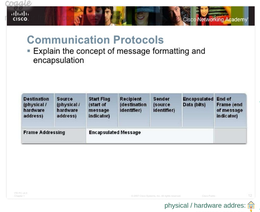
Chapter 3 Network Protocols and Communications



The frame has a source and destination in both the frame addressing portion and in the **encapsulated message**.

physical / hardware address:

recipient/sender:

1. Communication fundamentals

Prior to communicating, they must *agree* on how to communicate:
- If the communication is using voice, they must first*agree on the language*.
- Next, when they have a message to share, they must be able to*format* that message in a way that is understandable.

For example, if someone uses the English language, but poor sentence structure, the message can easily be misunderstood.

Communication begins with a message, that must be sent from a source to a destination. The sending of this message is governed by *rules* called **Protocols**.

All communication methods have three elements in common
- Sender or message **source**
- Receiver or **destination**
- **Channel** or media

2. The rules

Message Encoding: It is the process of converting information into another acceptable form, for transmission in the medium.
Decoding reverses this process in order to interpret the information

After **formatting** (**encoding**) a message, the message must be placed inside another message (**encapsulation**).

Just as a letter is encapsulated in an envelope for delivery:

Rule Establishment: Before communicating with one another, individuals must use established rules or agreements to govern the conversation.

Each computer message is encapsulated in a specific format, called a **frame**, *before it is sent over the network*. A frame acts like an envelope

3. Rules that Govern Communications

A protocol stack shows how the individual protocols within a suite are implemented. The protocols are viewed in terms of **layers**

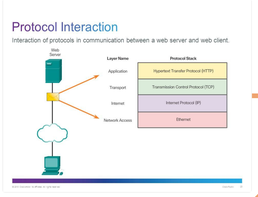
A ways to visualize how the protocols within a suite interact is to view the interaction as a **stack**.

A group of inter-related protocols necessary to perform a communication function is called a **Protocol Suite**.

4. Network Protocols

Networking protocols define a common format and set of rules for exchanging messages between devices

5. Protocol Interaction



HTTP: is an application protocol that *governs the way a web server and a web client interact.* It defines the content and formatting of the requests and responses

TCP: is the transport protocol that*manages the individual conversations.* TCP divides the HTTP messages into *smaller pieces*, called **segments**. TCP is also responsible for controlling the size and rate

IP - is responsible for taking the formatted segments from TCP, *encapsulating them into packets*, assigning them the appropriate addresses, and delivering them to the destination host.

Ethernet - is a network access protocol: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for *taking the packets from IP and formatting them to be transmitted over the media.*

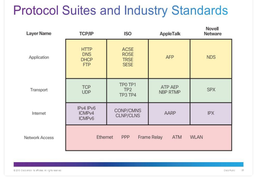
Communication between a web server and web client is an example of an interaction between several protocols.

6. Protocol Suites and Industry Standards

The use of standards in developing and implementing protocols ensures that products from different manufacturers can interoperate successfully.

The **TCP/IP** protocol suite is an open standard

A **protocol suite** is a set of protocols that work together to provide comprehensive network communication services.



7. Open Standards

They guarantee that no single company can monopolize the market, or have an unfair advantage over its competition.

Open standards encourage interoperability, competition, and innovation.

Other standard organizations have responsibilities for promoting and creating the electronic and communication standards used to deliver the IP packets as electronic signals over a wired or wireless medium.

Institute of Electrical and Electronics Engineers (**IEEE**, pronounced "I-triple-E") – Organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking. **802.X**

Electronic Industries Alliance (**EIA**) - Best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment. **EIA/TIA 568-B**

Telecommunications Industry Association (**TIA**) - Responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more. Figure 2 shows an example of an Ethernet cable meeting TIA/EIA standards.

International Telecommunications Union-Telecommunication Standardization Sector (**ITU-T**) - One of the largest and oldest communication standard organizations. The ITU-T defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

Standards organizations are important in maintaining an open Internet with freely accessible specifications and protocols that can be implemented by any vendor: **IEEE, IETF, IANA, ICANN, ITU, TIA**

Internet Society (**ISOC**) – Responsible for promoting the open development and evolution of Internet use throughout the world.

Internet Architecture Board (**IAB**) - Responsible for the overall management and development of Internet standards.

Internet Engineering Task Force (**IETF**) - Develops, updates, and maintains Internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols know as Request for Comments (RFC) documents.

Internet Research Task Force (**IRTF**) - Focused on long-term research related to Internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).

Internet Corporation for Assigned Names and Numbers (**ICANN**) - Based in the United States, coordinates IP address allocation, the management of domain names, and assignment of other information used TCP/IP protocols.

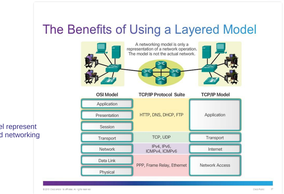
Internet Assigned Numbers Authority (**IANA**) - Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

8.The Benefits of Using a Layered Model

Protocol model - This model closely matches the structure of a particular protocol suite. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

Reference model - This model provides consistency within all types of network protocols and services by describing what has to be done at a particular layer, but not prescribing how it should be accomplished. The OSI model is a widely known internetwork reference model, but is also a protocol model for the OSI protocol suite.

TCP/IP and OSI model represent a basic type of layered networking models



9. The OSI Reference Model

7. Application: Contain protocols used for process-to process communications

6. Presentation: Provides a common representation of data transferred between application layer services

5. Session: Provides services to the presentation layer to organize its dialogue and to manage data exchange

4. Transport: Defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

3. Network: Provides services to exchange the individual of data over the network between identified end devices.

2. Data link: This layer describe methods for exchanging data frames between devices over a common media

1. Physical: This layers describe the mechanical, electrical, functional, and procedural means to active, maintain, and de-activate physical connections for bit transmission to and from a network device

Assisting in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.

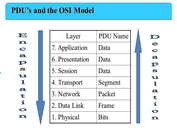
Fostering competition because products from different vendors can work together.

Preventing technology or capability changes in one layer from **affecting** other layers above and below.

Providing a **common language** to describe networking functions and capabilities.

10. Data encapsulation

The form that a piece of data takes at any layer is called a protocol data unit (**PDU**)



Multiplexing: Sending small individual pieces from many different senders by interleaving the segments

Segmentation: breaking communication into pieces

Segmentation can increase the efficiency of network communications. If part of the message fails to make it to the destination, due to failure in the network or network congestion, only the missing parts need to be retransmitted.

11. Network Addresses

The network and data link layers are responsible for delivering the data from the source device to the destination device.

Protocols at both layers contain a source and destination address, but their addresses have different purposes.

Network layer source and destination addresses – Responsible for delivering the IP packet from the original source to the final destination, **either on the same network or to a remote network.**

An **IP address** is the network layer, or Layer 3, **logical address** used to deliver the IP packet

An IP address **contains two parts**

Network portion – The left-most part of the address that indicates which network the IP address is a member.

The **subnet mask** is used to identify the network portion of an address from the host portion.

All devices on the same network will have the **same network portion** of the address.

Host portion – The remaining part of the address that identifies a specific device on the network.

The host portion is unique for each device on the network.

e.g. ip add: 192.168.0.3 /24
/23 = subnet mask = 24 bits of network portion= 11111111.11111111.11111111.00000000

192.168.0.3 = 11000000.10101000.00000000.00000011
The first 24 bits of the ip address are equal to the network portion: 11000000.10101000.00000000.00000011 = 192.168.0.0

the rest of the bits are for the host portion: 8 bits for host portion

Data link layer source and destination addresses – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC **on the same network.**

A Media Access Control (**MAC) address** or physical address (data link address) is the address of the device's NIC.

A MAC address is composed of 6 hexadecimal numbers separated bya dash, where each number has a length of 8 bits (2 hex characters): 00-11-22-33-44-AA-BB-CC-DD, the first 4 numbers represent the brand of the NIC.

MAC addresses are physically embedded on the Ethernet NIC

Message Delivery Options

Unicast: A one-to-one delivery ( )

Multicasting is the delivery of the same message to a group of host destinations, one-to-many. ( )

Broadcasting represents a one-to-all message delivery option ( )

Message Timing

Access Method: Determines when someone is able to send a message. Hosts on a network need an access method to know when to begin sending messages and how to respond when collisions occur.

Flow control: source and destination hosts negotiate how much information can be sent and the speed that it can be delivered.

Response Timeout: Hosts on the network have rules that specify how long to wait for responses and what action to take if a response timeout occurs

Message size

When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences.

The size restrictions of frames require the source host to break a long message into individual pieces that **meet both the minimum and maximum size requirements**

At the receiving host, the individual pieces of the **message are reconstructed** into the original message.