



Jaringan Komputer (CCNA-1)

#3 Network Protocols and Communications

Susmini I. Lestaringati, M.T

Upon completion of this chapter you will be able to:

- Explain why protocols are necessary in communication.
- Explain the purpose of adhering to a protocol suite.
- Explain the role of standards organizations in establishing protocols for network interoperability.
- Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
- Explain why RFCs became the process for establishing standards.
- Describe the RFC process.
- Explain how data encapsulation allows data to be transported across the network.
- Explain how local hosts access local resources on a network.
- Explain how local hosts access remote resources on a network.



Network Protocols and Standards make network communication easier.

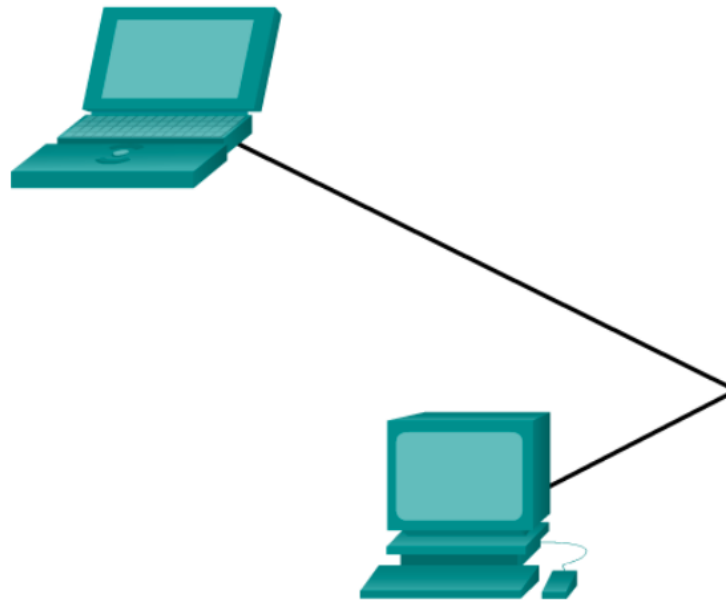
3.1. Rules of Communication

- **Human Communication**



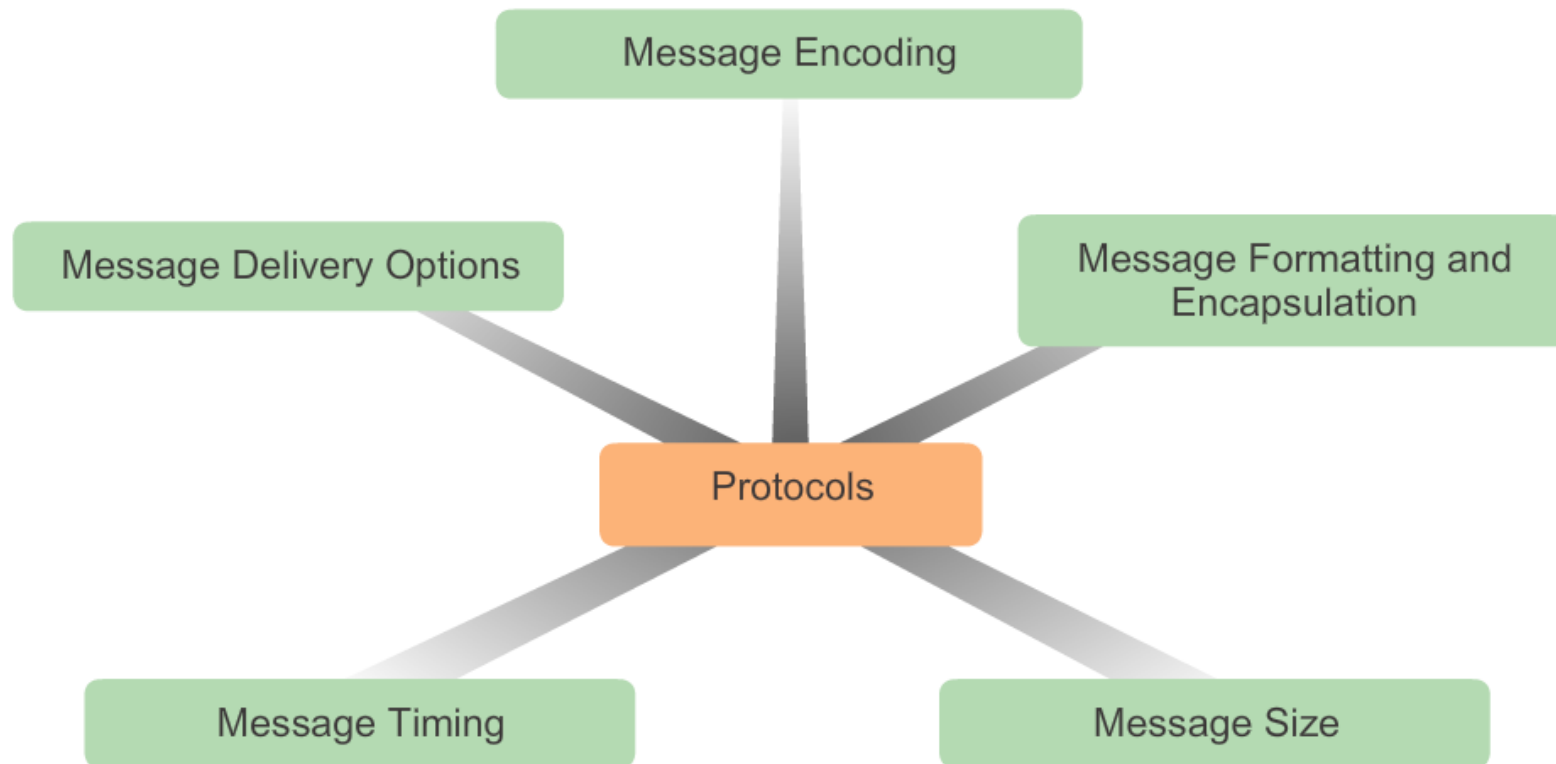
Rules of Communication

- **Computer Communication**



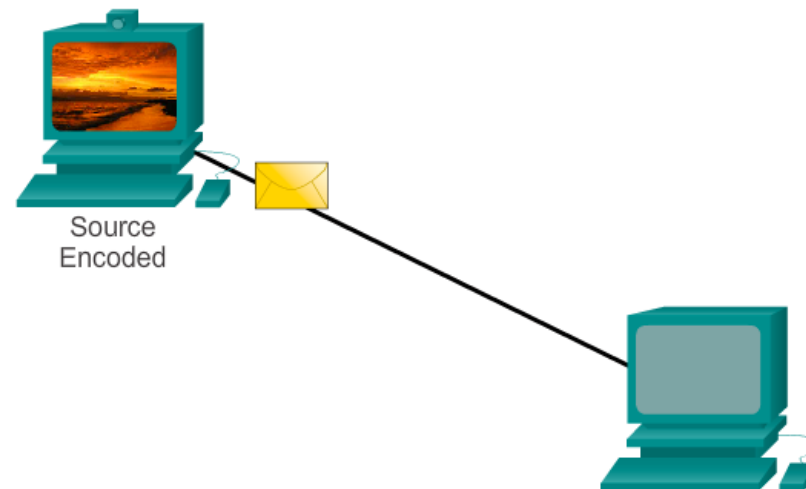
Rules of Communication

- Before communicating with one another, individuals must use established rules or agreements to govern the conversation.
- The protocols used are specific to the characteristics of the communication method, including the characteristics of the source, destination and channel. These rules, or protocols, must be followed in order for the message to be successfully delivered and understood.
- The protocols put in place must account for the following requirements:
 - An identified sender and receiver
 - Common language and grammar
 - Speed and timing of delivery
 - Confirmation or acknowledgement requirements



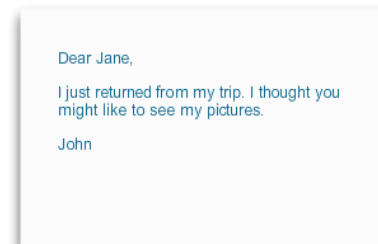
Message Encoding


- One of the first steps to sending a message is encoding it. Encoding is the process of converting information into another, acceptable form, for transmission. Decoding reverses this process in order to interpret the information.



Message Formatting and Encapsulation

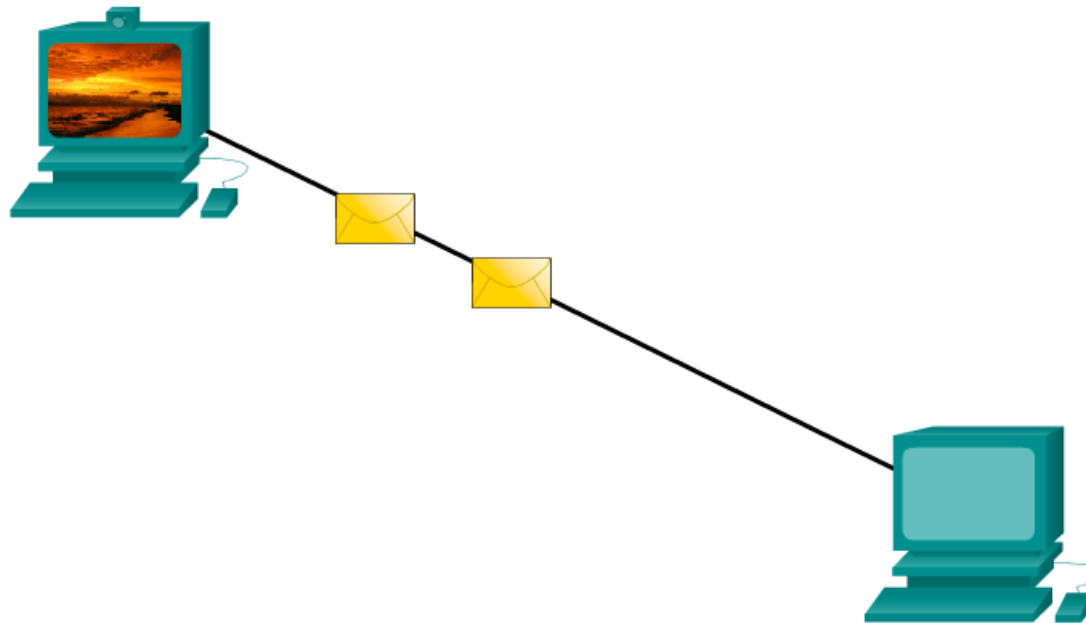
- When a message is sent from source to destination, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.



Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

Message Size

- When a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces, as shown in Figure 2. The rules that govern the size of the pieces, or frames, communicated across the network are very strict. They can also be different, depending on the channel used. Frames that are too long or too short are not delivered.



Message Timing

- **Message Timing**

Another factor that affects how well a message is received and understood is timing. People use timing to determine when to speak, how fast or slow to talk, and how long to wait for a response. These are the rules of engagement.

- **Access Method**

Access method determines when someone is able to send a message. These timing rules are based on the environment. For example, you may be able to speak whenever you have something to say. In this environment, a person must wait until no one else is talking before speaking. If two people talk at the same time, a collision of information occurs and it is necessary for the two to back off and start again, as shown in Figure 1. Likewise, 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.

- **Access Method**

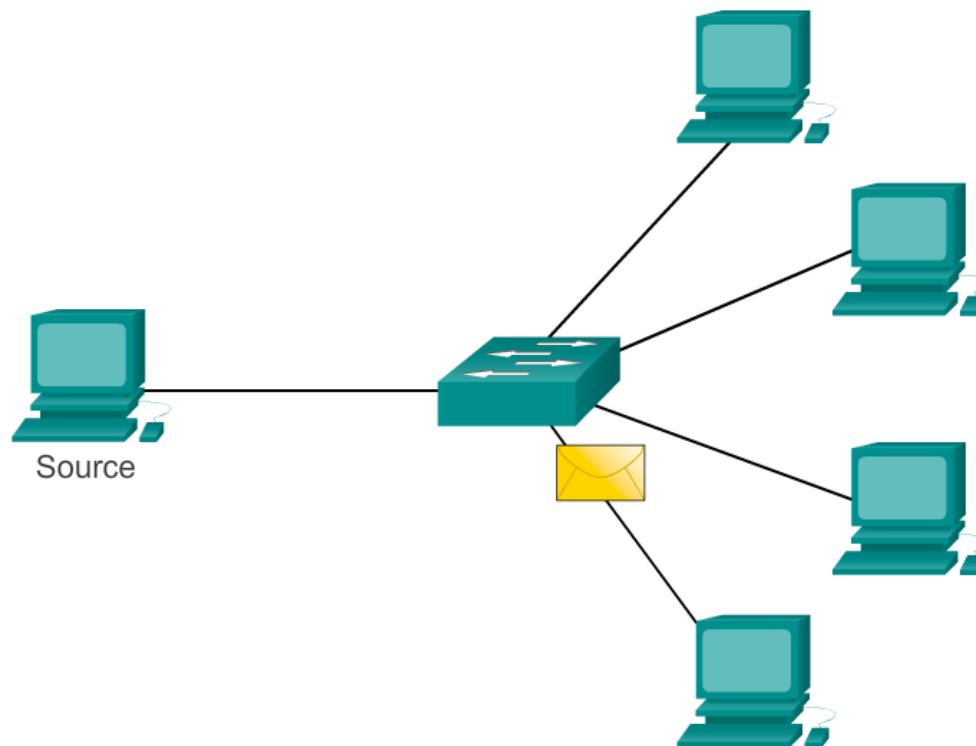
Access method determines when someone is able to send a message. These timing rules are based on the environment. For example, you may be able to speak whenever you have something to say. In this environment, a person must wait until no one else is talking before speaking. If two people talk at the same time, a collision of information occurs and it is necessary for the two to back off and start again, as shown in Figure 1. Likewise, 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.

- **Response Timeout**

If a person asks a question and does not hear a response within an acceptable amount of time, the person assumes that no answer is coming and reacts accordingly, as shown in Figure 3. The person may repeat the question, or may go on with the conversation. Hosts on the network also have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

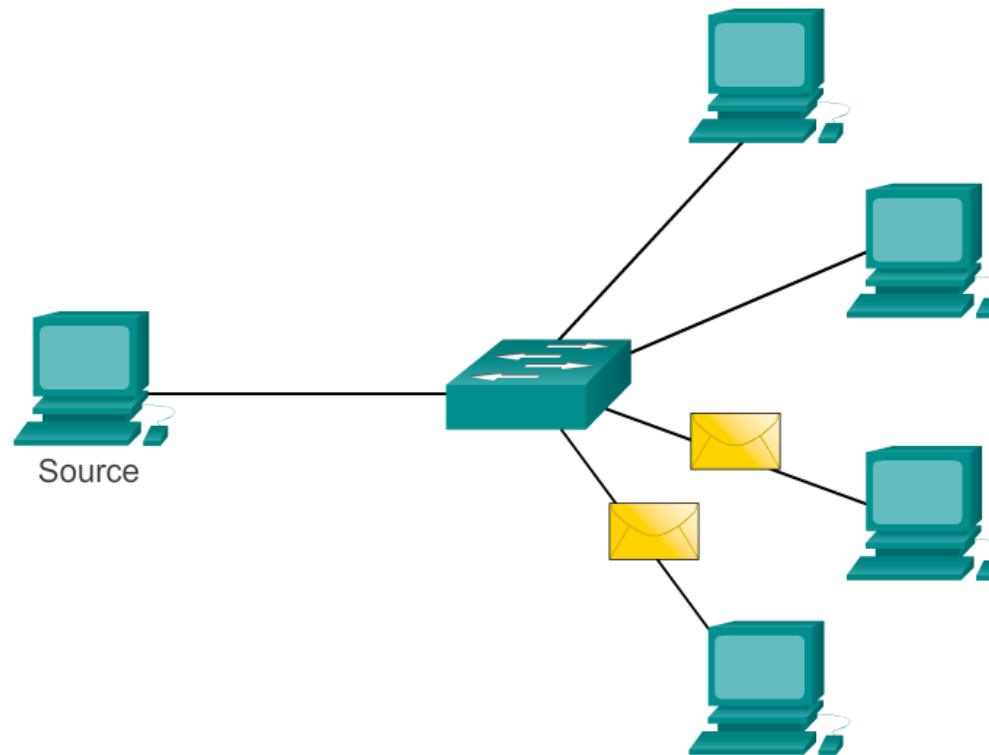
Message Delivery Option (1)

- A one-to-one delivery option is referred to as a **unicast**, meaning that there is only a single destination for the message.



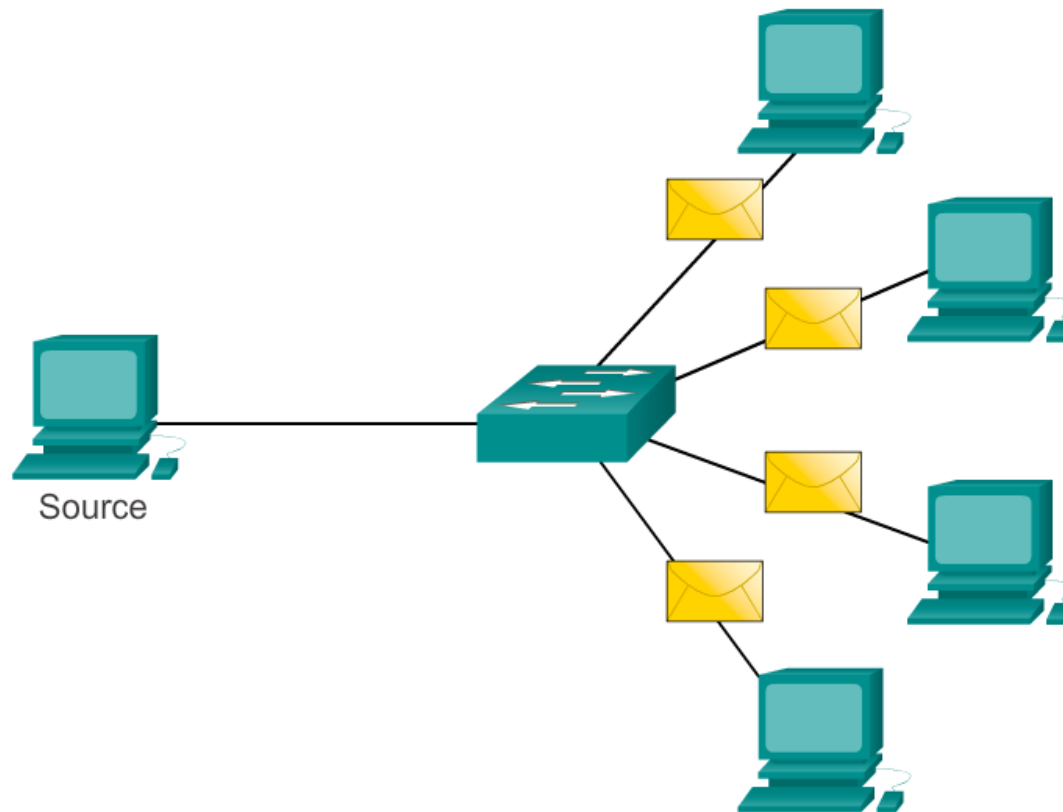
Message Delivery Option (2)

- When a host needs to send messages using a one-to-many delivery option, it is referred to as a **multicast**.
- Multicasting is the delivery of the same message to a group of host destinations simultaneously.



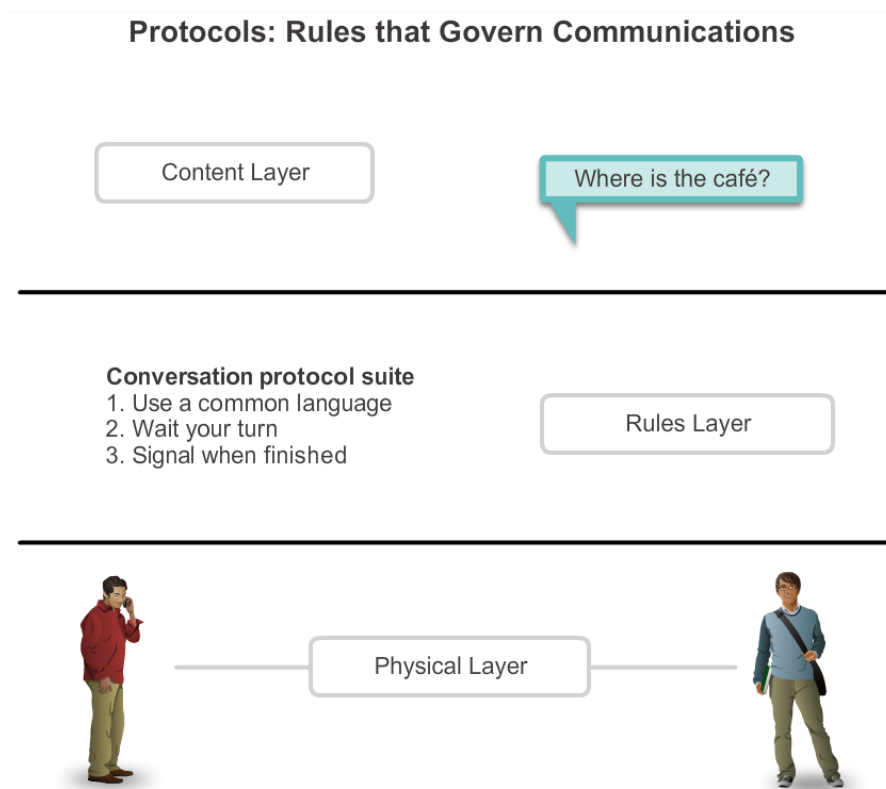
Message Delivery Option (3)

- If all hosts on the network need to receive the message at the same time, a broadcast is used.
- Broadcasting represents a one-to-all message delivery option.



3.2. Network Protocols and Standards

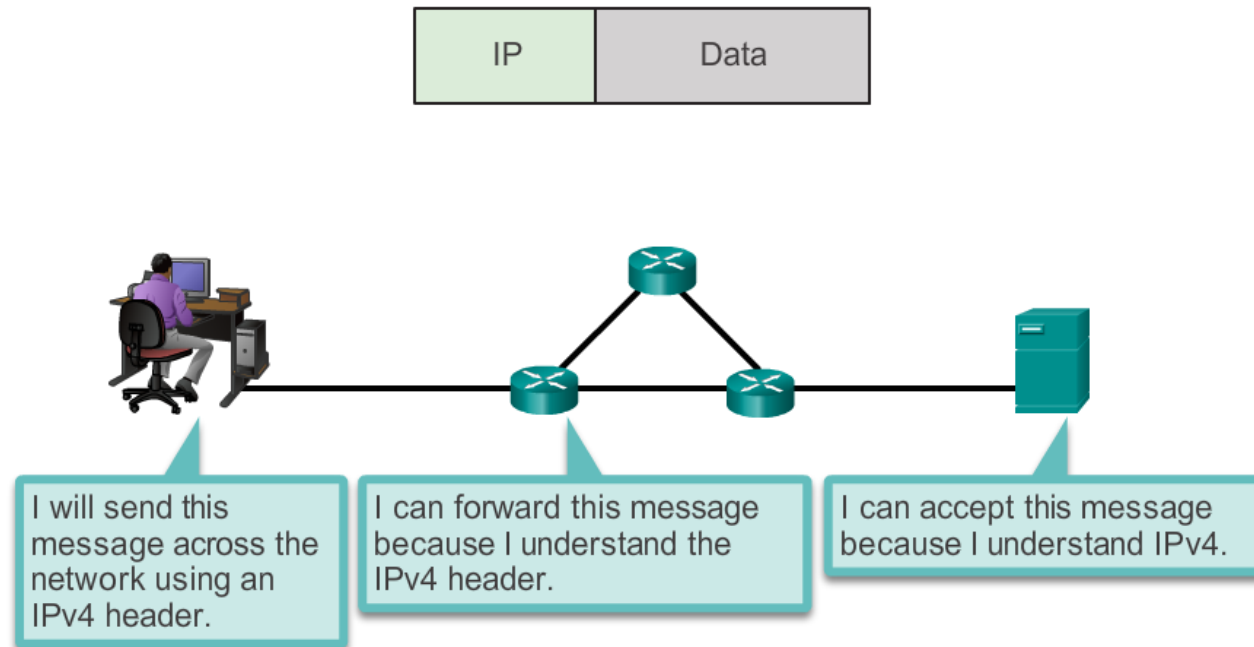
- Just like in human communication, the various network and computer protocols must be able to interact and work together for network communication to be successful. A group of inter-related protocols necessary to perform a communication function is called a protocol suite.
- Protocol suites are implemented by hosts and networking devices in software, hardware or both.



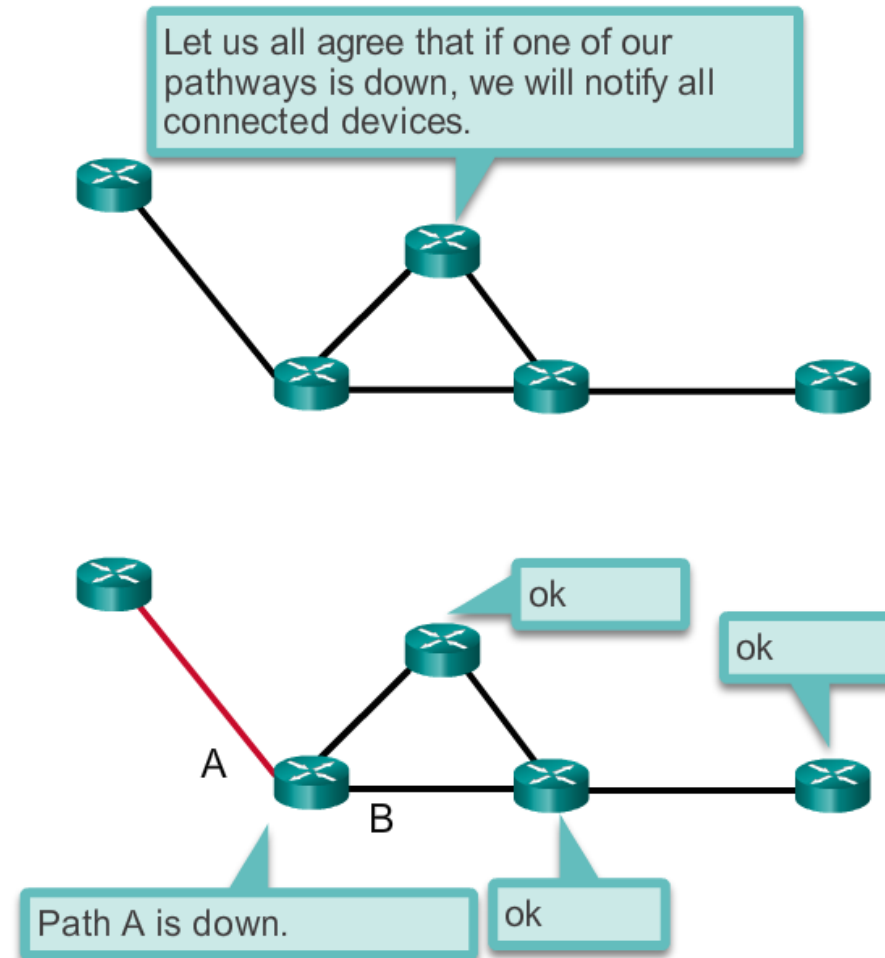
Protocol suites are sets of rules that work together to help solve a problem.

3.2.1 Protocols

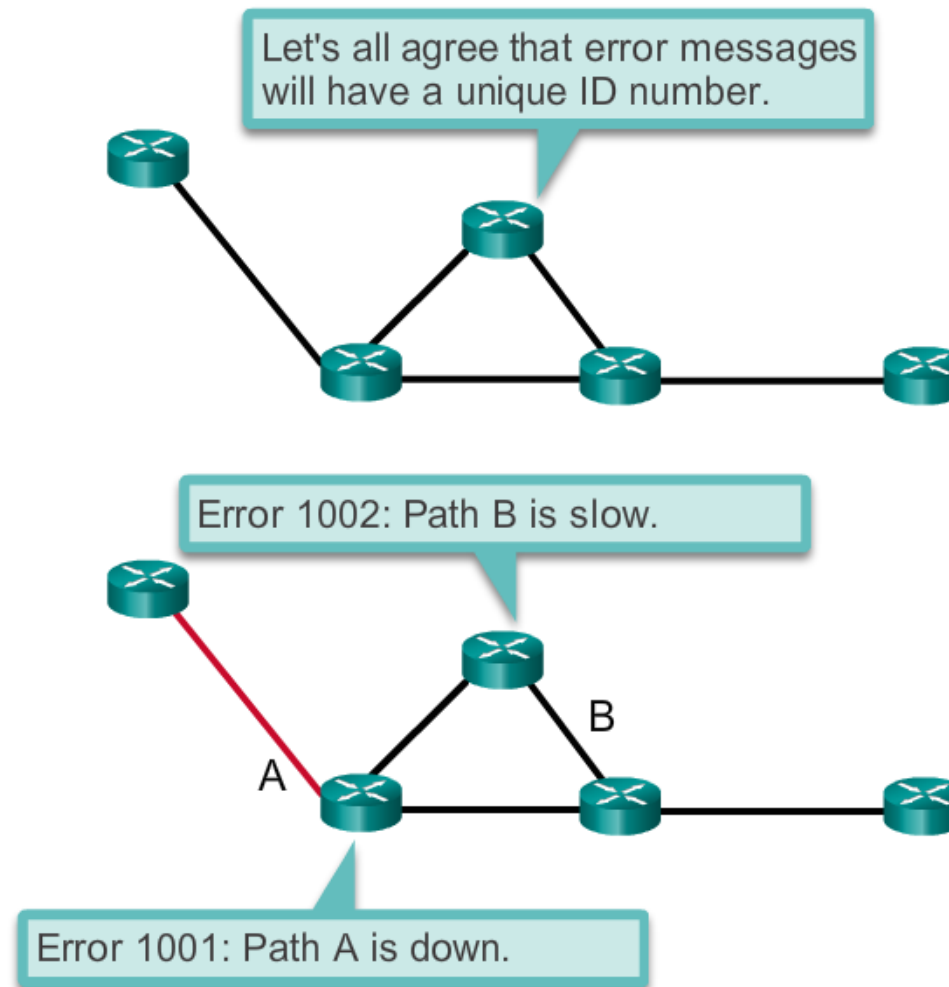
- For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. Networking protocols define a common format and set of rules for exchanging messages between devices.
- The figures illustrate networking protocols that describe the following processes:
 - How the message is formatted or structured, as shown in Figure 1



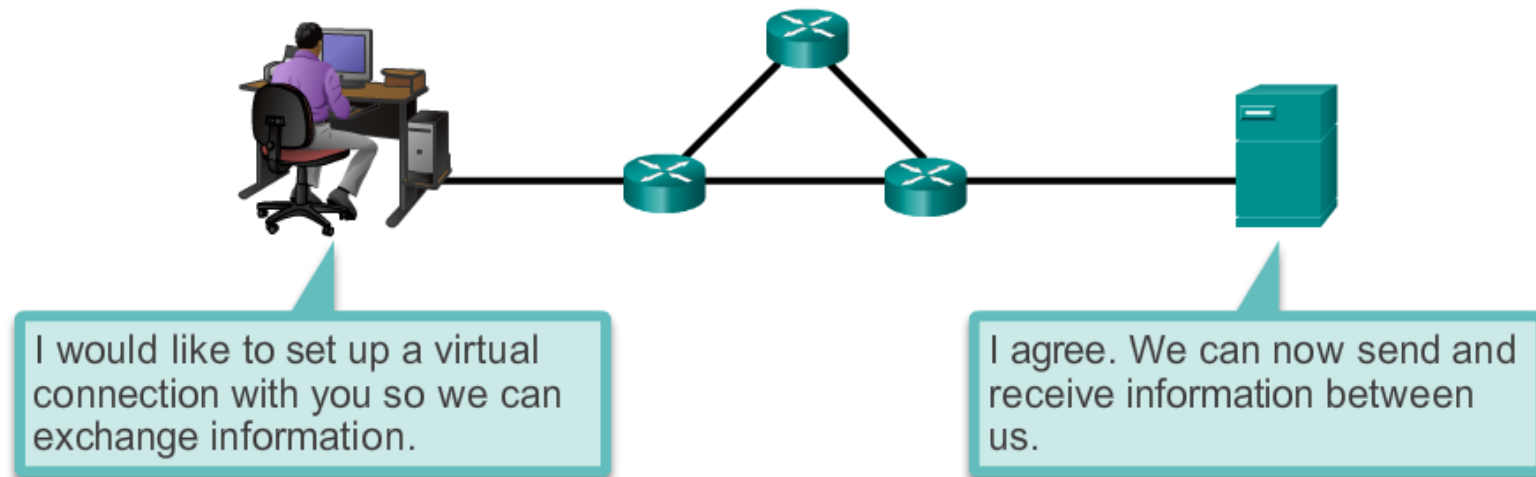
- The process by which networking devices share information about pathways with other networks, as shown in Figure 2



- How and when error and system messages are passed between devices, as shown in Figure 3

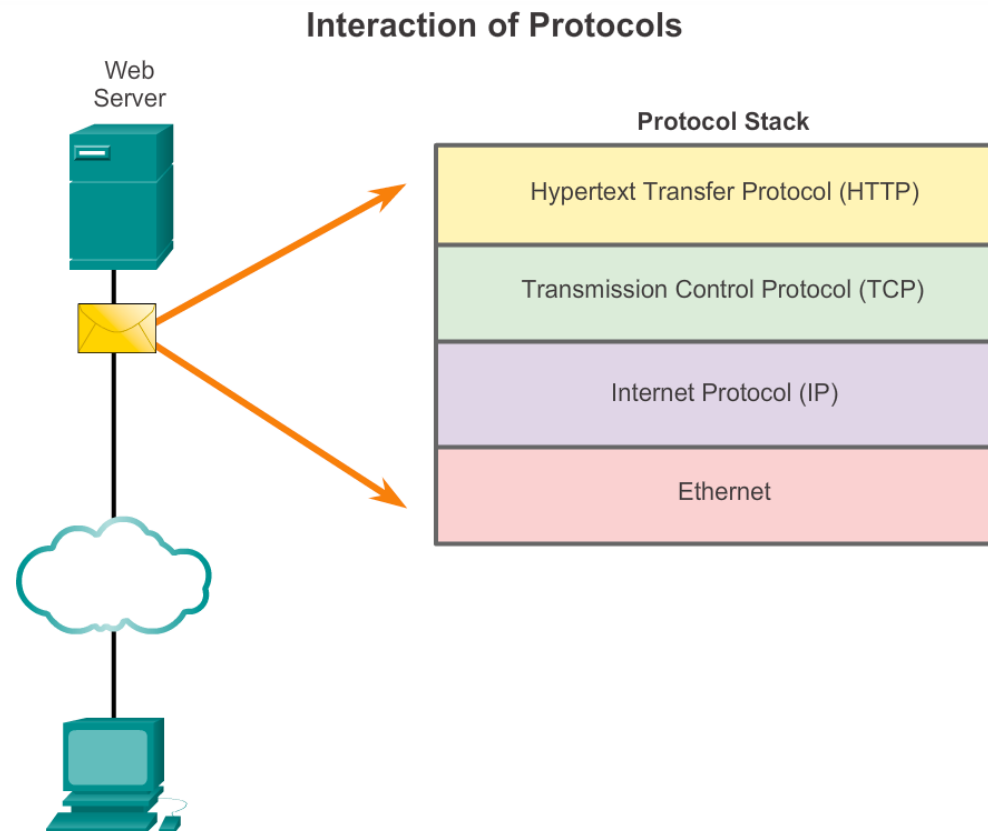


- The setup and termination of data transfer sessions, as shown in Figure 4



Interaction of Protocols

- An example of using the protocol suite in network communications is the interaction between a web server and a web client. This interaction uses a number of protocols and standards in the process of exchanging information between them. The different protocols work together to ensure that the messages are received and understood by both parties.



3.2.2. Protocol Suites

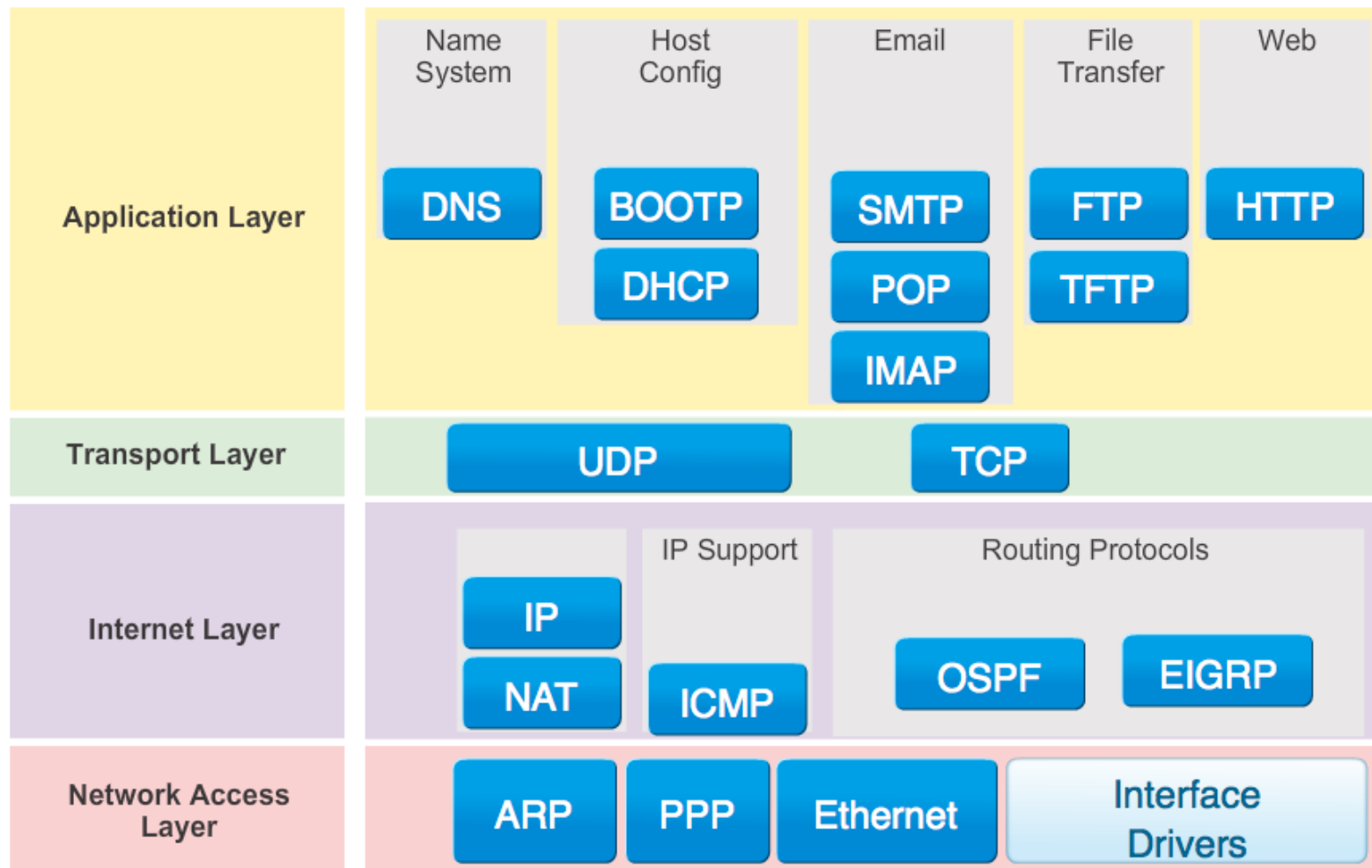
- A protocol suite is a set of protocols that work together to provide comprehensive network communication services. A protocol suite may be specified by a standards organization or developed by a vendor.
- The protocols IP, HTTP, and DHCP are all part of the Internet protocol suite known as Transmission Control Protocol/IP (TCP/IP). The TCP/IP protocol suite is an open standard, meaning these protocols are freely available to the public, and any vendor is able to implement these protocols on their hardware or in their software.

Protocol Suites and Industry Standards

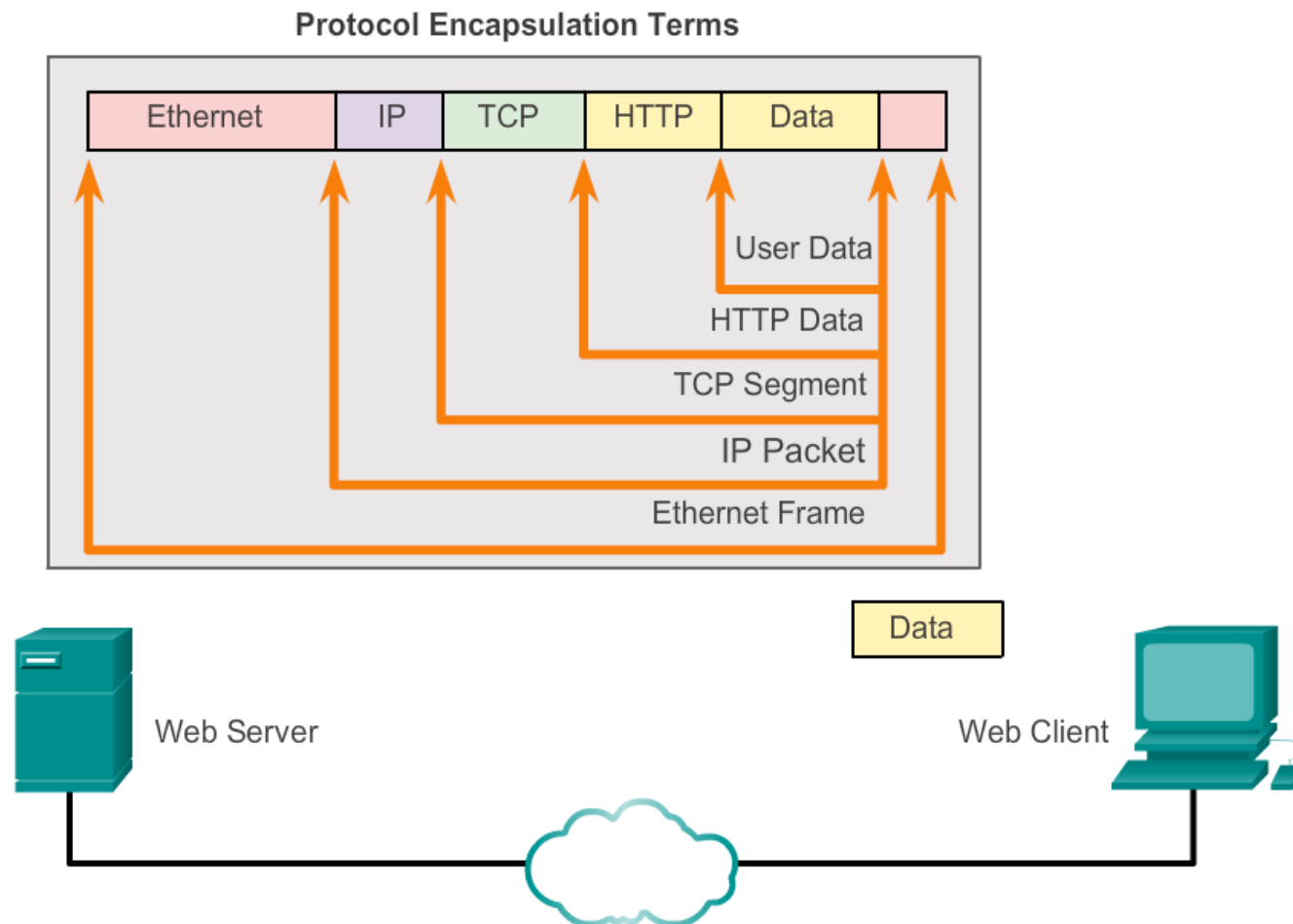
TCP/IP	ISO	AppleTalk	Novell Netware
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Ethernet PPP Frame Relay ATM WLAN			

TCP/IP Protocol Suite and Communication Process

TCP/IP Protocol Suite and Communication Process



Protocol Operation of Sending and Receiving a Message

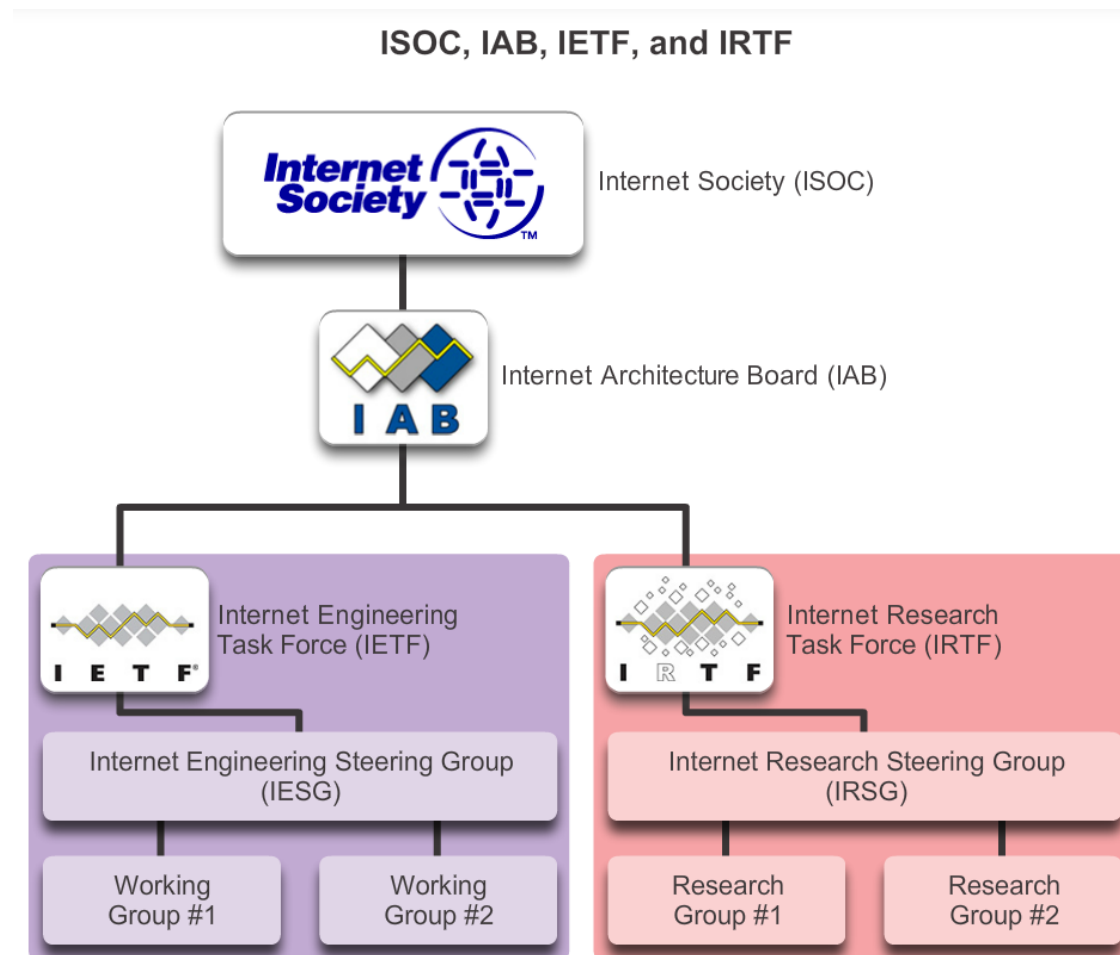


3.2.3. Standards Organisations

- Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards.
- Standards organizations include:
 - The Internet Society (ISOC)
 - The Internet Architecture Board (IAB)
 - The Internet Engineering Task Force (IETF)
 - The Institute of Electrical and Electronics Engineers (IEEE)
 - The International Organization for Standardization (ISO)



ISOC, IAB and IETF



- **The Internet Society (ISOC)** is responsible for promoting open development, evolution, and Internet use throughout the world. ISOC facilitates the open development of standards and protocols for the technical infrastructure of the Internet, including the oversight of the Internet Architecture Board (IAB).
- **The Internet Architecture Board (IAB)** is responsible for the overall management and development of Internet standards. The IAB provides oversight of the architecture for protocols and procedures used by the Internet. The IAB consists of 13 members, including the chair of the Internet Engineering Task Force (IETF). IAB members serve as individuals and not representatives of any company, agency, or other organization.
- The IETF's mission is to develop, update, and maintain Internet and TCP/IP technologies. One of the key responsibilities of the IETF is to produce Request for Comments (RFC) documents, which are a memorandum describing protocols, processes, and technologies for the Internet. The IETF consists of working groups (WGs), the primary mechanism for developing IETF specifications and guidelines. WGs are short term, and after the objectives of the group are met, the WG is terminated. The Internet Engineering Steering Group (IESG) is responsible for the technical management of the IETF and the Internet standards process.
- **The Internet Research Task Force (IRTF)** is focused on long-term research related to Internet and TCP/IP protocols, applications, architecture, and technologies. While the IETF focuses on shorter-term issues of creating standards, the IRTF consists of research groups for long-term development efforts. Some of the current research groups include Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), Peer-to-Peer Research Group (P2PRG), and Router Research Group (RRG).

IEEE

- The Institute of Electrical and Electronics Engineers (IEEE, pronounced “I-triple-E”) is a professional organization for those in the electrical engineering and electronics fields who are dedicated to advancing technological innovation and creating standards.

IEEE 802 Working Groups and Study Groups

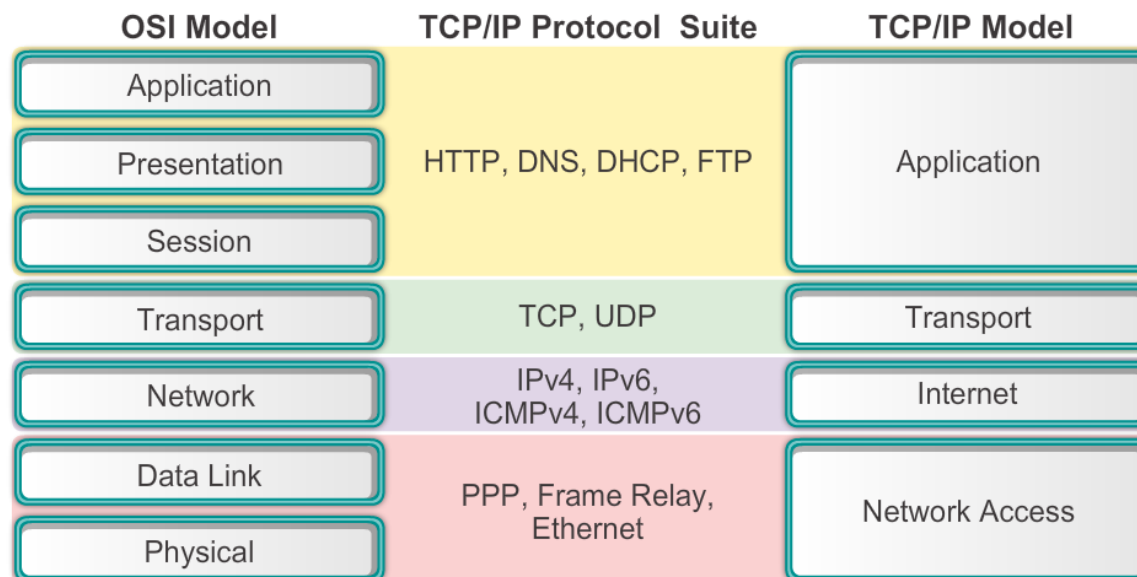
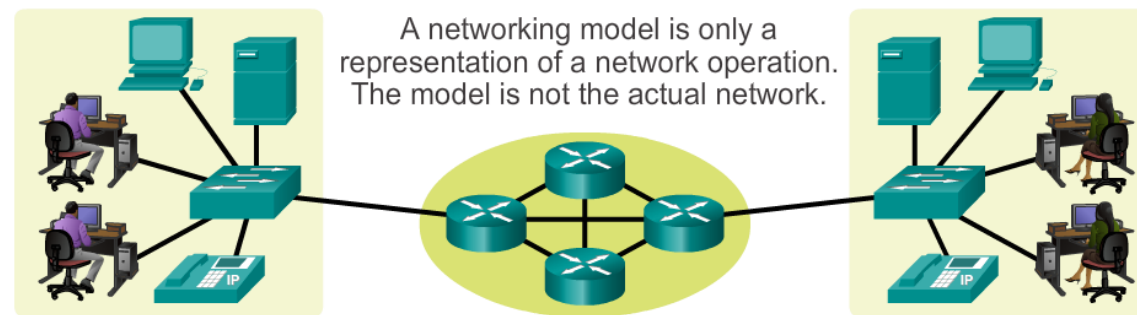
- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
-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

Other Standards Organisations

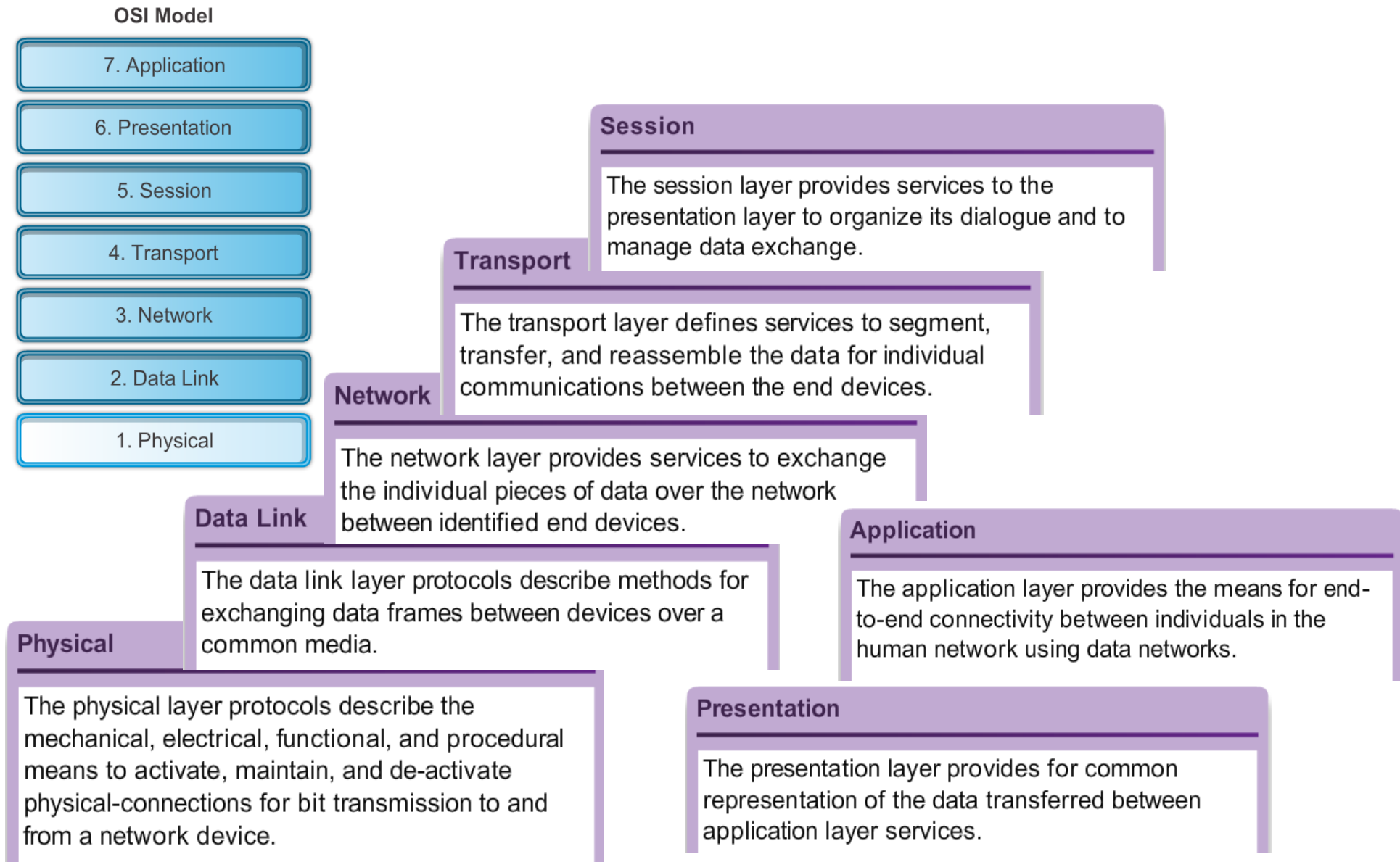
- Networking standards involve several other standards organizations. Some of the more common ones are:
 - **EIA** - The Electronic Industries Alliance (EIA), previously known as the Electronics Industries Association, is an international standards and trade organization for electronics organizations. The EIA is best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
 - **TIA** - The Telecommunications Industry Association (TIA) is responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more. Many of their standards are produced in collaboration with the EIA.
 - **ITU-T** - The International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) is 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). For example, when dialing another country, ITU country codes are used to make the connection.
 - **ICANN** - The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization based in the United States that coordinates IP address allocation, the management of domain names used by DNS, and the protocol identifiers or port numbers used by TCP and UDP protocols. ICANN creates policies and has overall responsibility for these assignments.
 - **IANA** - The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

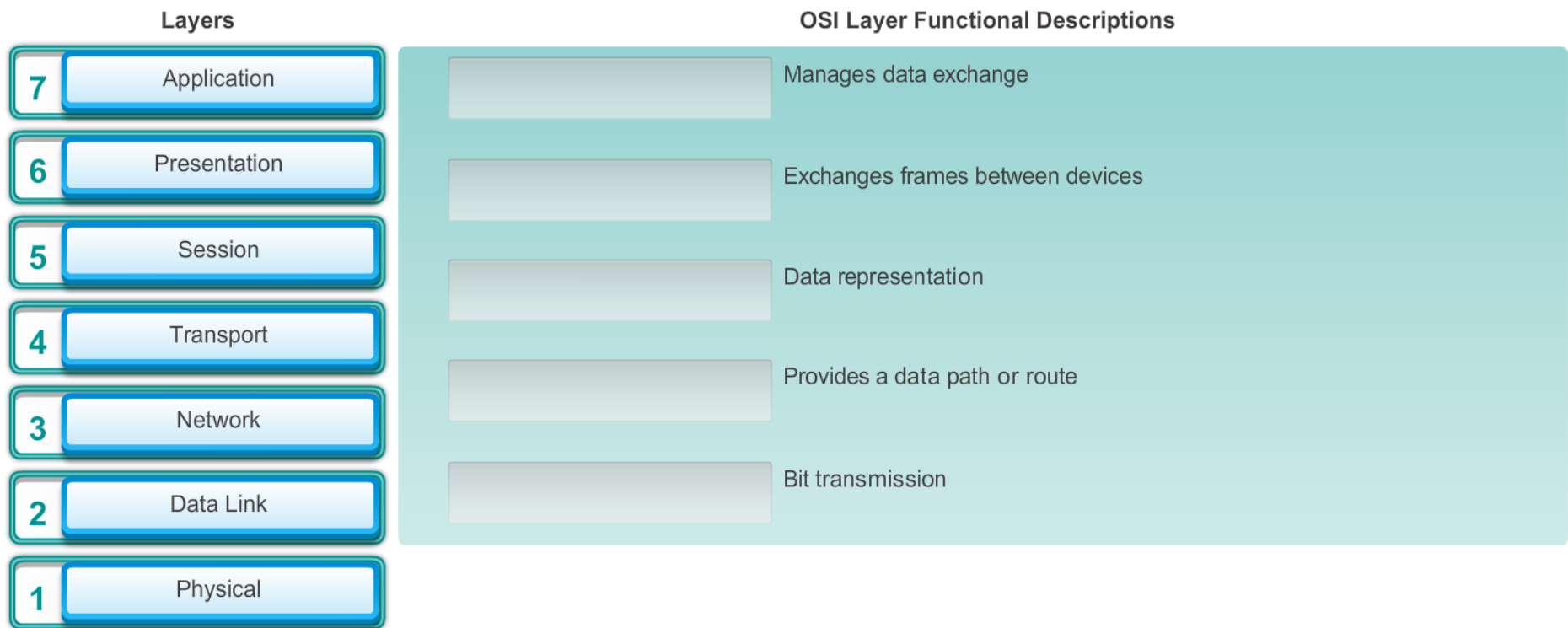
3.2.4. Reference Models

- The OSI model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

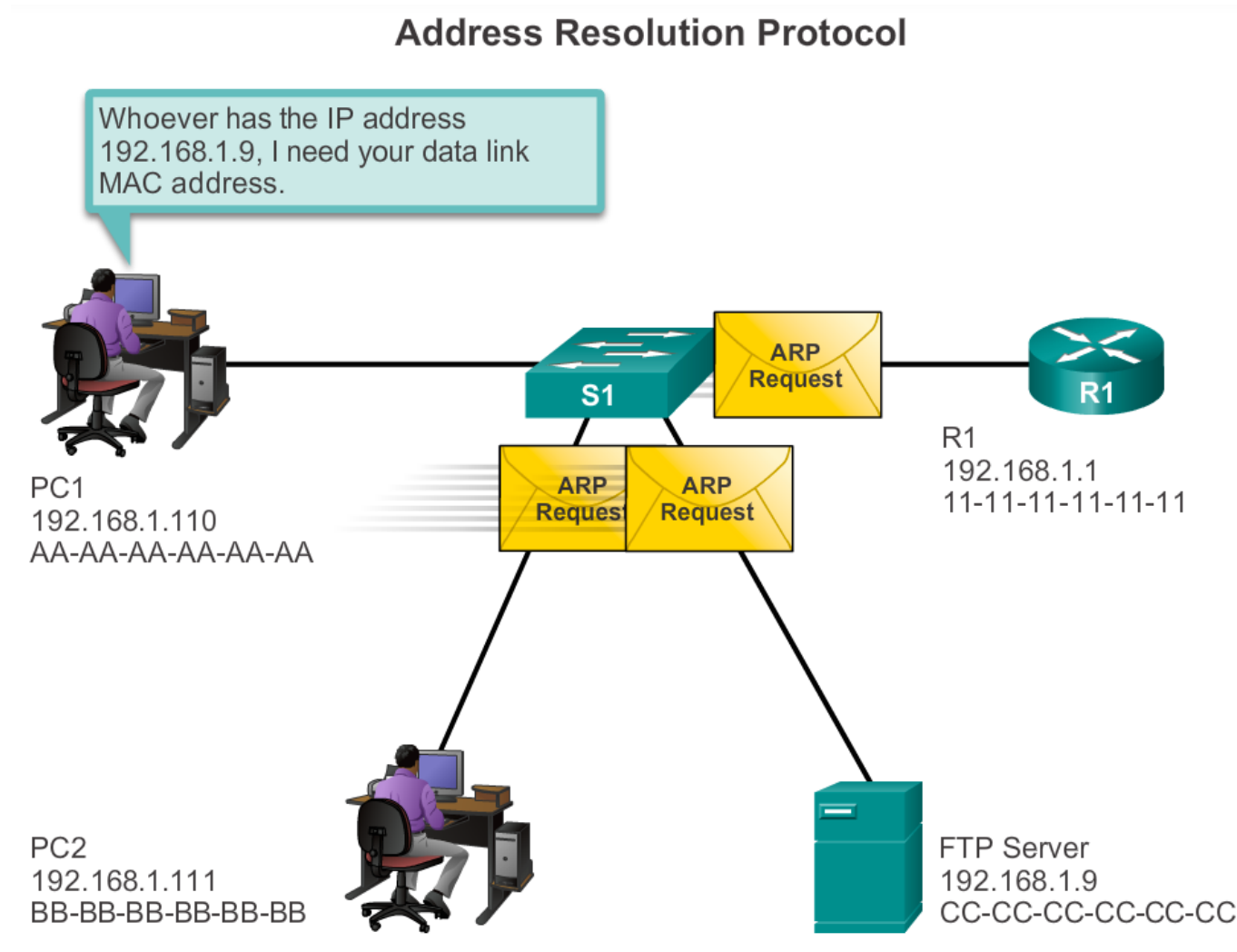


OSI Reference Model

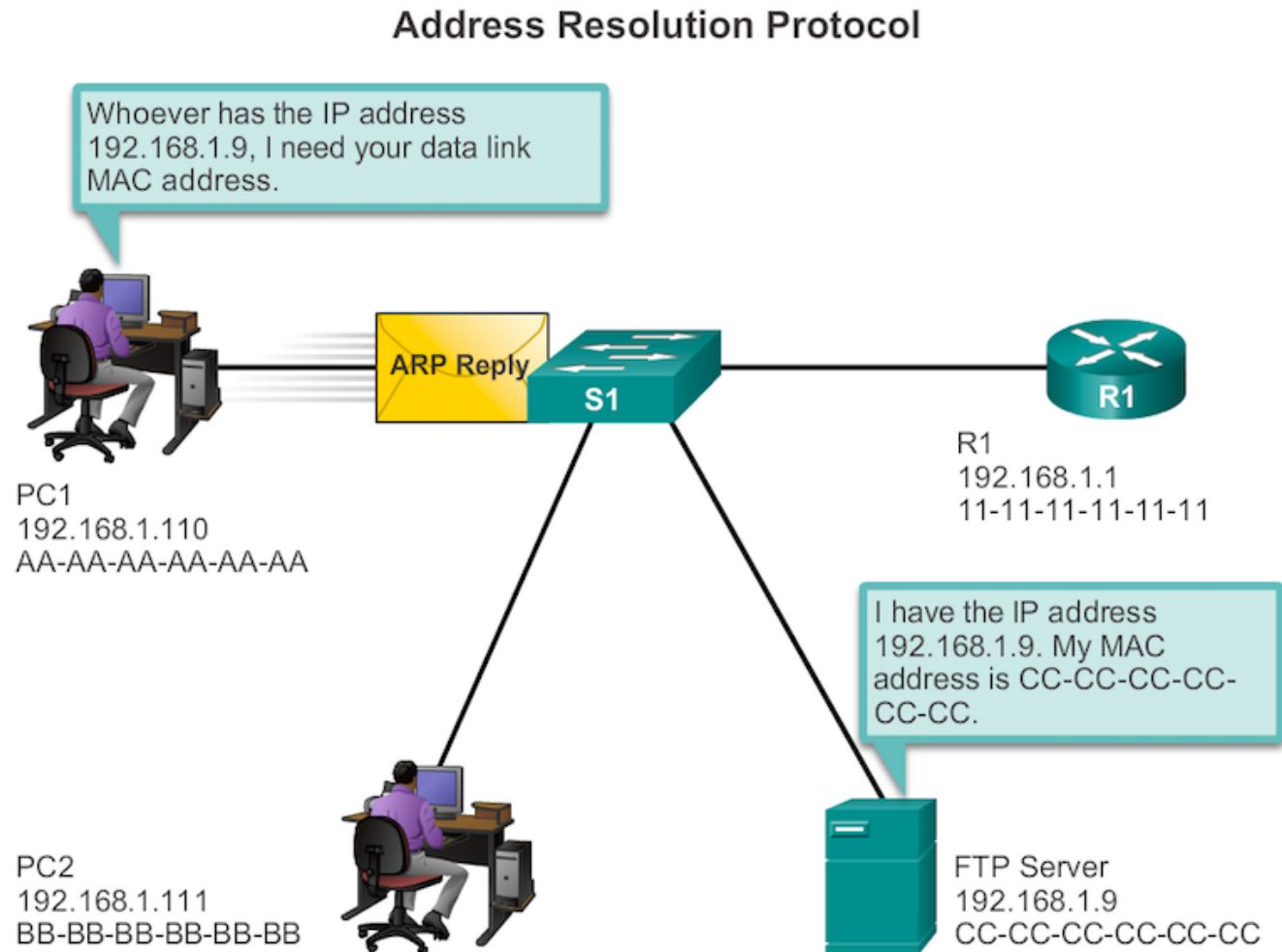




MAC and IP Address (1)



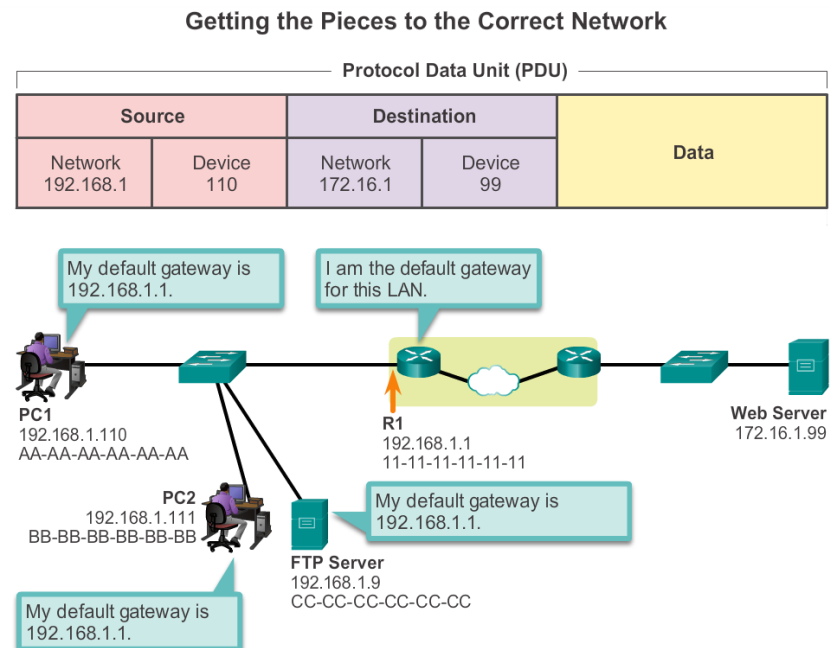
MAC and IP Address (2)



3.3.3. Accessing Remote Resources

Default Gateway

- When a host needs to send a message to a remote network, it must use the router, also known as the default gateway. The default gateway is the IP address of an interface on a router on the same network as the sending host.
- It is important that the address of the default gateway be configured on each host on the local network. If no default gateway address is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered.



Network Addresses

- IP addresses indicate the network and device addresses of the source and destination. When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.
 - Source IP address - The IP address of the sending device, the client computer PC1: 192.168.1.110.
 - Destination IP address - The IP address of the receiving device, the server, Web Server: 172.16.1.99.

