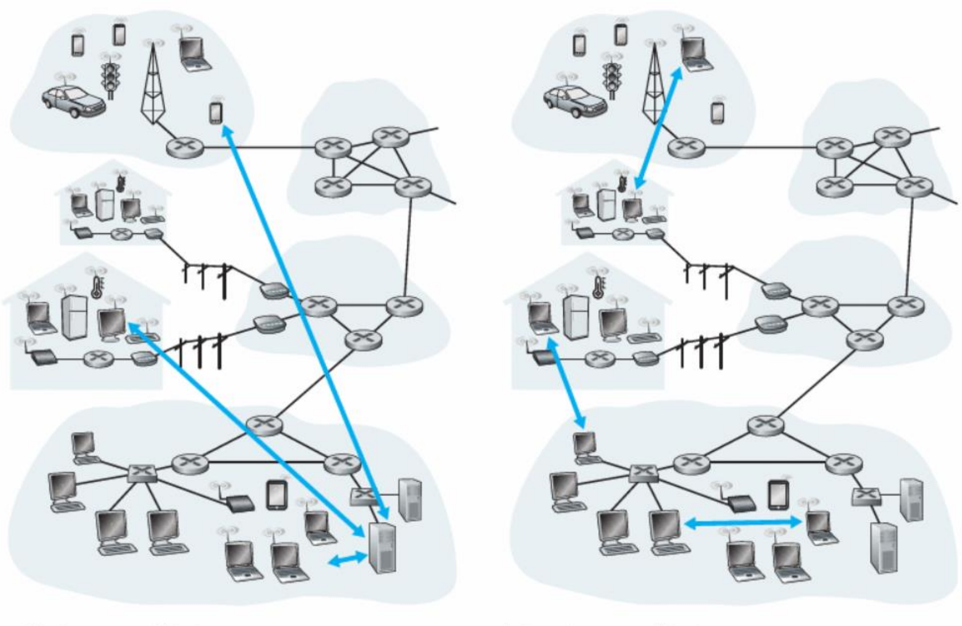


Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

(Kurose, 2017, p.81)

Application Layer

- Provides an interface between the applications used to communicate and the underlying network
- Network application architecture
  - ○ Client-server architecture
  - ○ Peer-to-peer architecture



a. Client-server architecture

b. Peer-to-peer architecture

Figure 2.2 ♦ (a) Client-server architecture; (b) P2P architecture

(Kurose, 2017, p.115)

Application Layer

- “A process can be thought of as a program that is running within an end system”
  - Sending process
  - Receiving process

- Application-layer data unit

= message/data

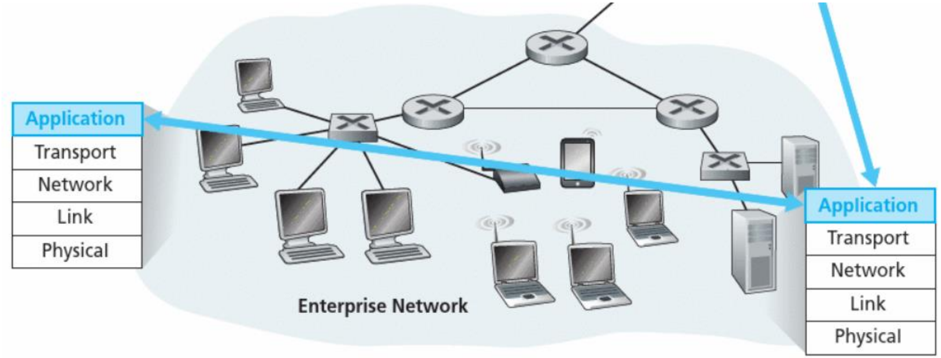


Figure 2.1 ♦ Communication for a network application takes place between end systems at the application layer

(Kurose, 2017, p.113)

Application Layer

- Socket is a virtual interface enabling the process of sending messages into and receiving messages from the network
  - An analogy: a door of a house
- Socket is referred as the API (Application Programming Interface) between the application and the network
- Application developer has the control of application layer and the choice of transport protocol

(Kurose, 2017, p.117)

Application Layer

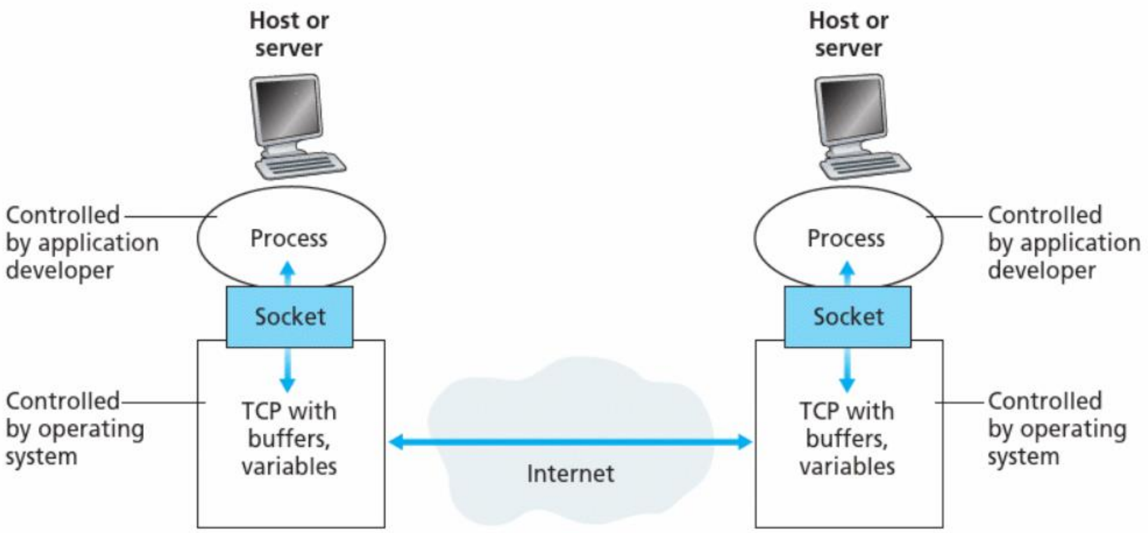

Host or server
Host or server
Controlled by application developer
Process
Socket
Controlled by operating system
TCP with buffers, variables
Internet
Process
Controlled by application developer
Socket
TCP with buffers, variables
Controlled by operating system

Figure 2.3 ♦ Application processes, sockets, and underlying transport protocol

(Kurose, 2017, p.118)

Application Layer

- Application layer protocols define:
  - Types of exchanged messages, e.g. request and response messages
  - Syntax of message types, e.g. fields in the message and how the fields are delineated
  - Semantics of the fields
  - Rules for determining when and how a process starts sending and receiving messages

Application Layer

- Application layer protocols
  - File services: FTP (File Transfer Protocol)
  - IP addressing services: DNS (Domain Name Service)
  - Web services: HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure)
  - Email protocols:
    - SMTP (Simple Mail Transfer Protocol)
    - POP (Post Office Protocol) & IMAP (Internet Message Access Protocol)

(Kurose, 2017, p.124)

Application Layer - Example

- Web Application
  - Client-server application
  - Components:
    - A standard for document format, e.g. HTML
    - Web browsers, e.g. Firefox, Chrome
    - Web servers, e.g. Apache
    - An application-layer protocol, e.g. HTTP which defines the format and sequence of messages exchanged between the web server and the browser
- Network application is different from application-layer protocol

(Kurose, 2017, p.125)

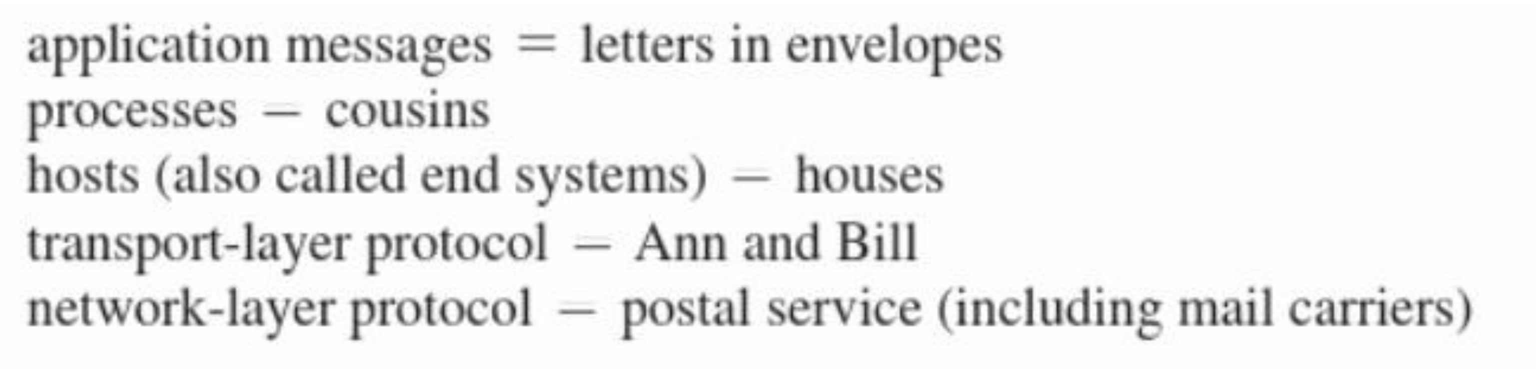
Transport Layer

- “A transport-layer protocol provides for logical communication processes running on different hosts.”
- Two popular protocols:
  - UDP (User Datagram Protocol)
  - TCP (Transmission Control Protocol)
- Transport-layer data unit = segment

(Kurose, 2017, p.216)

Transport Layer

- Household analogy



application messages = letters in envelopes
processes = cousins
hosts (also called end systems) = houses
transport-layer protocol = Ann and Bill
network-layer protocol = postal service (including mail carriers)

(Kurose, 2017, p.218)

Transport Layer - UDP

- UDP (User Datagram Protocol)
  - Provides unreliable and connectionless services
  - Does not guarantee that data sent by one process will arrive intact to the destination process
  - Dose not support congestion control mechanism
  - No handshaking before establishing connections

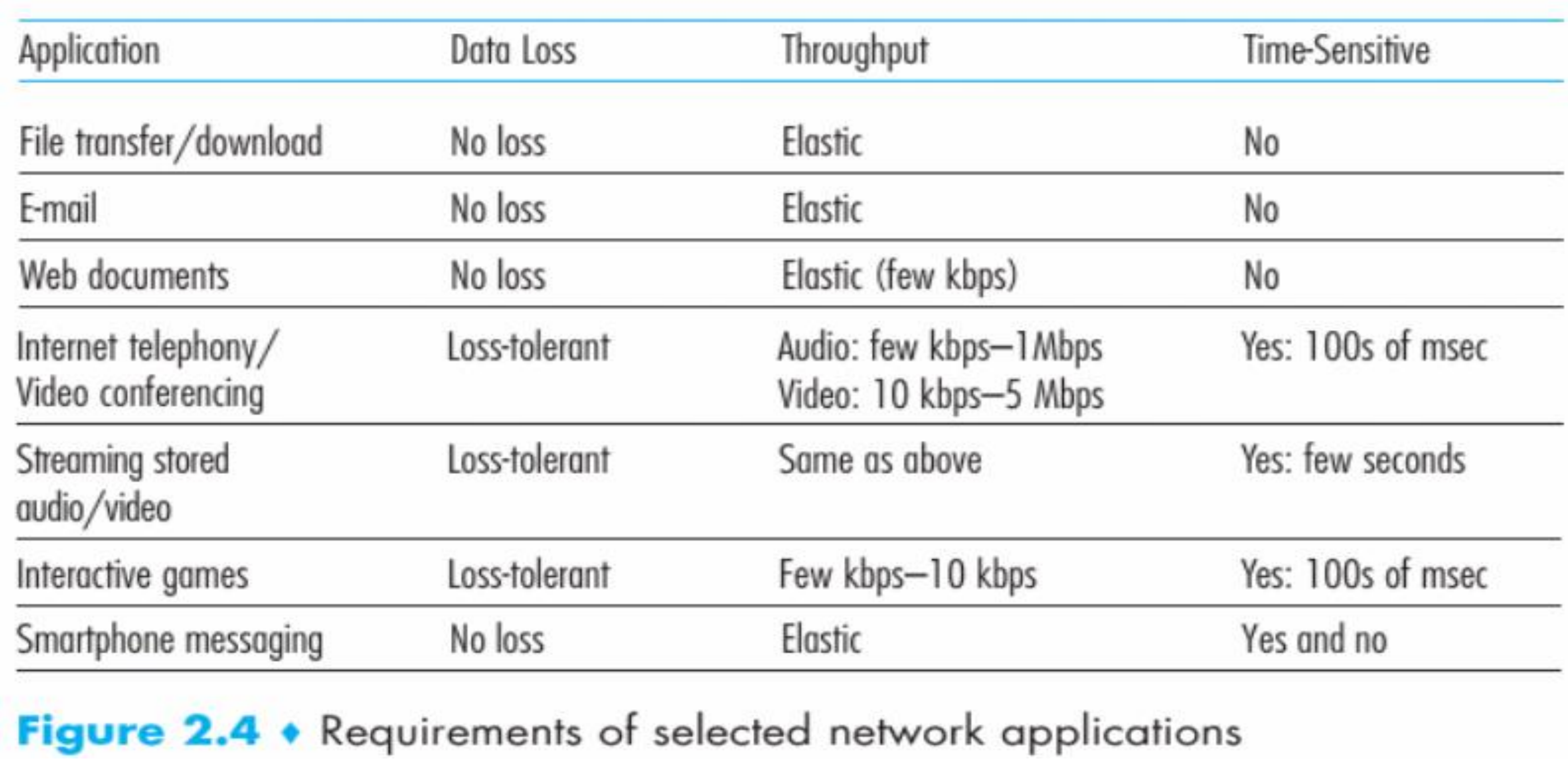
(Kurose, 2017, p.220)

Transport Layer - TCP

- TCP (Transmission Control Protocol)
  - Provides reliable and connection-oriented services
  - Uses flow control, sequence numbers, acknowledgements, and timers
  - Ensure data sent to the destination correctly and in order
  - Provide congestion control

(Kurose, 2017, p.220)

Transport Layer – TCP services

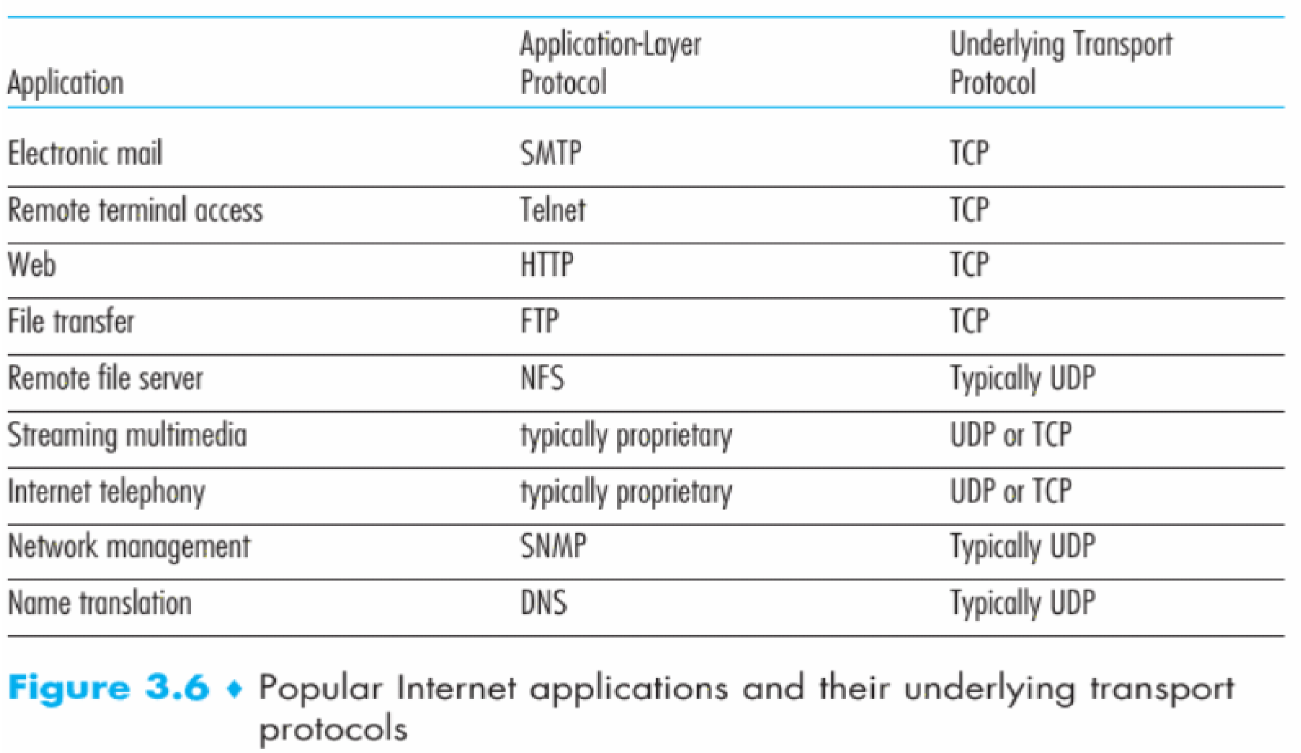


Application	Data Loss	Throughput	Time-Sensitive
File transfer/download	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No loss	Elastic (few kbps)	No
Internet telephony/ Video conferencing	Loss-tolerant	Audio: few kbps–1Mbps Video: 10 kbps–5 Mbps	Yes: 100s of msec
Streaming stored audio/video	Loss-tolerant	Same as above	Yes: few seconds
Interactive games	Loss-tolerant	Few kbps–10 kbps	Yes: 100s of msec
Smartphone messaging	No loss	Elastic	Yes and no

Figure 2.4 ♦ Requirements of selected network applications

(Kurose, 2017, p.121)

Transport Layer – with application protocol



Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Name translation	DNS	Typically UDP

Figure 3.6 ♦ Popular Internet applications and their underlying transport protocols

(Kurose, 2017, p.231)

Transport Layer – Demultiplexing + Multiplexing

- Delivering the data in a transport-layer segment to the correct socket is called demultiplexing.
- The job of gathering data chunks at the source host from different sockets, encapsulating each data chunk with header information (that will later be used in demultiplexing) to create segments, and passing the segments to the network layer is called multiplexing.
- Required information
  - Unique socket identifier
  - Source and Destination Port number

(Kurose, 2017, p.221-2)

Transport Layer – Demultiplexing + Multiplexing

- Required information
  - Unique socket identifier
  - Source and Destination Port number
    - 16-bit number, ranging from 0-65535
    - Registered port number ranging from 1024 – 49151
    - Remaining port numbers are private ones (49152 - 65535)
    - Well-known port number ranging from 0-1023

Application Protocol	Port number
HTTP	TCP port 80
HTTPS	TCP port 443
FTP	TCP port 21
POP3 email	TCP port 110

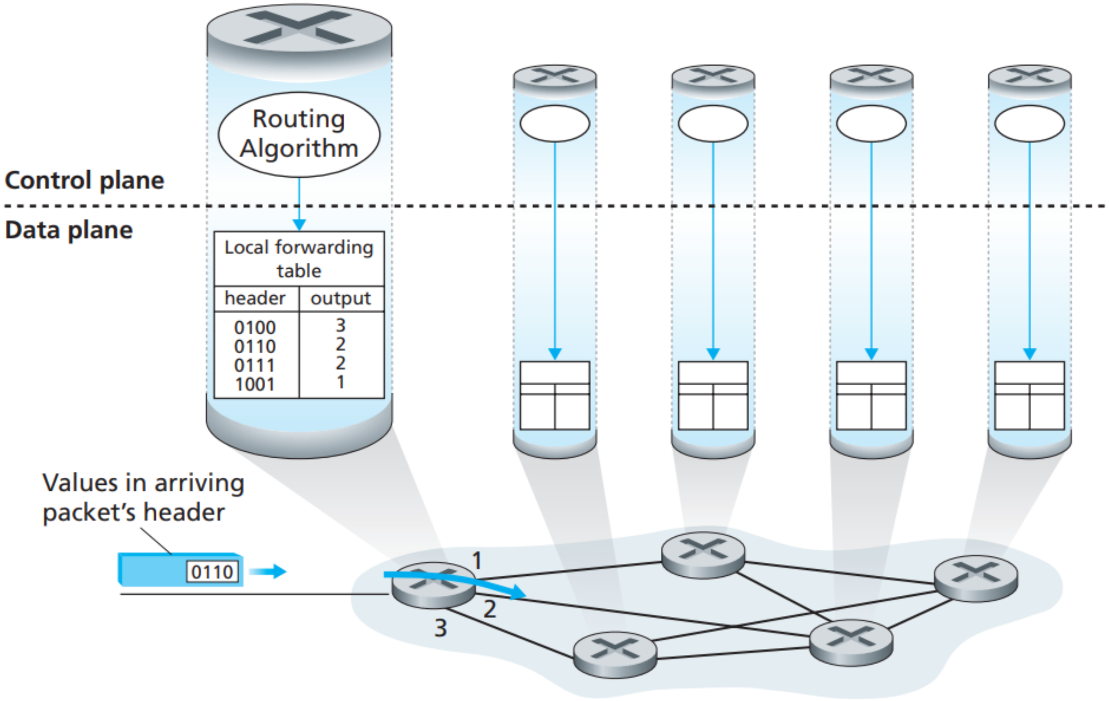
(Kurose, 2017, p.221-2)

Network Layer

- Network-layer data unit = packet
- Primary role is to move packets from a sender to a receiver
- Two main functions
  - Forwarding/Switching in data plane : move a packet from an input link interface to an output link interface
  - Routing in control plane : determine an end-to-end route/path for forwarding a packet from source to destination
    - Routing algorithms are for calculating the path
    - E.g. driving analogy

(Kurose, 2017, p.336)

Network Layer - Plane



Local forwarding table

header	output
0100	3
0110	2
0111	2
1001	1

Figure 4.2 ♦ Routing algorithms determine values in forward tables

(Kurose, 2017, p.337)

Network Layer - Router

- Four components
  - Input ports
  - Output ports
  - Switching fabric
  - Routing processor

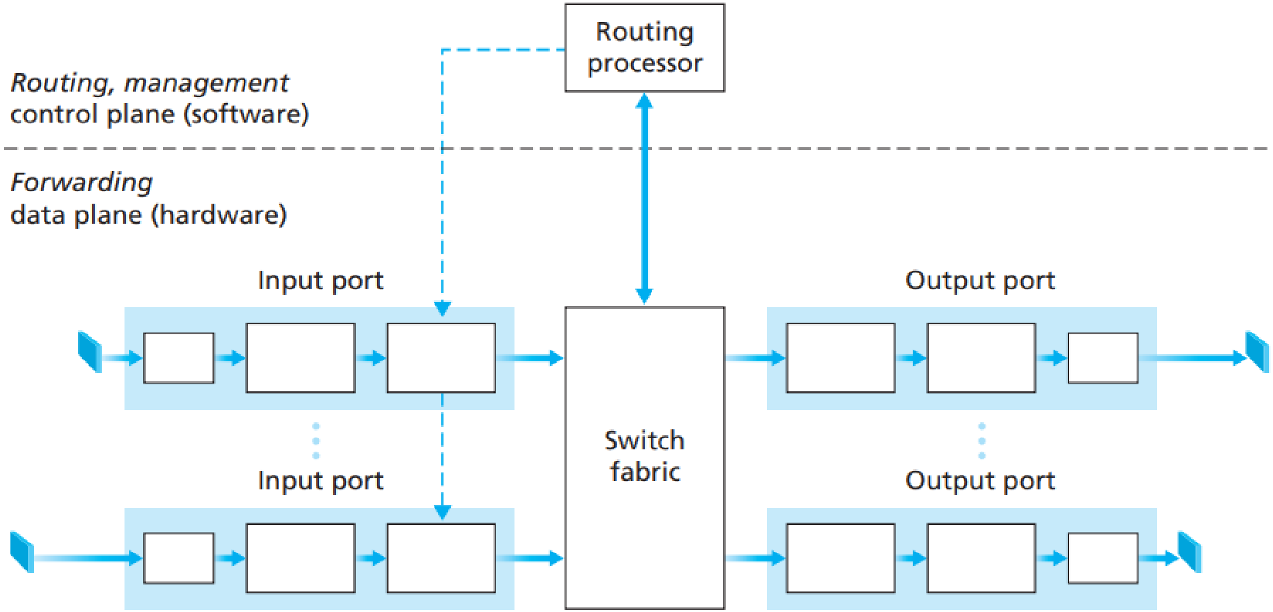


Figure 4.4 ♦ Router architecture

(Kurose, 2017, p.341)

Network Layer - Router

- Four components
  - Input ports performs several key functions
    - Physical-layer function of terminating an incoming physical link at a router
    - Link-layer function for interoperating with the link layer at the other side of the incoming link

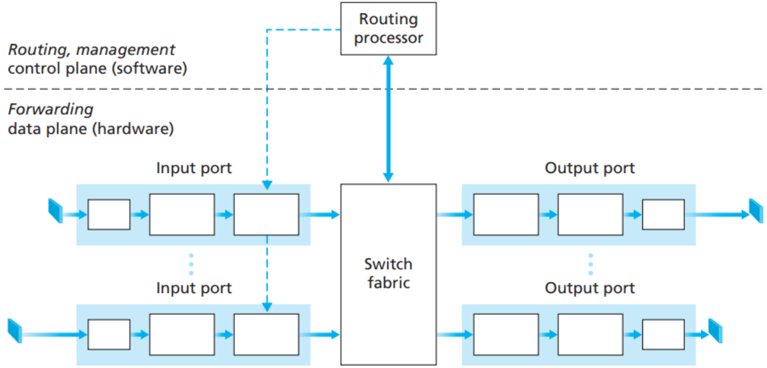


Figure 4.4 ♦ Router architecture

(Kurose, 2017, p.342)

Network Layer - Router

- Four components
  - Output ports
    - Stores packets received from the switching fabric and delivers the packet on the outgoing link by performing link-layer and physical-layer functions.
    - If a link is bidirectional carrying traffic in both directions, an output port will be paired with the input port on the same line card.

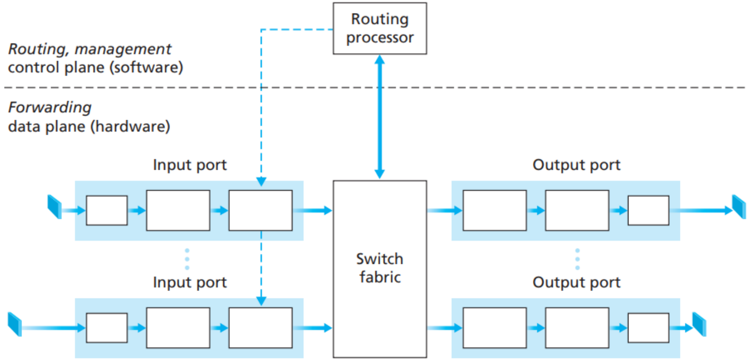


Figure 4.4 ♦ Router architecture

(Kurose, 2017, p.342)

Network Layer - Router

- Four components
  - Switch fabric
    - Connecting the router input ports an output ones
    - Is implemented inside the router

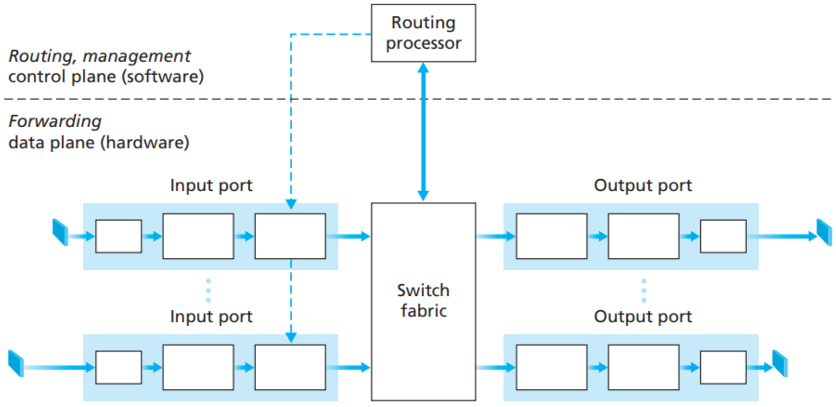


Figure 4.4 ♦ Router architecture

(Kurose, 2017, p.342)

Network Layer - Router

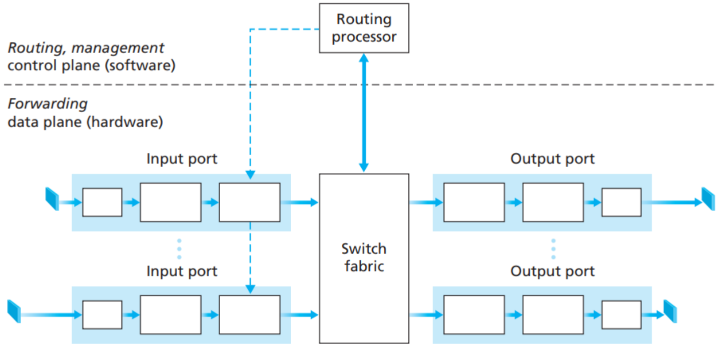


Figure 4.4 ♦ Router architecture

- Four components
  - Routing processor
    - Performs control-plane functions
    - In traditional routers
      - **Executes routing protocols**
      - **Maintains routing tables and attached link state information**
      - **Computes the forwarding tables**
    - In modern (SDN) routers
      - **Communicates with the SDN (Software-defined Network) controller to receive the forwarding table entries and implement them in the router's input ports**

(Kurose, 2017, p.342)

Network Layer – Forwarding table computation

- Two possible ways to compute the forwarding and flow tables
  - Per-router control: when each router runs a routing algorithm, both forwarding and routing function are included in the router
  - Logical centralized control: a logically centralized controller computes and distributes the forwarding tables to be used by every router.

(Kurose, 2017, p.402)

Network Layer – Routing algorithm

- To determine good paths to forward a packet from a source to a destination
- A good path → least cost path
- Three ways to classify routing algorithms
  - Centralized and decentralized routing algorithm
  - Static and dynamic routing algorithm
  - Load-sensitive and load-insensitive routing algorithm

(Kurose, 2017, p.406-7)

Network Layer – Routing algorithm

- Centralized routing algorithm
  - Computes least-cost path using complete, global knowledge about the network
  - Take inputs from all nodes and links in the network
  - Or called Link-State (LS) algorithm

(Kurose, 2017, p.406)

Network Layer – Routing algorithm

- Decentralized routing algorithm
  - Computes least-cost path using an interactive, distributed manner by the routers
  - Or called distance-vector (DV) algorithm since each node maintains a vector of estimates of the costs (distance) to all other nodes in the network.
  - DV operates efficiently in small networks

(Kurose, 2017, p.406)

Network Layer – Routing algorithm

- Static routing algorithm
  - Routes change very slowly over time
  - Needs human intervention, e.g. manually editing a link costs
- Dynamic routing algorithm
  - Changes the routing paths as network traffic loads or topology change
  - More responsive to network changes

(Kurose, 2017, p.407)

Network Layer – Routing algorithm

- Load-sensitive routing algorithm
  - Link costs vary dynamically to reflect the current level of congestion in the underlying link
  - If a high cost is associated with a link that is currently congested, a routing algorithm will tend to choose routes around such a congested link
  - E.g. ARPAnet
- Load-insensitive routing algorithm
  - A link’s cost does not explicitly reflect its current level of congestion
  - E.g. RIP, OSPF, BGP

(Kurose, 2017, p.407)

Network Layer - Routing protocols

- Link state protocols or called as shortest-path-first-protocols
  - The router creates 3 separate tables
    - Keep track of directly attached neighbours
    - Determine the topology of the entire network
    - Routing table
  - Know more about the internetwork than any distance-vector routing protocol
  - E.g. OSPF is a completely link state routing protocol
  - Send updates containing state of their own links to all other routers on the network

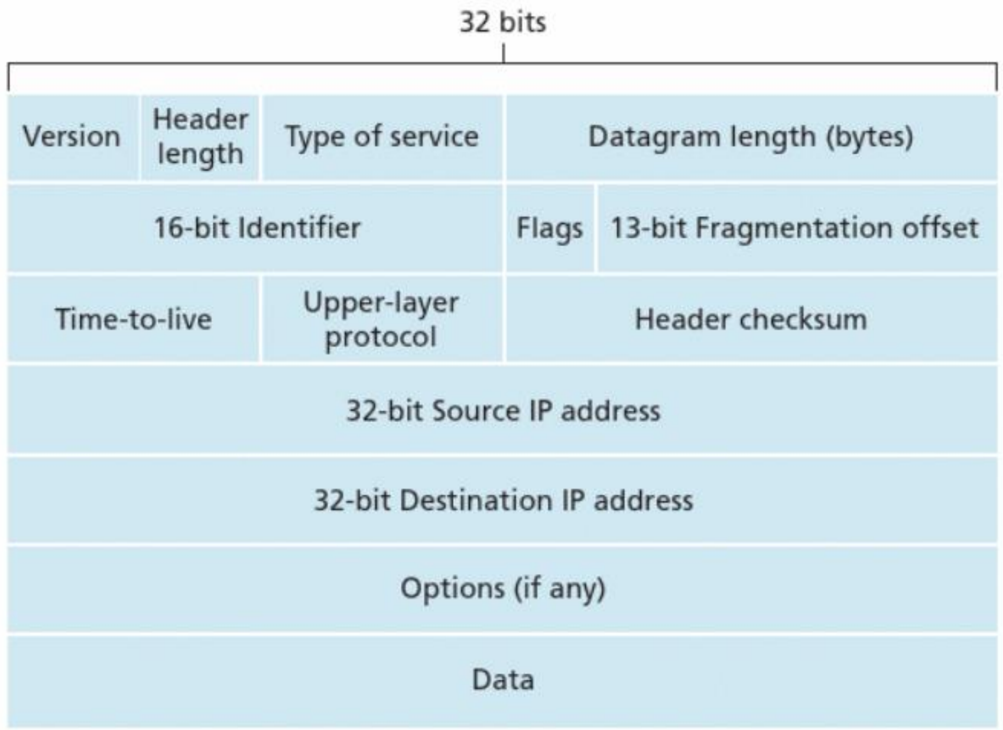
(Kurose, 2017, p.407)

Network Layer - Routing protocols

- Distance-Vector protocols pass complete routing table contents to neighboring routers
- E.g. RIP using only hop count to determine the best path to a network

(Kurose, 2017, p.412)

Network layer – Internet Protocol (IP)



32 bits

<table>
<tr><td colspan="4">Version</td><td colspan="4">Header length</td><td colspan="8">Type of service</td><td colspan="16">Datagram length (bytes)</td></tr>
<tr><td colspan="16">16-bit Identifier</td><td colspan="3">Flags</td><td colspan="13">13-bit Fragmentation offset</td></tr>
<tr><td colspan="8">Time-to-live</td><td colspan="8">Upper-layer protocol</td><td colspan="16">Header checksum</td></tr>
<tr><td colspan="32">32-bit Source IP address</td></tr>
<tr><td colspan="32">32-bit Destination IP address</td></tr>
<tr><td colspan="32">Options (if any)</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

Figure 4.16 ♦ IPv4 datagram format

(Kurose, 2017, p.358)

Network layer – Internet Protocol (IP)

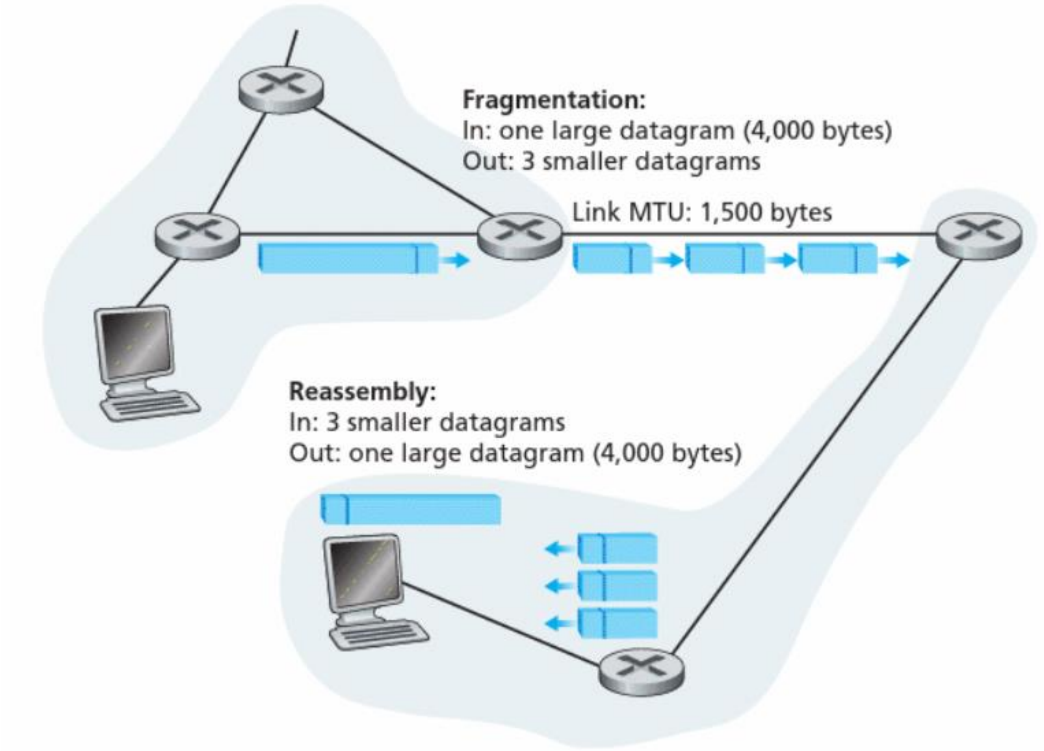
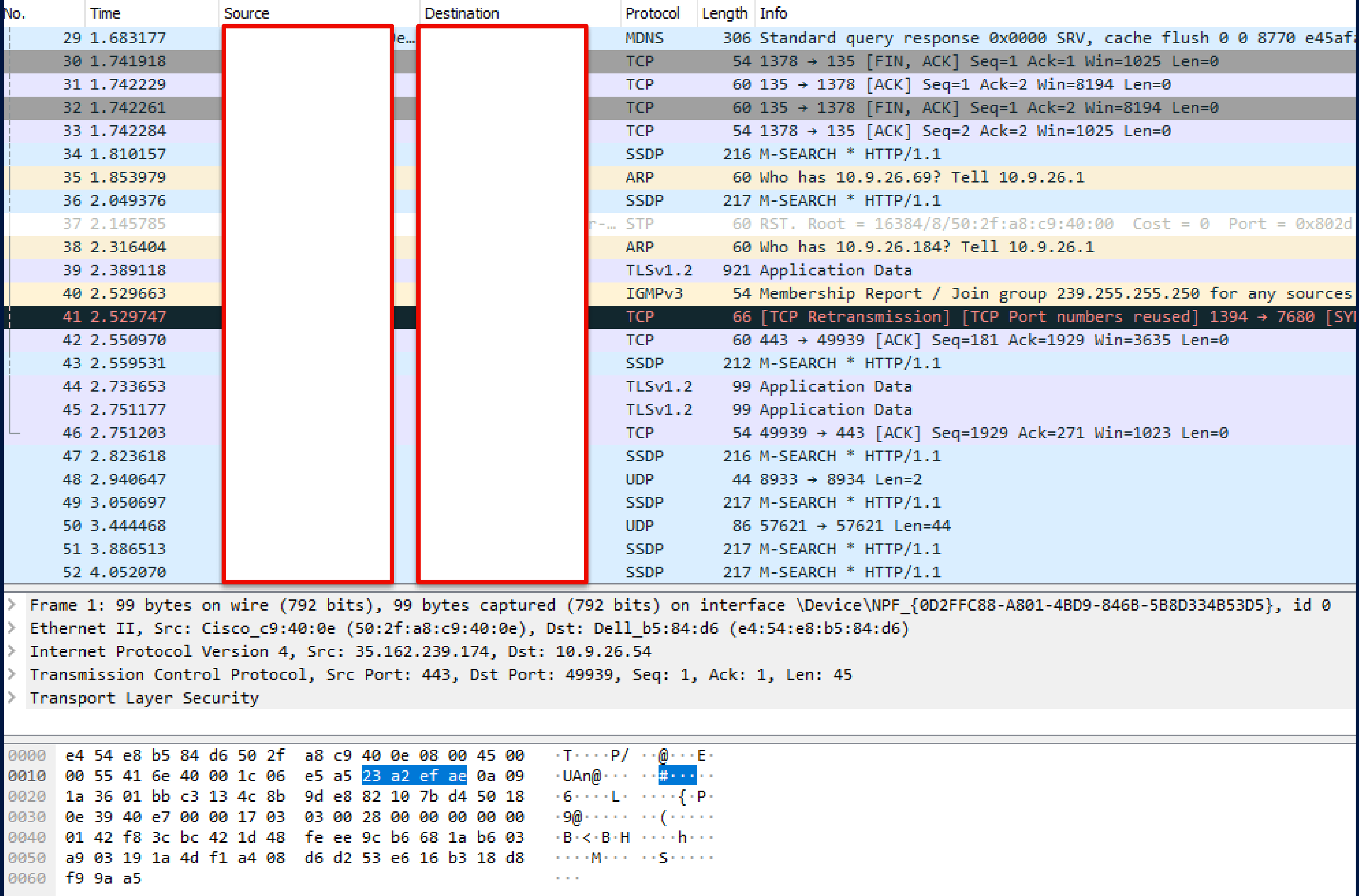


Figure 4.17 ♦ IP fragmentation and reassembly

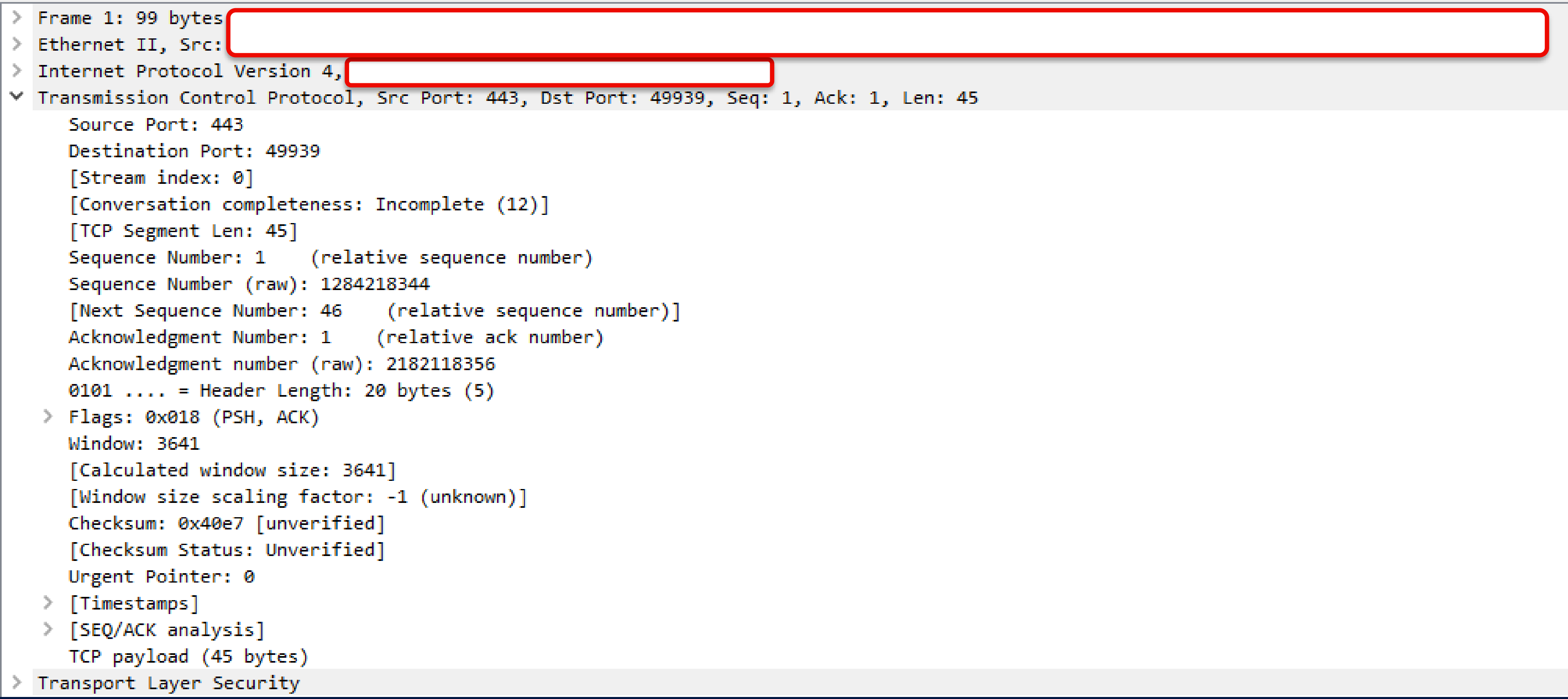
(Kurose, 2017, p.362)



No.	Time	Source	Destination	Protocol	Length	Info
29	1.683177	[redacted]	[redacted]	MDNS	306	Standard query response 0x0000 SRV, cache flush 0 0 8770 e45af
30	1.741918	[redacted]	[redacted]	TCP	54	1378 → 135 [FIN, ACK] Seq=1 Ack=1 Win=1025 Len=0
31	1.742229	[redacted]	[redacted]	TCP	60	135 → 1378 [ACK] Seq=1 Ack=2 Win=8194 Len=0
32	1.742261	[redacted]	[redacted]	TCP	60	135 → 1378 [FIN, ACK] Seq=1 Ack=2 Win=8194 Len=0
33	1.742284	[redacted]	[redacted]	TCP	54	1378 → 135 [ACK] Seq=2 Ack=2 Win=1025 Len=0
34	1.810157	[redacted]	[redacted]	SSDP	216	M-SEARCH * HTTP/1.1
35	1.853979	[redacted]	[redacted]	ARP	60	Who has 10.9.26.69? Tell 10.9.26.1
36	2.049376	[redacted]	[redacted]	SSDP	217	M-SEARCH * HTTP/1.1
37	2.145785	[redacted]	[redacted]	STP	60	RST. Root = 16384/8/50:2f:a8:c9:40:00 Cost = 0 Port = 0x802d
38	2.316404	[redacted]	[redacted]	ARP	60	Who has 10.9.26.184? Tell 10.9.26.1
39	2.389118	[redacted]	[redacted]	TLSv1.2	921	Application Data
40	2.529663	[redacted]	[redacted]	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
41	2.529747	[redacted]	[redacted]	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 1394 → 7680 [SY
42	2.550970	[redacted]	[redacted]	TCP	60	443 → 49939 [ACK] Seq=181 Ack=1929 Win=3635 Len=0
43	2.559531	[redacted]	[redacted]	SSDP	212	M-SEARCH * HTTP/1.1
44	2.733653	[redacted]	[redacted]	TLSv1.2	99	Application Data
45	2.751177	[redacted]	[redacted]	TLSv1.2	99	Application Data
46	2.751203	[redacted]	[redacted]	TCP	54	49939 → 443 [ACK] Seq=1929 Ack=271 Win=1023 Len=0
47	2.823618	[redacted]	[redacted]	SSDP	216	M-SEARCH * HTTP/1.1
48	2.940647	[redacted]	[redacted]	UDP	44	8933 → 8934 Len=2
49	3.050697	[redacted]	[redacted]	SSDP	217	M-SEARCH * HTTP/1.1
50	3.444468	[redacted]	[redacted]	UDP	86	57621 → 57621 Len=44
51	3.886513	[redacted]	[redacted]	SSDP	217	M-SEARCH * HTTP/1.1
52	4.052070	[redacted]	[redacted]	SSDP	217	M-SEARCH * HTTP/1.1

```
> Frame 1: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{0D2FFC88-A801-4BD9-846B-5B8D334B53D5}, id 0
> Ethernet II, Src: Cisco_c9:40:0e (50:2f:a8:c9:40:0e), Dst: Dell_b5:84:d6 (e4:54:e8:b5:84:d6)
> Internet Protocol Version 4, Src: 35.162.239.174, Dst: 10.9.26.54
> Transmission Control Protocol, Src Port: 443, Dst Port: 49939, Seq: 1, Ack: 1, Len: 45
> Transport Layer Security
```

```
0000  e4 54 e8 b5 84 d6 50 2f  a8 c9 40 0e 08 00 45 00   ·T····P/ ··@···E·
0010  00 55 41 6e 40 00 1c 06  e5 a5 23 a2 ef ae 0a 09   ·UAn@··· ··#·····
0020  1a 36 01 bb c3 13 4c 8b  9d e8 82 10 7b d4 50 18   ·6····L· ····{·P·
0030  0e 39 40 e7 00 00 17 03  03 00 28 00 00 00 00 00   ·9@····· ··(·····
0040  01 42 f8 3c bc 42 1d 48  fe ee 9c b6 68 1a b6 03   ·B·<·B·H ····h···
0050  a9 03 19 1a 4d f1 a4 08  d6 d2 53 e6 16 b3 18 d8   ····M··· ··S·····
0060  f9 9a a5                                           ···
```



```
> Frame 1: 99 bytes [redacted]
> Ethernet II, Src:
> Internet Protocol Version 4, [redacted]
v Transmission Control Protocol, Src Port: 443, Dst Port: 49939, Seq: 1, Ack: 1, Len: 45
    Source Port: 443
    Destination Port: 49939
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 45]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1284218344
    [Next Sequence Number: 46    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2182118356
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 3641
    [Calculated window size: 3641]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x40e7 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (45 bytes)
> Transport Layer Security
```

Network service model

- Define characteristics of end-to-end delivery of packets between senders and receivers

- Services
  - Guaranteed delivery
  - Guaranteed delivery with bounded delay
  - In-order packet delivery
  - Guaranteed minimal bandwidth
  - Security
  - Best-effort service is a special one

(Kurose, 2017, p.339)

Network Access – Data Link layer

- Data Link layer or layer 2 protocol in the OSI model
- Data units = frames
- Links are communication channels connecting adjacent nodes
- Connecting end-device and network interface cards (NIC)
- A device needs a NIC (network interface card) to connect to a network
    - One device may have one or multiple NICs

(Kurose, 2017, p.79, 471)

Network Access – Data Link layer

- Services provided by link layer
  - Framing
  - Link access
  - Reliable delivery
  - Error detection and correction

(Kurose, 2017, p.470)

Network Access – Physical layer

- Data unites = bits
- Physical connection must be established before any network communication occurs
- Connections can be wired or wireless
- Protocols in this layer depend on the actual transmission medium of the link, e.g., twisted-pair copper wire, single-mode fiber optics

(Kurose, 2017, p.80, 471)

References and Reading

- **Chapter 1** - Kizza, J. M. (2020). Computer Network Fundamentals. In J. M. Kizza (Ed.), *Guide to Computer Network Security* (pp. 3-40). Cham: Springer International Publishing. *(Available online via UOW library)*
- **Chapter 1 -** Kurose, J. F. (2017). *Computer networking : a top-down approach* (Seventh, global edition. ed.). Boston: Pearson.
- **Chapter 4** - Shinde, S. (2000). *Computer network*. New Age International Ltd.
- CCNAv7: Introduction to Networks (ITN) – Module 1,3

Thank you
Q&A ?

UNIVERSITY
OF WOLLONGONG
AUSTRALIA