Chapter 3:
Network Protocols & Communication
Chapter 3 - Scope

3.1 Rules of Communication
3.2 Network Protocols and Standards
3.3 Moving Data in the Network
3.4 Summary
The Rules

What is Communication?

Communication is exchange of information through a medium.

Human Communication

Message Source → Transmitter → Transmission Medium → Receiver → Message Destination

Jane............voice box..............air.....................ears......................Kelvin
Rules for Communication

- There must be a sender and receiver
- Method of communicating must be agreed, eg
  - face-to-face,
  - telephone,
  - letter,
  - photograph, etc.
- There must be common language and grammar
- Speed and timing of delivery must be specified
- Confirmation or acknowledgment requirements must be decided on
Machine Communication
Message Formatting and Encapsulation

- Before being sent, a message must be formatted and encapsulated.
- Encapsulation means binding together the data and functions that manipulate the data, and keeping them safe from outside interference and misuse.
Message Formatting and Encapsulation

A message can contain the following elements:

- Identifier of the recipient’s location (**where**)
- Identifier of the sender’s location (**where**)
- Salutation or greeting ("Hello")
- Recipient identifier ("Peter")
- The message content ("How are you")
- Source identifier
- End of message indicator
Message Size, segment, frame

An overview of the segmenting process:

- A message has a minimum and maximum size.
- A message is broken into *segments*.
- Each segment is encapsulated in a separate *frame* with the address information. The size of one frame is usually limited.
- The frames are sent to the *receiving host*.
- At the receiving host, each frame is *de-encapsulated* and put back together as a message. It is then processed and interpreted.
The Rules

Message Sending process

- A message is broken into segments.
- Each segment is encapsulated in a separate frame with the address information, and is sent over the network.
- At the receiving host, the message is de-encapsulated and put back together to be processed and interpreted.

PROCESS OF MESSAGE SENT AND RECEIVED

message

segment

segment

framed

framed

SEND

framed

framed

segment

segment

message received
Message Timing

Access Method
Managing data on a **network** is a form of data traffic control.

- The **set of rules** that governs how **network** traffic is controlled is called the **access method**.

- Access Method determines **when it is ready** for a computer to send a message to avoid a collision of information.

- It is necessary for computers to define an access method.

- Hosts on a network need an access method to know when to begin sending messages and **how to respond when errors occur**.
Message Timing

- **Flow Control**
  Source and destination hosts use flow control to,
  - negotiate correct timing for successful communication
  - determine the amount of data to send,
  - determine the speed of sending.
Message Timing

Response Timeout

When a message is sent, it can be received successfully.

But sometimes, the receiver may take too long to do so. A time duration for timeout needs to be set. This is known as Response Timeout.

- Hosts on the network have rules that specify,
  - how long to wait for responses; after a pre-set time, the hosts will stop trying and issue a response timeout message
  - what action to take if a response timeout occurs.
Message Delivery Options

3 ways of sending messages are:

- **Unicast** (one-to-one)
  Unicast is communication between a single sender and a single receiver over a network.

- **Multicast** (one-to-many)
  Multicast is communication between a single sender and many interested receivers over a network.

- **Broadcast** (one-to-all)
  Broadcast is communication between a single sender and ALL devices in a network.
Protocols

Rules that Govern Communications

Protocols: Rules that Govern Communications

Content Layer

Where is the café?

Conversation protocol suite
1. Use a common language
2. Wait your turn
3. Signal when finished

Rules Layer

Physical Layer

Protocol suites are sets of rules that work together to help solve a problem.
Network Protocols

Communication in networks also need rules to govern:

- Message format or structure
- The process by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions
4 Layers of Protocols

- Application Protocol – Hypertext Transfer Protocol (HTTP)
- Transport Protocol – Transmission Control Protocol (TCP)
- Internet Protocol – Internet Protocol (IP)
- Network Access Protocols – Data link & physical layers
Protocol Suites

TCP/IP Protocol Suite and Communication
### Protocol Suites and Industry Standards

Four protocol suites used in the industry are:
- TCP/IP
- ISO
- Apple Talk
- Novell Netware

<table>
<thead>
<tr>
<th>Protocol Suite</th>
<th>TCP/IP</th>
<th>ISO</th>
<th>AppleTalk</th>
<th>Novell Netware</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>HTTP</td>
<td>ACSE</td>
<td>AFP</td>
<td>NDS</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS</td>
<td>ROSE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP</td>
<td>TRSE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>FTP</td>
<td>SESE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>TP0</td>
<td>TP0</td>
<td>ATP</td>
<td>SPX</td>
</tr>
<tr>
<td>UDP</td>
<td>TP1</td>
<td>TP1</td>
<td>AEP</td>
<td></td>
</tr>
<tr>
<td>IPv4</td>
<td>TP2</td>
<td>TP2</td>
<td>NBP</td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>TP3</td>
<td>TP3</td>
<td>RTMP</td>
<td></td>
</tr>
<tr>
<td>ICMPv4</td>
<td>TP4</td>
<td>TP4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMPv6</td>
<td></td>
<td>CONP/CMNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLNP/CLNS</td>
<td></td>
<td>AARP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
<td></td>
<td>AARP</td>
<td></td>
</tr>
<tr>
<td>PPP</td>
<td></td>
<td></td>
<td>IPX</td>
<td></td>
</tr>
<tr>
<td>Frame Relay</td>
<td></td>
<td></td>
<td>IPX</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Open Standards

- The Internet Society (ISOC)
- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- The International Organization for Standards (ISO)
Standards Organizations

IEEE

- 38 societies
- 130 journals
- 1,300 conferences each year
- 1,300 standards and projects
- 400,000 members
- 160 countries
- IEEE 802.3
- IEEE 802.11

IEEE 802 Working Groups and Study Groups

- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.24 Smart Grid TAG
Standards Organizations

Open Systems Interconnection (OSI)

The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system.

OSI Model has 7 layers; data packets will travel through these layers.
Models Compared

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>TCP/IP Protocol Suite</th>
<th>TCP/IP Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>HTTP, DNS, DHCP, FTP</td>
<td>Application</td>
</tr>
<tr>
<td>Presentation</td>
<td>TCP, UDP</td>
<td>Transport</td>
</tr>
<tr>
<td>Session</td>
<td>IPv4, IPv6, ICMPv4, ICMPv6</td>
<td>Internet</td>
</tr>
<tr>
<td>Transport</td>
<td>PPP, Frame Relay, Ethernet</td>
<td>Network Access</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reference Models
The TCP/IP Reference Model

TCP/IP Model

Application
Represents data to the user, plus encoding and dialog control.

Transport
Supports communication between diverse 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.
## Reference Models
### Comparing the OSI and TCP/IP Models

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>TCP/IP Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Application</td>
<td>Application</td>
</tr>
<tr>
<td>6. Presentation</td>
<td></td>
</tr>
<tr>
<td>5. Session</td>
<td>Transport</td>
</tr>
<tr>
<td>4. Transport</td>
<td>Internet</td>
</tr>
<tr>
<td>3. Network</td>
<td>Network Access</td>
</tr>
<tr>
<td>2. Data Link</td>
<td></td>
</tr>
<tr>
<td>1. Physical</td>
<td></td>
</tr>
</tbody>
</table>
The Rules

Message Sending process

- A message is broken into segments.
- Each segment is encapsulated in a separate frame with the address information, and is sent over the network.
- At the receiving host, the message is de-encapsulated and put back together to be processed and interpreted.
Data Encapsulation

Communicating the Messages

- Segmenting message benefits
  - Different conversations can be interleaved (mixed together as one)
  - Increased reliability of network communications

- Segmenting message disadvantage
  - Increased level of complexity – more programming processes are needed to split a message into segments
Data Encapsulation

Protocol Data Units (PDUs)

- Data (to be sent, such as an email)
- Segment
- Packet
- Frame
- Bits
Data Encapsulation

OSI Protocol Data Units (PDUs)

During data encapsulation, headers are added to the previous data.
Data Encapsulation

TCP/IP PDU

During protocol encapsulation, protocol headers of each OSI layer are added to the data.
Data Encapsulation

TCP/IP Protocol De-encapsulation
Network Addresses and Data Link Addresses

- **Physical**: Timing and synchronization bits
- **Data Link**: Destination and source physical addresses
- **Network**: Destination and source logical network addresses
- **Transport**: Destination and source process number (ports)
- **Upper Layers**: Encoded application data
Accessing Local Resources

MAC Address

A media access control address (MAC address) is the physical address of a computer. It is a unique identifier assigned to devices in a network segment. Using this address, data can reach the intended Destination.
Accessing Local Resources

Communicating with Device / Same Network

- Ethernet frame header contains MAC addresses of Source and Destination.
- IP packet header contains IP addresses of Source and Destination.

- Data Link
  - Ethernet Frame Header
- Network Layer
  - IP Packet Header

- Destination MAC address
- Source MAC address
- Source IP address
- Destination IP address
- Data

- PC1 (source)
  - IP address: 192.168.1.110
  - MAC address: AA-AA-AA-AA-AA

- FTP Server (destination)
  - IP address: 192.168.1.9
  - MAC address: CC-CC-CC-CC-CC-CC

A media access control address (MAC address), also called a physical address of a computer. It is a unique identifier assigned to network interfaces.
Accessing **Remote** Resources

**Default Gateway**

- In a TCP/IP network, nodes such as servers, workstations, and network devices each have a defined **default** route setting.
- This setting points to the default **gateway** where packets are sent to.
- The gateway is a router.
- Information for routing are stored in the PDU.

![Diagram](image)
Accessing **Remote** Resources

**Communicating Device / Remote Network**

One router controls traffic for one network. Data can be sent from one network to another network.
Review

1. In a network, data are sent in the form of ________.
Before being sent, a message must be formatted and ____________.
Encapsulation means ________ together the data and functions that manipulate the data, and keeping them safe from outside interference and misuse.
1. In a network, data are sent in the form of messages. Before being sent, a message must be formatted and encapsulated.

Encapsulation means binding together the data and functions that manipulate the data, and keeping them safe from outside interference and misuse.
Review

2. A message has a minimum and maximum size.
   It is broken into __________.

   Each segment is encapsulated in a separate __________ with the address information. The size of one frame is usually limited.

   The frames are sent to the receiving ____.

   At the receiving host, each frame is ___________ and put back together as a message. It is then processed and interpreted.
Review

2. A message has a minimum and maximum size. It is broken into segments.

Each segment is encapsulated in a separate frame with the address information. The size of one frame is usually limited.

The frames are sent to the receiving host.

At the receiving host, each frame is de-encapsulated and put back together as a message. It is then processed and interpreted.
Review

3. The set of rules that governs how network traffic is controlled is called the __________ _________.

Access Method determines when it is ready for a computer to send a message to avoid a _____________ of information.
Review

3. The set of rules that governs how network traffic is controlled is called the access method.

Access Method determines when it is ready for a computer to send a message to avoid a collision of information.
Review

4. Source and destination hosts use ______ ______ to,

- negotiate correct timing for successful communication
- determine the amount of data to send,
- determine the speed of sending.
Review

4. Source and destination hosts use flow control to,
- negotiate correct timing for successful communication
- determine the amount of data to send,
- determine the speed of sending.
5. When a message is sent, it can be received successfully. But sometimes, the receiver may take too long to do so. A time duration for timeout needs to be set. This is known as _________ _________.
Review

5. When a message is sent, it can be received successfully. But sometimes, the receiver may take too long to do so. A time duration for timeout needs to be set. This is known as **Response Timeout**.
Review

6. Three ways of sending messages are:

• ________
• ________
• ________
Review

6. Three ways of sending messages are:

- **Unicast** (one-to-one)
  Unicast is communication between a single sender and a single receiver over a network.

- **Multicast** (one-to-many)
  Multicast is communication between a single sender and many interested receivers over a network.

- **Broadcast** (one-to-all)
  Broadcast is communication between a single sender and ALL devices in a network.
Review

7. The four TCP/IP protocol layers are:
   A__________
   T__________
   I__________
   N__________
Review

7. The four protocol layers are:

   - Application Protocol – Hypertext Transfer Protocol (HTTP)
   - Transport Protocol – Transmission Control Protocol (TCP)
   - Internet Protocol – Internet Protocol (IP)
   - Network Access Protocols – Data link & physical layers
Review

8. Four protocol suites used in the Industry are:
   - TCP/IP
   - Novell Netware
Review

8. Four protocol suites used in the Industry are:
- TCP/IP
- ISO
- Apple Talk
- Novell Netware
Review

9. The **Open Systems Interconnection** model (OSI model) is a conceptual model that characterizes and standardizes the ________________ functions of a telecommunication or computing system.

The OSI Model has _______ layers;

_______ packets will travel through these layers.
Review

9. The **Open Systems Interconnection** model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system.

The OSI Model has **7** layers;

data packets will travel through these layers.
10. Name the two models shown:
Review

10. Name the two models shown:
11. PDU stands for _______ ______ _____. A PDU consists of,

- Data
- S_______
- Packet
- F_______
- Bits
Review

11. PDU stands for Packet Data Unit. A PDU consists of,

- Data
- Segment
- Packet
- Frame
- Bits
Data Encapsulation

OSI PDUs

12. During data encapsulation, headers are added to the previous data.

Segment = _______ header + data
Packet = _______ header + segment
Frame = _______ header + packet
Frame = set of _______
OSI PDUs

12. During data encapsulation, headers are added to the previous data.

Segment = transport header + data
Packet = network header + segment
Frame = frame header + packet
Frame = set of bits
Review

13. During protocol encapsulation for TCP/IP model, protocol headers of each layer are added to the data.

TCP segment = User Data + _____ header
IP Packet = TCP segment + _____ header
Ethernet Frame = IP packet + _______ header
Review

13. During protocol encapsulation for TCP/IP model, protocol headers of each layer are added to the data.

TCP segment = User Data + TCP header
IP Packet = TCP segment + IP header
Ethernet Frame = IP packet + Ethernet header
Review

14. A **media access control address (MAC address)** is the ______ address of a computer.

It is a **unique identifier** assigned to devices in a network segment. Using this address, data can reach the intended __________.
Review

14. A **media access control address (MAC address)** is the physical address of a computer.

It is a **unique identifier** assigned to devices in a network segment. Using this address, data can reach the intended Destination.
Review

15. In a TCP/IP network, the ______ is a router.

All data must pass this gateway to reach its network.
Review

15. In a TCP/IP network, the gateway is a router.

All data must pass this gateway to reach its network.
Review

16. One router controls _______ for one network. _______ can be sent from one network to another network.
Review

16. One router controls traffic for one network. Data can be sent from one network to another network.
END OF REVIEW