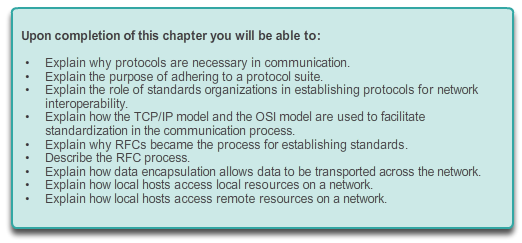
**Chapter 3: Network Protocols and Communications**

**Chapter 3: Network Protocols and Communications**



**Network Protocols and Communications**

**Introduction**

More and more, it is networks that connect us. People communicate online from everywhere. Conversations in classrooms spill into instant message chat sessions, and online debates continue at school. New services are being developed daily to take advantage of the network.

Rather than developing unique and separate systems for the delivery of each new service, the network industry as a whole has adopted a developmental framework that allows designers to understand current network platforms, and maintain them. At the same time, this framework is used to facilitate the development of new technologies to support future communications needs and technology enhancements.

Central to this developmental framework, is the use of generally-accepted models that describe network rules and functions.

Within this chapter, you will learn about these models, as well as the standards that make networks work, and how communication occurs over a network.

**3.0.1.2 Class Activity - Designing a Communications System**



# Network Protocols and Communications

## Introduction

**Let’s just talk about this…**

You have just purchased a new automobile for your personal use. After driving the car for a week or so, you find that it is not working correctly.

After discussing the problem with several of your peers, you decide to take it to an automotive repair facility that they highly recommend. It is the only repair facility located in close proximity to you.

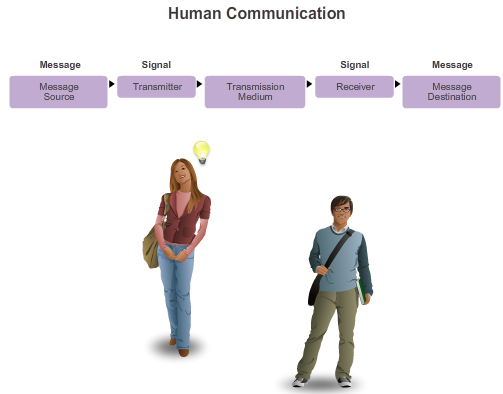
When you arrive at the repair facility, you find that all of the mechanics speak another language. You are having difficulty explaining the automobile’s performance problems, but the repairs really need to be done. You are not sure you can drive it back home to research other options.

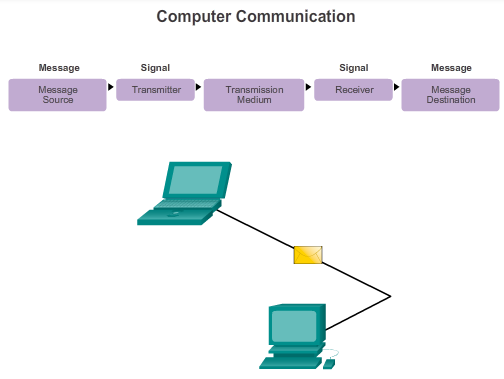
You must find a way to work with the repair facility to ensure that your automobile is fixed correctly.

How will you communicate with the mechanics in this firm? Design a communications model to ensure that the car is properly repaired.

[Class Activity - Let's just talk about this... Instructions](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.0.1.2%20Class%20Activity%20-%20Let's%20just%20talk%20about%20this...%20Instructions.pdf)

**3.1.1.1 What is Communication?**





# Rules of Communication

## The Rules

A network can be as complex as devices connected across the Internet, or as simple as two computers directly connected to one another with a single cable, and anything in-between. Networks can vary in size, shape, and function. However, simply having the physical connection between end devices is not enough to enable communication. For communication to occur, devices must know “how” to communicate.

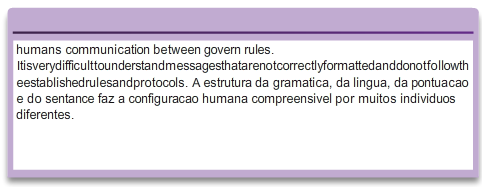
People exchange ideas using many different communication methods. However, regardless of the method chosen, all communication methods have three elements in common. The first of these elements is the message source, or sender. Message sources are people, or electronic devices, that need to send a message to other individuals or devices. The second element of communication is the destination, or receiver, of the message. The destination receives the message and interprets it. A third element, called a channel, consists of the media that provides the pathway over which the message travels from source to destination.

Communication begins with a message, or information, that must be sent from a source to a destination. The sending of this message, whether by face-to-face communication or over a network, is governed by rules called protocols. These protocols are specific to the type of communication method occurring. In our day-to-day personal communication, the rules we use to communicate over one medium, like a telephone call, are not necessarily the same as the protocols for using another medium, such as sending a letter.

For example, consider two people communicating face-to-face, as shown in Figure 1. 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. Each of these tasks describes protocols put in place to accomplish communication. This is true of computer communication, as shown in Figure 2.

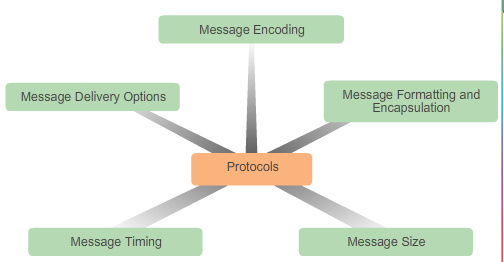
Think of how many different rules or protocols govern all the different methods of communication that exist in the world today.

**3.1.1.2 Establishing the Rules**









# Rules of Communication

## The Rules

**Establishing the Rules**

Before communicating with one another, individuals must use established rules or agreements to govern the conversation. For example, consider Figure1, protocols are necessary for effective communication. 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. There are many protocols available that govern successful human communication. Once there is an agreed upon method of communicating (face-to-face, telephone, letter, photography), the protocols put in place must account for the following requirements:

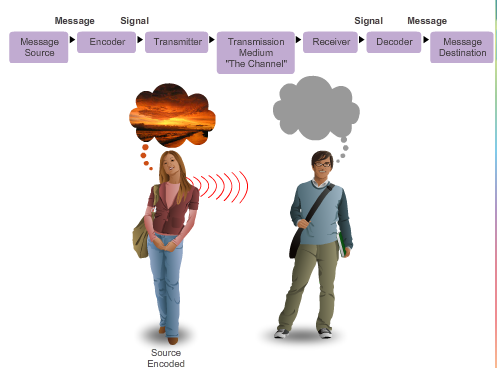
* An identified sender and receiver
* Common language and grammar
* Speed and timing of delivery
* Confirmation or acknowledgement requirements

The protocols that are used in network communications share many of the fundamental traits as those protocols used to govern successful human conversations, see Figure 2. In addition to identifying the source and destination, computer and network protocols define the details of how a message is transmitted across a network to answer the above requirements. While there are many protocols that must interact, common computer protocols include:

* Message encoding
* Message formatting and encapsulation
* Message size
* Message timing
* Message delivery options

Each of these will be discussed in more detail next.

**3.1.1.3 Message Encoding**



# Rules of Communication

## The Rules

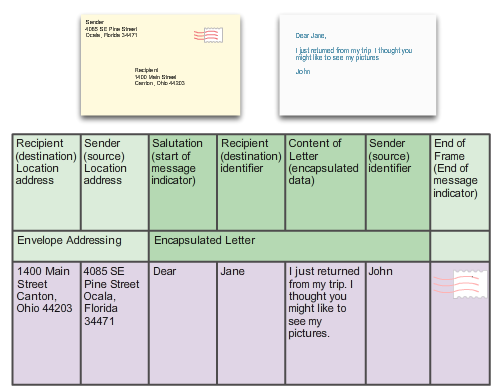
**Message Encoding**

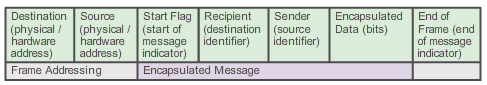
One of the first steps to sending a message is encoding it. Encoding is the process of converting information into another, acceptable form, for transmission. Decoding reverses this process in order to interpret the information.

Imagine a person planning a holiday trip with a friend, and calling the friend to discuss the details of where they want to go, as shown in Figure 1. To communicate the message, the sender must first convert, or encode, their thoughts and perceptions about the location into words. The words are spoken into the telephone using the sounds and inflections of spoken language that convey the message. On the other end of the telephone line, the person listening to the description, receives and decodes the sounds in order to visualize the image of the sunset described by the sender.

Encoding also occurs in computer communication, as shown in Figure 2. Encoding between hosts must be in an appropriate form for the medium. Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message.

**3.1.1.4 Message Formatting and Encapsulation**





**Rules of Communication**

**The Rules**

**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.

Letter writing is one of the most common forms of written human communication. For centuries, the agreed format for personal letters has not changed. In many cultures, a personal letter contains the following elements:

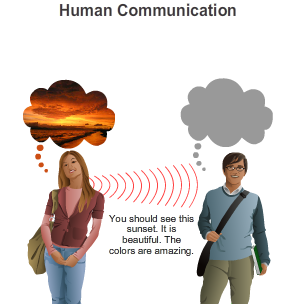
* An identifier of the recipient
* A salutation or greeting
* The message content
* A closing phrase
* An identifier of the sender

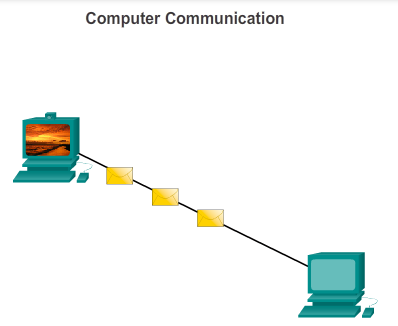
In addition to having the correct format, most personal letters must also be enclosed, or encapsulated, in an envelope for delivery, as shown in Figure 1. The envelope has the address of the sender and receiver on it, each located at the proper place on the envelope. If the destination address and formatting are not correct, the letter is not delivered. The process of placing one message format (the letter) inside another message format (the envelope) is called encapsulation. De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.

A letter writer uses an accepted format to ensure that the letter is delivered and understood by the recipient. In the same way, a message that is sent over a computer network follows specific format rules for it to be delivered and processed. Just as a letter is encapsulated in an envelope for delivery, so too are computer messages encapsulated. 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; it provides the address of the intended destination and the address of the source host, as shown in Figure 2.

The format and contents of a frame are determined by the type of message being sent and the channel over which it is communicated. Messages that are not correctly formatted are not successfully delivered to or processed by the destination host.

**3.1.1.5 Message Size**





# Rules of Communication

## The Rules

**Message Size**

Another rule of communication is size. When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences. These sentences are limited in size to what the receiving person can process at one time, as shown in Figure 1. An individual conversation may be made up of many smaller sentences to ensure that each part of the message is received and understood. Imagine what it would be like to read this course if it all appeared as one long sentence; it would not be easy to read and comprehend.

Likewise, 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.

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. This is known as segmenting. Each segment is encapsulated in a separate frame with the address information, and is sent over the network. At the receiving host, the messages are de-encapsulated and put back together to be processed and interpreted.

**3.1.1.6 Message Timing**



# Rules of Communication

## The Rules

**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.

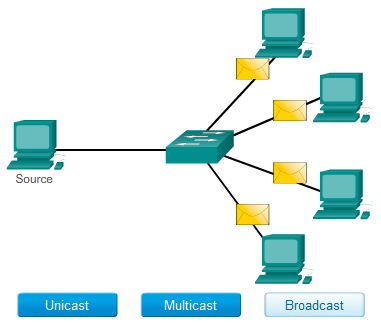
**Flow Control**

Timing also affects how much information can be sent and the speed that it can be delivered. If one person speaks too quickly, it is difficult for the other person to hear and understand the message, as shown in Figure 2. The receiving person must ask the sender to slow down. In network communication, a sending host can transmit messages at a faster rate than the destination host can receive and process. Source and destination hosts use flow control to negotiate correct timing for successful communication.

**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 show 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.

**3.1.1.7 Message Delivery Options**



# Rules of Communication

## The Rules

**Message Delivery Options**

A message may need to be best delivered in different ways, as shown in Figure 1. Sometimes, a person wants to communicate information to a single individual. At other times, the person may need to send information to a group of people at the same time, or even to all people in the same area. A conversation between two people is an example of a one-to-one delivery. When a group of recipients need to receive the same message simultaneously, a one-to-many or one-to-all message delivery is necessary.

There are also times when the sender of a message needs to be sure that the message is delivered successfully to the destination. In these cases, it is necessary for the recipient to return an acknowledgement to the sender. If no acknowledgement is required, the delivery option is referred to as unacknowledged.

Hosts on a network use similar delivery options to communicate, as shown in Figure 2.

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

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.

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. Additionally, hosts have requirements for acknowledged versus unacknowledged messages.

**3.2.1.1 Protocols: Rules that Govern Communications**



# Network Protocols and Standards

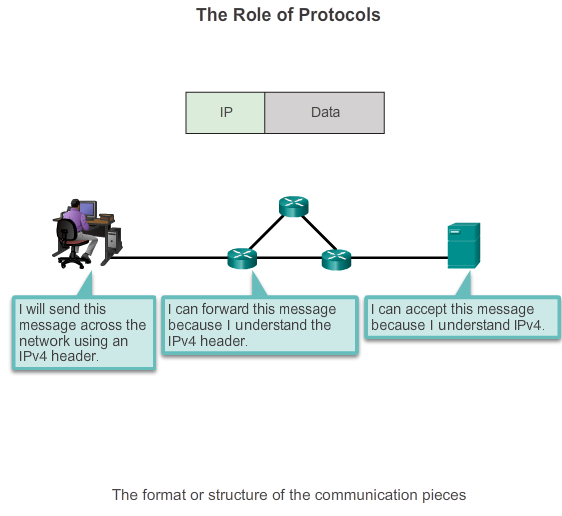
## Protocols

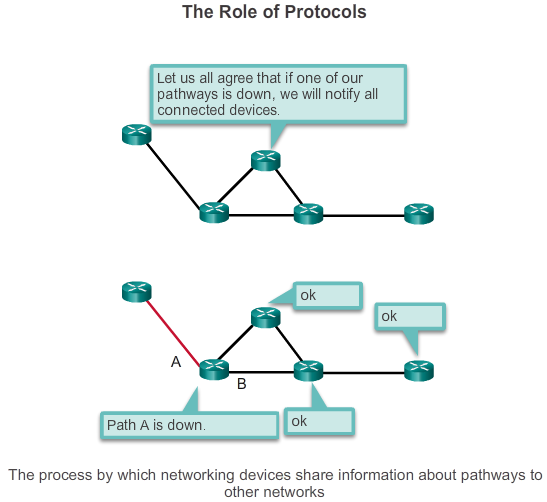
Just like in human communication, the various network and computer protocols must be able to interact and work together for network communication to be successful. A group of inter-related protocols necessary to perform a communication function is called a protocol suite. Protocol suites are implemented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

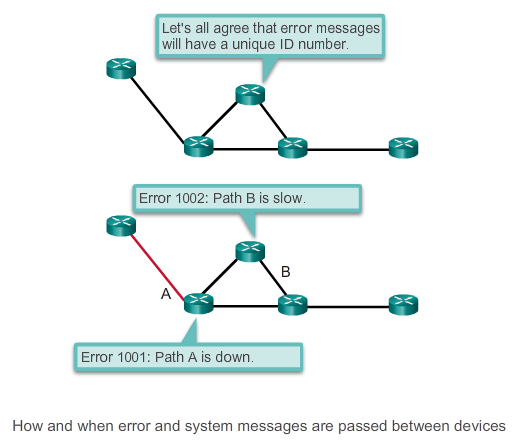
One of the best ways to visualize how the protocols within a suite interact is to view the interaction as a stack. A protocol stack shows how the individual protocols within a suite are implemented. The protocols are viewed in terms of layers, with each higher level service depending on the functionality defined by the protocols shown in the lower levels. The lower layers of the stack are concerned with moving data over the network and providing services to the upper layers, which are focused on the content of the message being sent. As the figure shows, we can use layers to describe the activity occurring in our face-to-face communication example. At the bottom layer, the physical layer, we have two people, each with a voice that can say words out loud. At the second layer, the rules layer, we have an agreement to speak in a common language. At the top layer, the content layer, there are words that are actually spoken. This is the content of the communication.

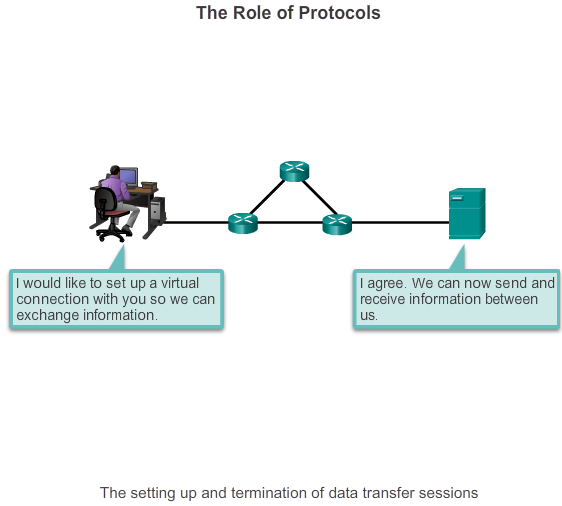
Were we to witness this conversation, we would not actually see layers floating in space. The use of layers is a model that provides a way to conveniently break a complex task into parts and describe how they work.

**3.2.1.2 Network Protocols**









# Network Protocols and Standards

## Protocols

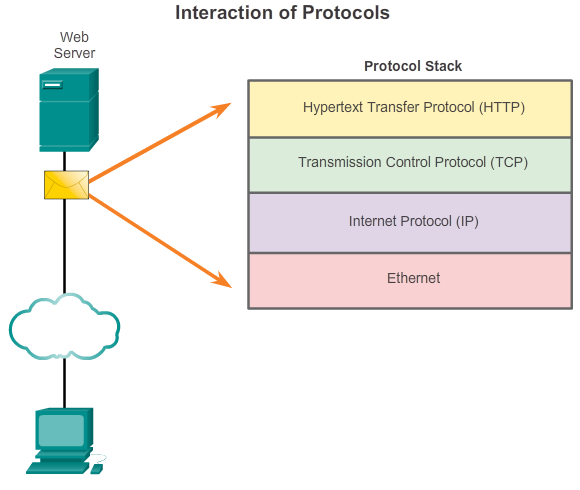
At the human level, some communication rules are formal and others are simply understood based on custom and practice. For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. Networking protocols define a common format and set of rules for exchanging messages between devices. Some common networking protocols are IP, HTTP, and DHCP.

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

For example, IP defines how a packet of data is delivered within a network or to a remote network. The information in the IPv4 protocol is transmitted in a specific format so that the receiver can interpret it correctly. This is not much different than the protocol used to address an envelope when mailing a letter. The information must adhere to a certain format or the letter cannot be delivered to the destination by the post office.

**3.2.1.3 Interaction of Protocols**



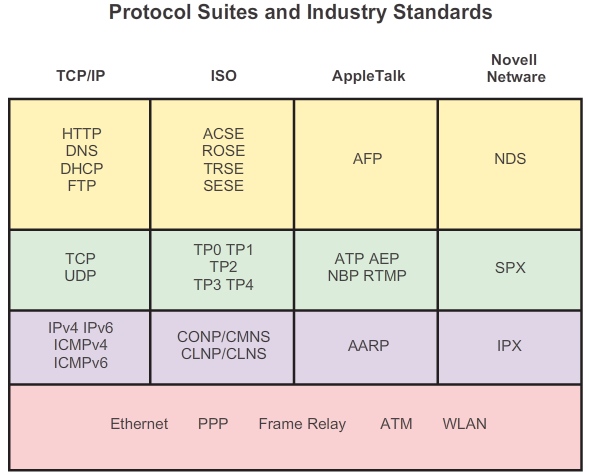
# Network Protocols and Standards

## 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. Examples of these protocols are:

* **Application Protocol** - Hypertext Transfer Protocol (HTTP) is a protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.
* **Transport Protocol** - Transmission Control Protocol (TCP) is the transport protocol that manages the individual conversations between web servers and web clients. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.
* **Internet Protocol** - IP is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them across the best path to the destination host.
* **Network Access Protocols** - Network access protocols describe two primary functions, communication over a data link and the physical transmission of data on the network media. Data-link management protocols take the packets from IP and format them to be transmitted over the media. The standards and protocols for the physical media govern how the signals are sent and how they are interpreted by the receiving clients. An example of a network access protocol is Ethernet.

**3.2.2.1 Protocol Suites and Industry Standards**



# Network Protocols and Standards

## Protocol Suites

As stated previously, 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.

A standards-based protocol is a process or protocol that has been endorsed by the networking industry and ratified, or approved, by a standards organization. The use of standards in developing and implementing protocols ensures that products from different manufacturers can interoperate successfully. If a protocol is not rigidly observed by a particular manufacturer, their equipment or software may not be able to successfully communicate with products made by other manufacturers.

In data communications, for example, if one end of a conversation is using a protocol to govern one-way communication and the other end is assuming a protocol describing two-way communication, in all probability, no data will be exchanged.

Some protocols are proprietary. Proprietary, in this context, means that one company or vendor controls the definition of the protocol and how it functions. Some proprietary protocols can be used by different organizations with permission from the owner. Others can only be implemented on equipment manufactured by the proprietary vendor. Examples of proprietary protocols are AppleTalk and Novell Netware.

Several companies may even work together to create a proprietary protocol. It is not uncommon for a vendor (or group of vendors) to develop a proprietary protocol to meet the needs of its customers and later assist in making that proprietary protocol an open standard. For example, Ethernet was a protocol originally developed by Bob Metcalfe at the XEROX Palo Alto Research Center (PARC) in the 1970s. In 1979, Bob Metcalfe formed his own company, 3COM, and worked with Digital Equipment Corporation (DEC), Intel, and Xerox to promote the “DIX” standard for Ethernet. In 1985, the Institute of Electrical and Electronics Engineers (IEEE) published the IEEE 802.3 standard that was almost identical to Ethernet. Today, 802.3 is the common standard used on local-area networks (LANs). Another example, most recently, Cisco opened the EIGRP routing protocol as an informational RFC to meet the needs of customers who desire to use the protocol in a multivendor network.

**3.2.2.2 Creation of the Internet and Development of TCP/IP**



# Network Protocols and Standards

## Protocol Suites

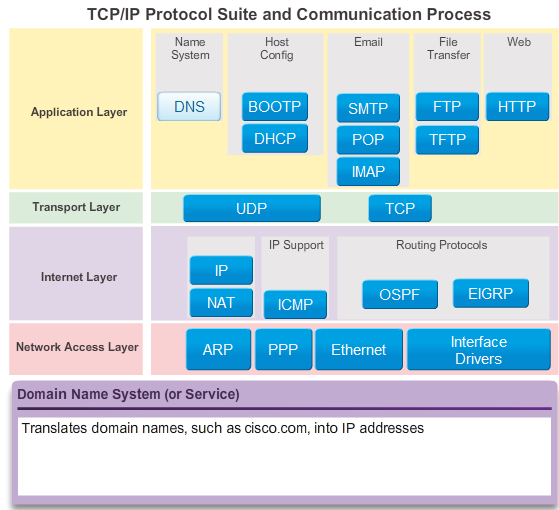
The IP suite is a suite of protocols required for transmitting and receiving information using the Internet. It is commonly known as TCP/IP because the first two networking protocols defined for this standard were TCP and IP. The open standards-based TCP/IP has replaced other vendor proprietary protocol suites, such as Apple’s AppleTalk and Novell’s Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

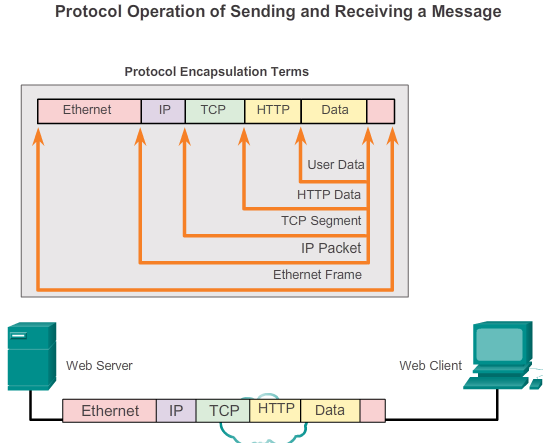
The first packet switching network and predecessor to today’s Internet was the Advanced Research Projects Agency Network (ARPANET), which came to life in 1969 by connecting mainframe computers at four locations. ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories. Bolt, Beranek and Newman (BBN) was the contractor that did much of the initial development of the ARPANET, including creating the first router known as an Interface Message Processor (IMP).

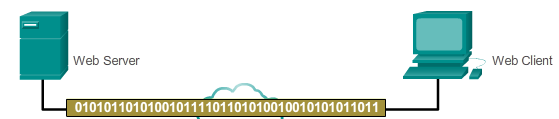
In 1973, Robert Kahn and Vinton Cerf began work on TCP to develop the next generation of the ARPANET. TCP was designed to replace ARPANET’s current Network Control Program (NCP). In 1978, TCP was divided into two protocols: TCP and IP. Later, other protocols were added to the TCP/IP suite of protocols including Telnet, FTP, DNS, and many others.

Click through the timeline in the figure to see details about the development of other network protocols and applications.

**3.2.2.3 TCP/IP Protocol Suite and Communication Process**







# Network Protocols and Standards

## Protocol Suites

Today, the suite includes dozens of protocols, as shown in Figure 1. Click each protocol to view its description. They are organized in layers using the TCP/IP protocol model. TCP/IP protocols are included in the internet layer to the application layer when referencing the TCP/IP model. The lower layer protocols in the data link or network access layer are responsible for delivering the IP packet over the physical medium. These lower layer protocols are developed by standards organizations, such as IEEE.

The TCP/IP protocol suite is implemented as a TCP/IP stack on both the sending and receiving hosts to provide end-to-end delivery of applications over a network. The 802.3 or Ethernet protocols are used to transmit the IP packet over the physical medium used by the LAN.

Figures 2 and 3 demonstrate the complete communication process using an example of a web server transmitting data to a client.

Click the Play button to view the animated demonstrations:

**1**. The web server’s Hypertext Markup Language (HTML) page is the data to be sent.

**2**. The application protocol HTTP header is added to the front of the HTML data. The header contains various information, including the HTTP version the server is using and a status code indicating it has information for the web client.

**3.** The HTTP application layer protocol delivers the HTML-formatted web page data to the transport layer. The TCP transport layer protocol is used to manage the individual conversation between the web server and web client.

**4**. Next, the IP information is added to the front of the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet.

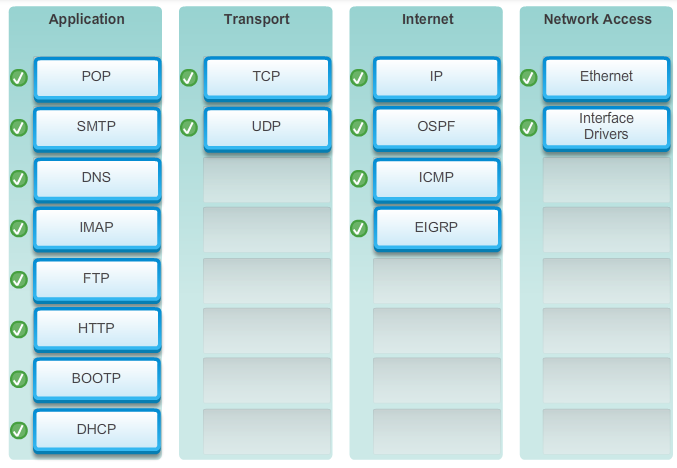
**5**. The Ethernet protocol adds information to both ends of the IP packet, known as a data link frame. This frame is delivered to the nearest router along the path towards the web client. This router removes the Ethernet information, analyzes the IP packet, determines the best path for the packet, inserts the packet into a new frame, and sends it to the next neighboring router towards the destination. Each router removes and adds new data link information before forwarding the packet.

**6**. This data is now transported through the internetwork, which consists of media and intermediary devices.

**7**. The client receives the data link frames that contain the data and each protocol header is processed and then removed in the opposite order that it was added. The Ethernet information is processed and removed, followed by the IP protocol information, then the TCP information, and finally the HTTP information.

**8**. The web page information is then passed on to the client’s web browser software.

**3.2.2.4 Activity – Mapping the Protocols of the TCP/IP Suite**



**3.2.3.1 Open Standards**



# Network Protocols and Standards

## Standards Organizations

Open standards encourage competition and innovation. They also guarantee that no single company’s product can monopolize the market, or have an unfair advantage over its competition. A good example of this is when purchasing a wireless router for the home. There are many different choices available from a variety of vendors, all of which incorporate standard protocols such as IPv4, DHCP, 802.3 (Ethernet), and 802.11 (Wireless LAN). These open standards also allow a client running Apple’s OS X operating system to download a web page from a web server running the Linux operating system. This is because both operating systems implement the open standard protocols, such as those in the TCP/IP suite.

Standards organizations are important in maintaining an open Internet with freely accessible specifications and protocols that can be implemented by any vendor. A standards organization may draft a set of rules entirely on its own or in other cases may select a proprietary protocol as the basis for the standard. If a proprietary protocol is used, it usually involves the vendor who created the protocol.

Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards.

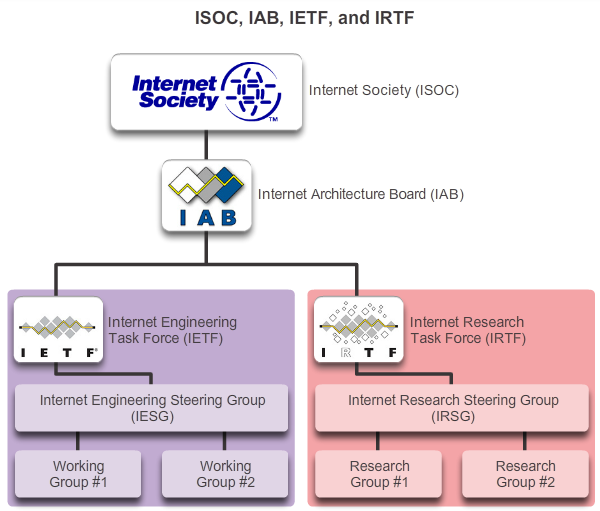
Standards organizations include:

* 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)

Each of these organizations will be discussed in more detail in the next couple of pages.

In the figure, click each logo to view standards information.

**3.2.3.2 ISOC, IAB, and IETF**



# Network Protocols and Standards

## Standards Organizations

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).

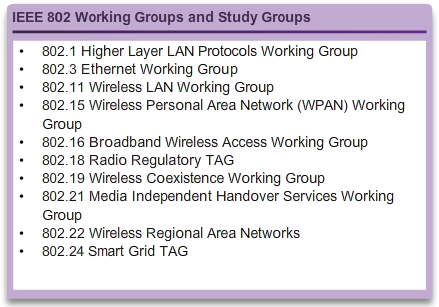
The Internet Architecture Board (IAB) is responsible for the overall management and development of Internet standards. The IAB provides oversight of the architecture for protocols and procedures used by the Internet. The IAB consists of 13 members, including the chair of the Internet Engineering Task 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).

**3.2.3.3 IEEE**





# Network Protocols and Standards

## Standards Organizations

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. As of 2012, IEEE consists of 38 societies, publishes 130 journals, and sponsors more than 1,300 conferences each year worldwide. The IEEE has over 1,300 standards and projects currently under development.

IEEE has more than 400,000 members in more than 160 countries. More than 107,000 of those members are student members. IEEE provides educational and career enhancement opportunities to promote the skills and knowledge with the electronics industry.

IEEE is one of the leading standard producing organizations in the world. It creates and maintains standards affecting a wide range of industries including power and energy, healthcare, telecommunications, and networking. The IEEE 802 family of standards deals with local area networks and metropolitan area networks, including both wired and wireless. As shown in the figure, each IEEE standard consists of a WG responsible for creating and improving the standards.

The IEEE 802.3 and IEEE 802.11 standards are significant IEEE standards in computer networking. The IEEE 802.3 standard defines Media Access Control (MAC) for wired Ethernet. This technology is usually for LANs, but also has wide-area network (WAN) applications. The 802.11 standard defines a set of standards for implementing wireless local-area networks (WLANs). This standard defines the Open Systems Interconnection (OSI) physical and data link MAC for wireless communications.

**3.2.3.4 ISO**



# Network Protocols and Standards

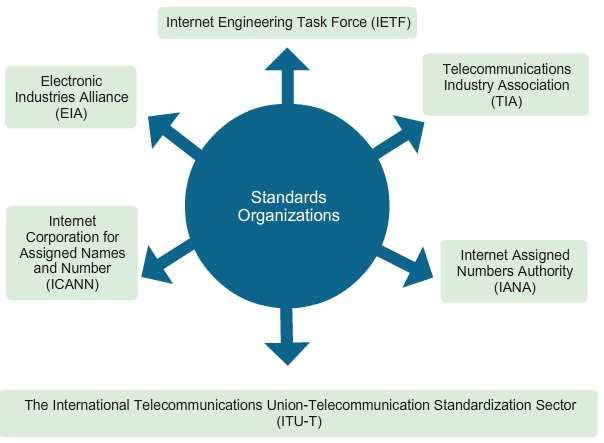
## Standards Organizations

ISO, the International Organization for Standardization, is the world’s largest developer of international standards for a wide variety of products and services. ISO is not an acronym for the organization’s name; rather the ISO term is based on the Greek word “isos”, meaning equal. The International Organization for Standardization chose the ISO term to affirm its position as being equal to all countries.

In networking, ISO is best known for its Open Systems Interconnection (OSI) reference model. ISO published the OSI reference model in 1984 to develop a layered framework for networking protocols. The original objective of this project was not only to create a reference model but also to serve as a foundation for a suite of protocols to be used for the Internet. This was known as the OSI protocol suite. However, due to the rising popularity of the TCP/IP suite, developed by Robert Kahn, Vinton Cerf, and others, the OSI protocol suite was not chosen as the protocol suite for the Internet. Instead, the TCP/IP protocol suite was selected. The OSI protocol suite was implemented on telecommunications equipment and can still be found in legacy telecommunication networks.

You may be familiar with some of the products that use ISO standards. The ISO file extension is used on many CD images to signify that it uses the ISO 9660 standard for its file system. ISO is also responsible for creating standards for routing protocols.

**3.2.3.5 Other Standards Organizations**



# Network Protocols and Standards

## Standards Organizations

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.

Familiarization with the organizations that develop standards used in networking will help you have a better understanding of how these standards create an open, vendor-neutral Internet, and allow you to learn about new standards as they develop.

**3.2.3.6 Lab - Researching Networking Standards**



# Network Protocols and Standards

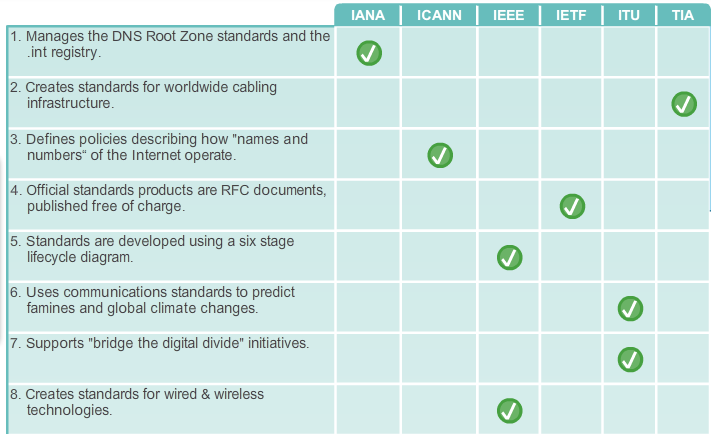
## Standards Organizations

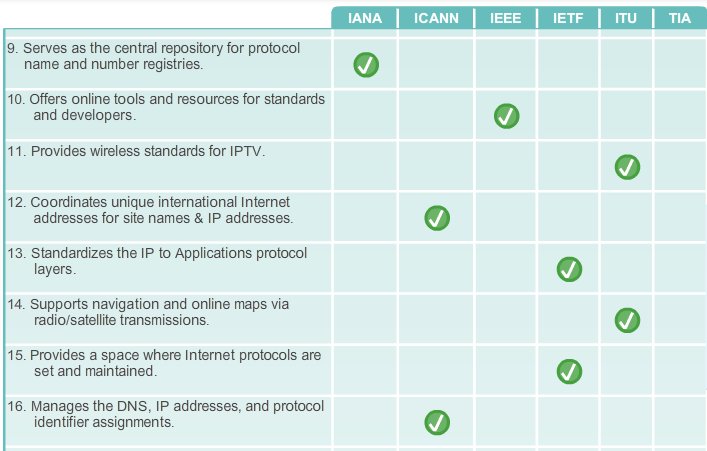
**In this lab, you will complete the following objectives:**

* Part 1: Research Networking Standards Organizations
* Part 2: Reflect on Internet and Computer Networking Experiences

[Lab - Researching Networking Standards](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.2.3.6%20Lab%20-%20Researching%20Networking%20Standards.pdf)

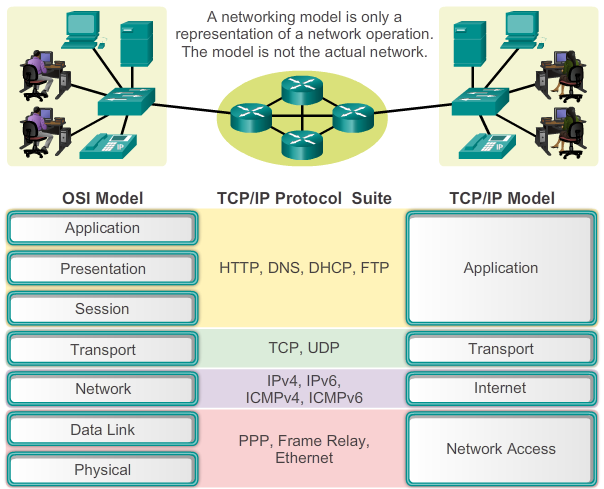
**3.2.3.7 Activity - Standards Body Scavenger Hunt**







**3.2.4.1 The Benefits of Using a Layered Model**



# Network Protocols and Standards

## Reference Models

A layered model, such as the TCP/IP model, is often used to help visualize the interaction between various protocols. A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction of protocols with the layers above and below each layer.

There are benefits to using a layered model to describe network protocols and operations. Using a layered model:

* Assists 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.
* Fosters competition because products from different vendors can work together.
* Prevents technology or capability changes in one layer from affecting other layers above and below.
* Provides a common language to describe networking functions and capabilities.

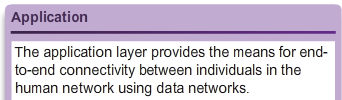
There are two basic types of networking models:

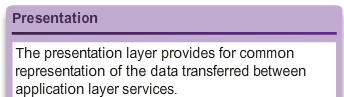
* **Protocol model** - This model closely matches the structure of a particular protocol suite. The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network. The TCP/IP model is a protocol model, because 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. A reference model is not intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes involved.

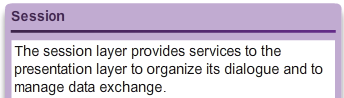
The OSI model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

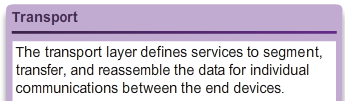
As shown in the figure, the TCP/IP and OSI models are the primary models used when discussing network functionality. Designers of network protocols, services, or devices can create their own models to represent their products. Ultimately, designers are required to communicate to the industry by relating their product or service to either the OSI model or the TCP/IP model, or to both.

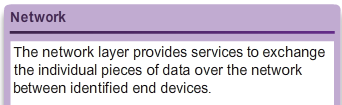
**3.2.4.2 The OSI Reference Model**

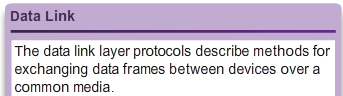


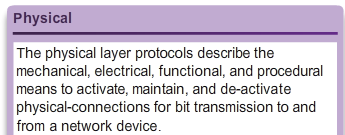












Network Protocols and Standards

## Reference Models

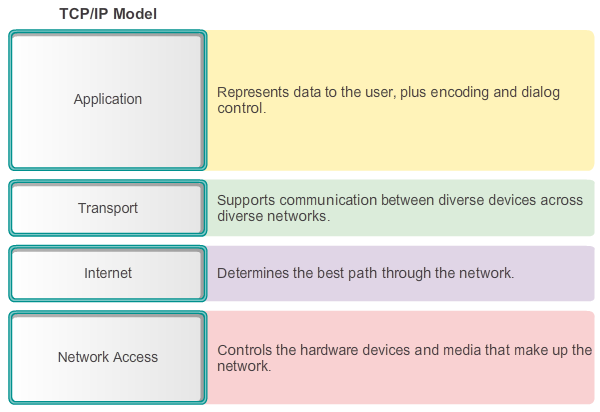
Initially the OSI model was designed by the ISO to provide a framework on which to build a suite of open systems protocols. The vision was that this set of protocols would be used to develop an international network that would not be dependent on proprietary systems.

Ultimately, the speed at which the TCP/IP-based Internet was adopted, and the rate at which it expanded, caused the development and acceptance of the OSI protocol suite to lag behind. Although a few of the developed protocols using the OSI specifications are widely used today, the seven-layer OSI model has made major contributions to the development of other protocols and products for all types of new networks.

The OSI model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below it. Although the content of this course is structured around the OSI reference model, the focus of discussion is the protocols identified in the TCP/IP protocol model. Click each layer name to view the details.

**Note**: Whereas the TCP/IP model layers are referred to only by name, the seven OSI model layers are more often referred to by number rather than by name. For instance, the physical layer is referred to as Layer 1 of the OSI model.

**3.2.4.3 The TCP/IP Protocol Model**



# Network Protocols and Standards

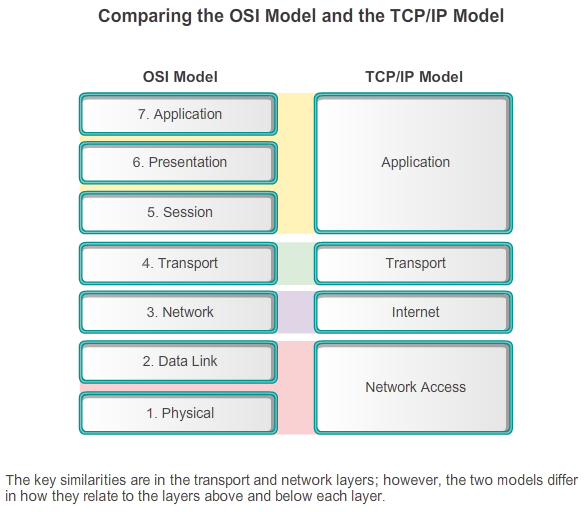
## Reference Models

The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the Internet model. As shown in the figure, it defines four categories of functions that must occur for communications to be successful. The architecture of the TCP/IP protocol suite follows the structure of this model. Because of this, the Internet model is commonly referred to as the TCP/IP model.

Most protocol models describe a vendor-specific protocol stack. However, because the TCP/IP model is an open standard, one company does not control the definition of the model. The definitions of the standard and the TCP/IP protocols are discussed in a public forum and defined in a publicly available set of RFCs. The RFCs contain both the formal specification of data communications protocols and resources that describe the use of the protocols.

The RFCs also contain technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the IETF.

**3.2.4.4 Comparing the OSI Model with the TCP/IP Model**



# Network Protocols and Standards

## Reference Models

The protocols that make up the TCP/IP protocol suite can be described in terms of the OSI reference model. In the OSI model, the network access layer and the application layer of the TCP/IP model are further divided to describe discrete functions that must occur at these layers.

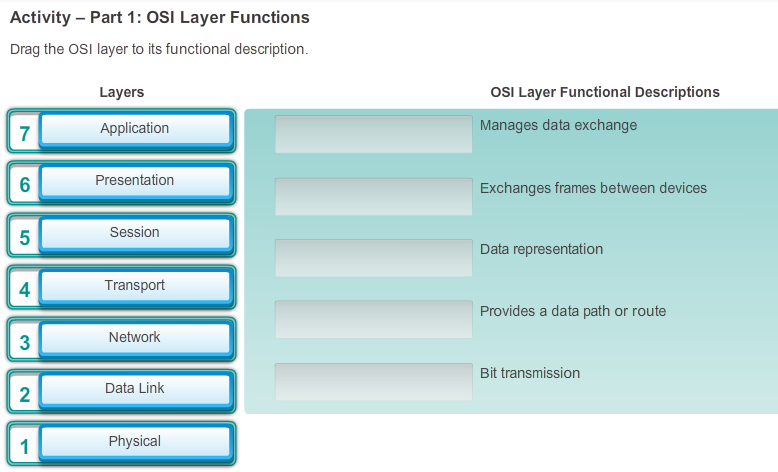
At the network access layer, the TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium; it only describes the handoff from the internet layer to the physical network protocols. OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

As shown in the figure, the critical parallels between the two network models occur at the OSI Layers 3 and 4. OSI Layer 3, the network layer, is almost universally used to describe the range of processes that occur in all data networks to address and route messages through an internetwork. IP is the TCP/IP suite protocol that includes the functionality described at OSI Layer 3.

Layer 4, the transport layer of the OSI model, describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts. These functions include acknowledgement, error recovery, and sequencing. At this layer, the TCP/IP protocols TCP and User Datagram Protocol (UDP) provide the necessary functionality.

The TCP/IP application layer includes a number of protocols that provide specific functionality to a variety of end user applications. The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce products that operate on networks.

**3.2.4.5 Activity – Identify Layers and Functions**



**3.2.4.6 Packet Tracer - Investigating the TCP/IP and OSI Models in Action**



# Network Protocols and Standards

## Reference Models

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Even though much of the information displayed will be discussed in more detail later, this is an opportunity to explore the functionality of Packet Tracer and be able to visualize the encapsulation process.

[Packet Tracer - Investigating the TCP/IP and OSI Models in Action Instructions](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.2.4.6%20Packet%20Tracer%20-%20Investigating%20the%20TCP-IP%20and%20OSI%20Models%20in%20Action%20Instructions.pdf)

[Packet Tracer - Investigating the TCP/IP and OSI Models in Action - PKA](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.2.4.6%20Packet%20Tracer%20-%20Investigating%20the%20TCP-IP%20and%20OSI%20Models%20in%20Action.pka)

**3.2.4.7 Lab - Researching RFCs**



# Network Protocols and Standards

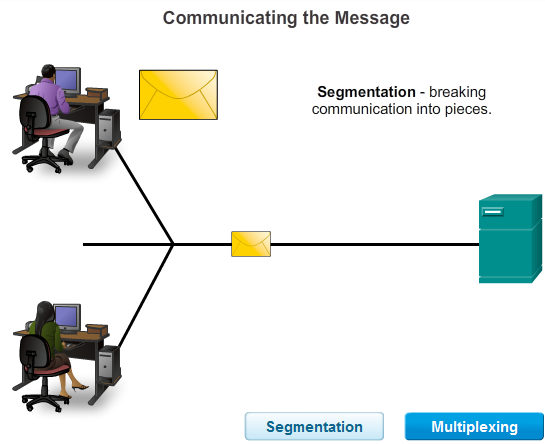
## Reference Models

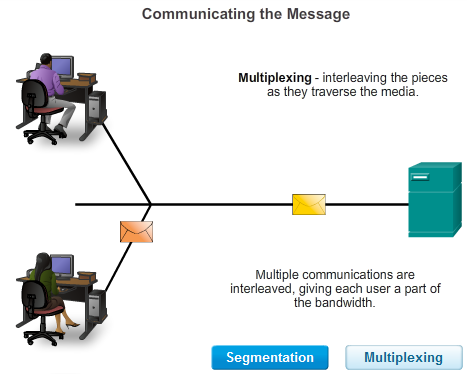
**In this lab, you will complete the following objectives:**

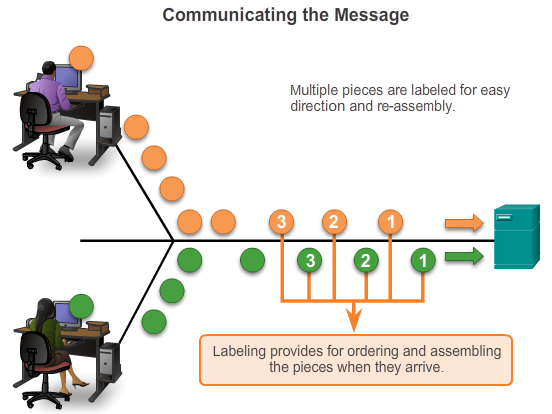
* Part 1: RFC Editor
* Part 2: Publishing RFCs

[Lab - Researching RFCs](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.2.4.7%20Lab%20-%20Researching%20RFCs.pdf)

**3.3.1.1 Communicating the Messages**







# Moving Data in the Network

## Data Encapsulation

In theory, a single communication, such as a music video or an email message, could be sent across a network from a source to a destination as one massive, uninterrupted stream of bits. If messages were actually transmitted in this manner, it would mean that no other device would be able to send or receive messages on the same network while this data transfer was in progress. These large streams of data would result in significant delays. Further, if a link in the interconnected network infrastructure failed during the transmission, the complete message would be lost and have to be retransmitted in full.

A better approach is to divide the data into smaller, more manageable pieces to send over the network. This division of the data stream into smaller pieces is called segmentation. Segmenting messages has two primary benefits:

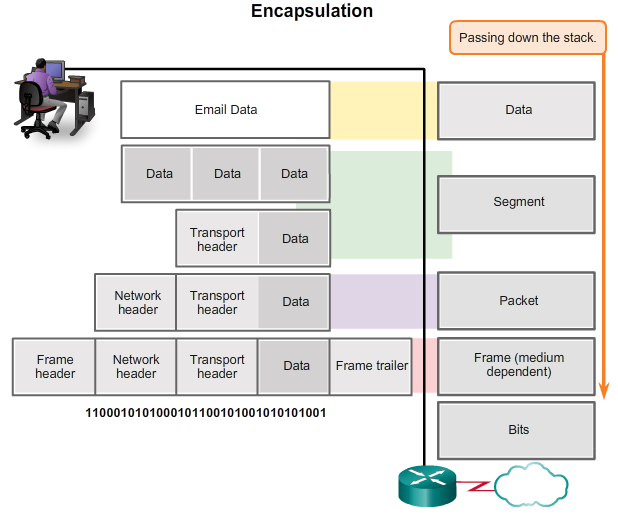
* By sending smaller individual pieces from source to destination, many different conversations can be interleaved on the network. The process used to interleave the pieces of separate conversations together on the network is called multiplexing. Click each button in Figure 1, and then click the Play button to view the animations of segmentation and multiplexing.
* Segmentation can increase the reliability of network communications. The separate pieces of each message need not travel the same pathway across the network from source to destination. If a particular path becomes congested with data traffic or fails, individual pieces of the message can still be directed to the destination using alternate pathways. If part of the message fails to make it to the destination, only the missing parts need to be retransmitted.

The downside to using segmentation and multiplexing to transmit messages across a network is the level of complexity that is added to the process. Imagine if you had to send a 100-page letter, but each envelope would only hold one page. The process of addressing, labeling, sending, receiving, and opening the entire 100 envelopes would be time-consuming for both the sender and the recipient.

In network communications, each segment of the message must go through a similar process to ensure that it gets to the correct destination and can be reassembled into the content of the original message, as shown in Figure 2.

Various types of devices throughout the network participate in ensuring that the pieces of the message arrive reliably at their destination.

**3.3.1.2 Protocol Data Units (PDUs)**



# Moving Data in the Network

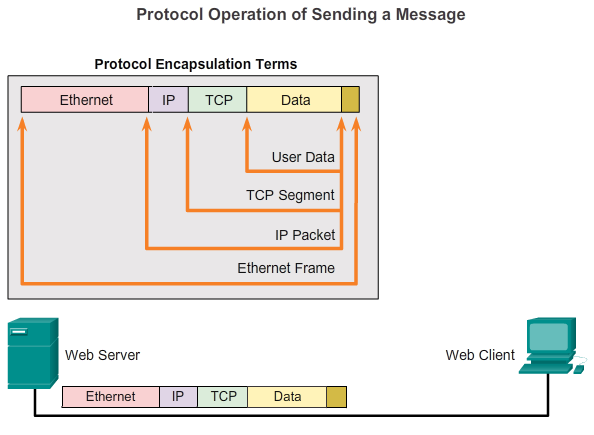
## Data Encapsulation

As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level. This is commonly known as the encapsulation process.

The form that a piece of data takes at any layer is called a protocol data unit (PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. At each stage of the process, a PDU has a different name to reflect its new functions. Although there is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite, as shown in the figure:

* **Data** - The general term for the PDU used at the application layer
* **Segment** - Transport layer PDU
* **Packet** - Network layer PDU
* **Frame** – Data Link layer PDU
* **Bits** - A Physical layer PDU used when physically transmitting data over the medium

**3.3.1.3 Encapsulation**



# Moving Data in the Network

## Data Encapsulation

Data encapsulation is the process that adds additional protocol header information to the data before transmission. In most forms of data communications, the original data is encapsulated or wrapped in several protocols before being transmitted.

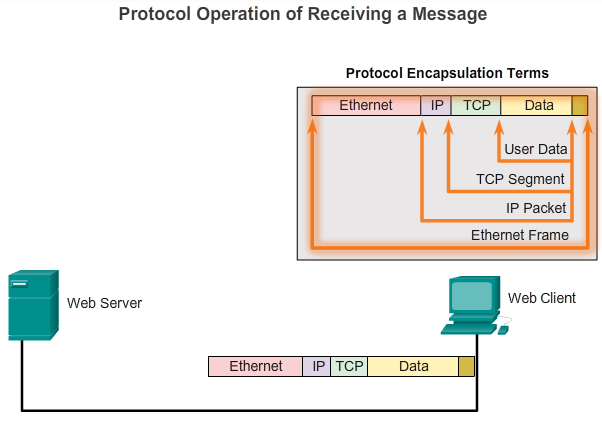
When sending messages on a network, the protocol stack on a host operates from top to bottom. In the web server example, we can use the TCP/IP model to illustrate the process of sending an HTML web page to a client.

The application layer protocol, HTTP, begins the process by delivering the HTML formatted web page data to the transport layer. There the application data is broken into TCP segments. Each TCP segment is given a label, called a header, containing information about which process running on the destination computer should receive the message. It also contains the information that enables the destination process to reassemble the data back to its original format.

The transport layer encapsulates the web page HTML data within the segment and sends it to the internet layer, where the IP protocol is implemented. Here the entire TCP segment is encapsulated within an IP packet, which adds another label, called the IP header. The IP header contains source and destination host IP addresses, as well as information necessary to deliver the packet to its corresponding destination process.

Next, the IP packet is sent to the network access layer where it is encapsulated within a frame header and trailer. Each frame header contains a source and destination physical address. The physical address uniquely identifies the devices on the local network. The trailer contains error checking information. Finally the bits are encoded onto the media by the server network interface card (NIC). Click the Play button in the figure to see the encapsulation process.

**3.3.1.4 De-encapsulation**

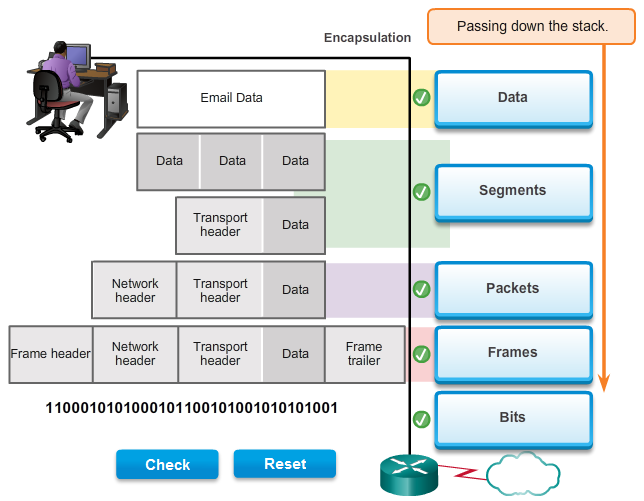


# Moving Data in the Network

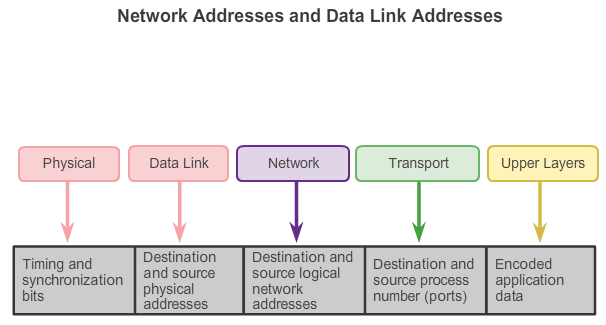
## Data Encapsulation

This process is reversed at the receiving host, and is known as de-encapsulation. De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application. Click the Play button in the figure to see the de-encapsulation process.

**3.3.1.5 Activity – Identify the PDU Layer**



**3.3.2.1 Network Addresses and Data Link addresses**



# Moving Data in the Network

## Accessing Local Resources

OSI model describes the processes of encoding, formatting, segmenting, and encapsulating data for transmission over the network. The network layer and data link layer are responsible for delivering the data from the source device or sender, to the destination device or receiver. Protocols at both layers contain source and destination addresses, but their addresses have different purposes.

**Network Address**

The network layer, or Layer 3, logical address contains information required to deliver the IP packet from the source device to the destination device. A Layer 3 IP address has two parts, the network prefix and the host part. The network prefix is used by routers to forward the packet to the proper network. The host part is used by the last router in the path to deliver the packet to the destination device.

An IP packet contains two IP addresses:

* **Source IP address** - The IP address of the sending device.
* **Destination IP address** - The IP address of the receiving device. The destination IP address is used by routers to forward a packet to its destination.

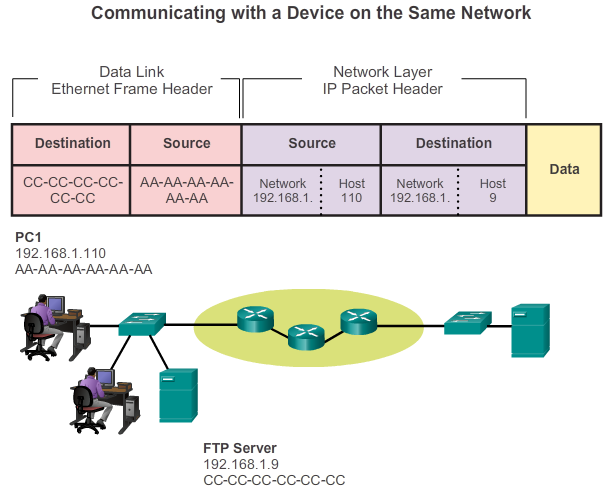
**Data Link Address**

The data link, or Layer 2, physical address has a different role. The purpose of the data link address is to deliver the data link frame from one network interface to another network interface on the same network. Before an IP packet can be sent over a wired or wireless network it must be encapsulated in a data link frame so it can be transmitted over the physical medium, the actual network. Ethernet LANs and wireless LANs are two examples of networks that have different physical media each with its own type of data link protocol.

The IP packet is encapsulated into a data link frame to be delivered to the destination network. The source and destination data link addresses are added, as shown in the figure:

* **Source data link address** - The physical address of the device that is sending the packet. Initially this is the NIC that is the source of the IP packet.
* **Destination data link address** - The physical address of the network interface of either the next hop router or the network interface of the destination device.

**3.3.2.2 Communicating with a Device on the Same Network**



# Moving Data in the Network

## Accessing Local Resources

To understand how communication is successful in the network, it is important to understand the roles of both the network layer addresses and the data link addresses when a device is communicating with another device on the same network. In this example we have a client computer, PC1, communicating with a file server, FTP server, on the same IP network.

**Network Addresses**

The network layer addresses, or IP addresses, indicate the network and host address of the source and destination. The network portion of the address will be the same; only the host or device portion of the address will be different.

* **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, FTP server: 192.168.1.9.

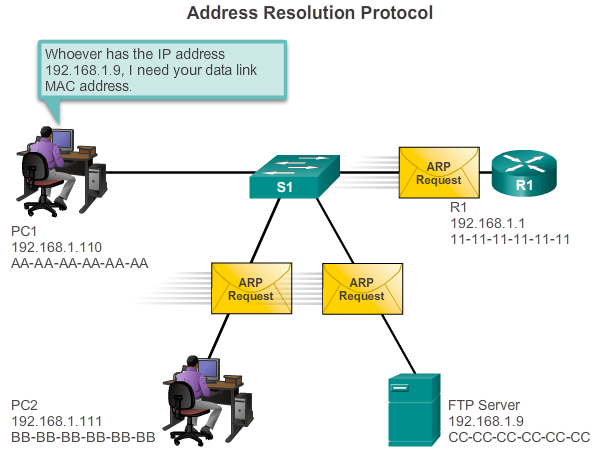
**Data Link Addresses**

When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet MAC addresses. MAC addresses are 48-bit addresses that are physically embedded on the Ethernet NIC. A MAC address is also known as the physical address or burned-in address (BIA).

* **Source MAC address** - This is the data link address, or the Ethernet MAC address, of the device that sends the IP packet, PC1. The MAC address of the Ethernet NIC of PC1 is AA-AA-AA-AA-AA-AA.
* **Destination MAC address** - When the receiving device is on the same network as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server: CC-CC-CC-CC-CC-CC.

The source and destination addresses are added to the Ethernet frame. The frame with the encapsulated IP packet can now be transmitted from PC1 directly to the FTP server.

**3.3.2.3 MAC and IP Addresses**



# Moving Data in the Network

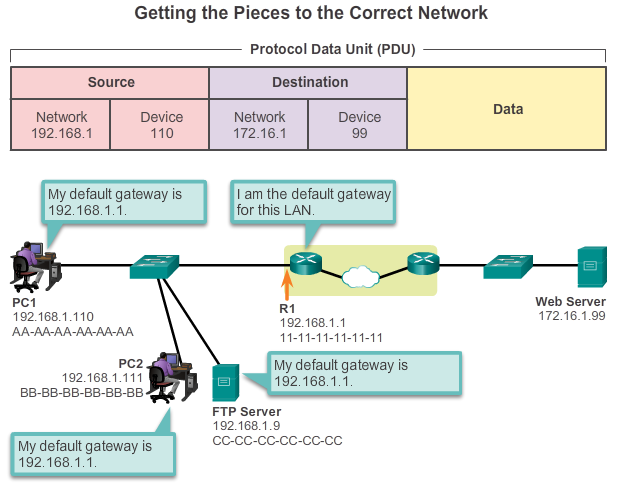
## Accessing Local Resources

It should now be clear that to send data to another host on the same LAN the source host must know both the physical and logical addresses of the destination host. Once this is known, it can create a frame and send it out on the network media. The source host can learn the destination IP address in a number of ways. For example, it may learn the IP address through the use of the Domain Name System (DNS), or it may know the destination IP address because the address is entered in the application manually, such as when a user specifies the IP address of a destination FTP server. But how does a host determine the Ethernet MAC address of another device?

Most network applications rely on the logical IP address of the destination to identify the location of the communicating hosts. The data link MAC address is required to deliver the encapsulated IP packet inside the Ethernet frame across the network to the destination.

The sending host uses a protocol called Address Resolution Protocol (ARP) to discover the MAC address of any host on the same local network. The sending host sends an ARP Request message to the entire LAN. The ARP Request is a broadcast message. The ARP Request contains the IP address of the destination device. Every device on the LAN examines the ARP Request to see if it contains its own IP address. Only the device with the IP address contained in the ARP Request responds with an ARP Reply. The ARP Reply includes the MAC address associated with the IP address in the ARP Request.

**3.3.3.1 Default Gateway**



# Moving Data in the Network

## Accessing Remote Resources

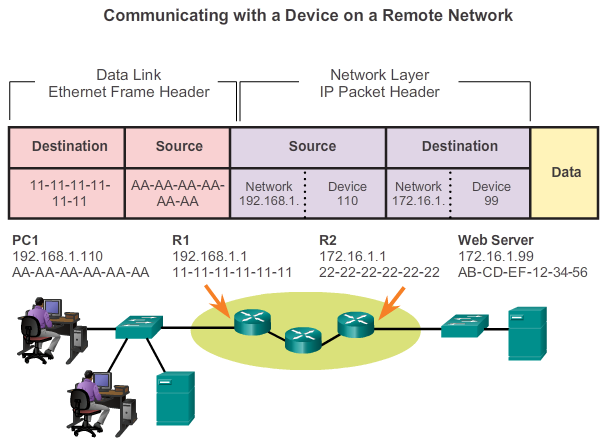
The method that a host uses to send messages to a destination on a remote network differs from the way a host sends messages to a destination on the same local network. When a host needs to send a message to another host located on the same network, it will forward the message directly. A host will use ARP to discover the MAC address of the destination host. It includes the destination IP address within the packet header and encapsulates the packet into a frame containing the MAC address of the destination and forwards it.

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.

In the figure, the hosts on the LAN are using R1 as the default gateway with its 192.168.1.1 address configured in their TCP/IP settings. If the destination of a PDU is on a different IP network, the hosts send the PDUs to the default gateway on the router for further transmission.

**3.3.3.2 Communicating with a Device on a Remote Network**



# Moving Data in the Network

## Accessing Remote Resources

But what are the roles of the network layer address and the data link layer address when a device is communicating with a device on a remote network? In this example we have a client computer, PC1, communicating with a server, named Web Server, on a different IP network.

**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.

**Data Link Addresses**

When the sender and receiver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway. In our example, the default gateway is R1. R1 has an interface and an IP address that is on the same network as PC1. This allows PC1 to reach the router directly.

* **Source MAC address** - The Ethernet MAC address of the sending device, PC1. The MAC address of the Ethernet interface of PC1 is AA-AA-AA-AA-AA-AA.

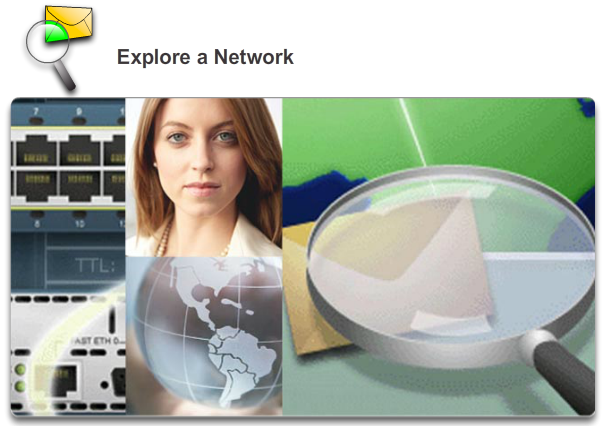
**Destination MAC address** - When the receiving device is on a different network from the sending device, this is the Ethernet MAC address of the default gateway or router. In this example, the destination MAC address is the MAC address of the R1 Ethernet interface that is attached to the PC1 network, which is 11-11-11-11-11-11.

The Ethernet frame with the encapsulated IP packet can now be transmitted to R1. R1 forwards the packet to the destination, Web Server. This may mean that R1 forwards the packet to another router or directly to Web Server if the destination is on a network connected to R1.

How does the sending device determine the MAC address of the router?

Each device knows the IP address of the router through the default gateway address configured in its TCP/IP settings. The default gateway address is the address of the router interface connected to the same local network as the source device. All devices on the local network use the default gateway address to send messages to the router. After the host knows the default gateway IP address, it can use ARP to determine the MAC address of that default gateway. The MAC address of the default gateway is then placed in the frame.

**3.3.3.3 Packet Tracer - Explore a Network**



# Moving Data in the Network

## Accessing Remote Resources

This simulation activity is intended to help you understand the flow of traffic and the contents of data packets as they traverse a complex network. Communications will be examined at three different locations simulating typical business and home networks.

[Packet Tracer - Explore a Network Instructions](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.3.3.3%20Packet%20Tracer%20-%20Explore%20a%20Network%20Instructions.pdf)

[Packet Tracer - Explore a Network - PKA](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.3.3.3%20Packet%20Tracer%20-%20Explore%20a%20Network.pka)

**3.3.3.4 Lab - Using Wireshark to View Network Traffic**



# Moving Data in the Network

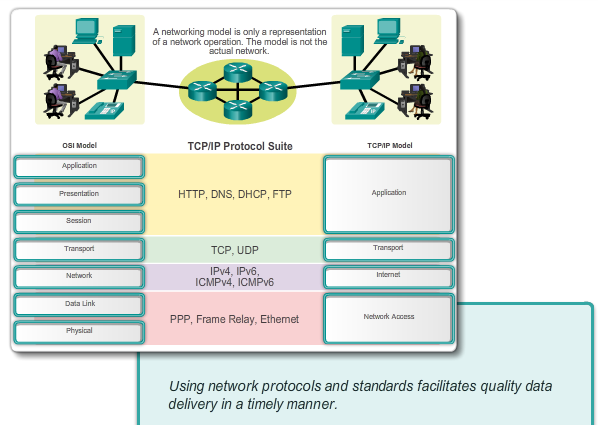
## Accessing Remote Resources

**In this lab, you will complete the following objectives:**

* Part 1: Download and Install Wireshark
* Part 2: Capture and Analyze Local ICMP Data in Wireshark
* Part 3: Capture and Analyze Remote ICMP Data in Wireshark

[Lab - Using Wireshark to View Network Traffic](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.3.3.4%20Lab%20-%20Using%20Wireshark%20to%20View%20Network%20Traffic.pdf)

**3.4.1.1 Class Activity - Guaranteed to Work!**



# Summary

## Summary

**Guaranteed to work!**

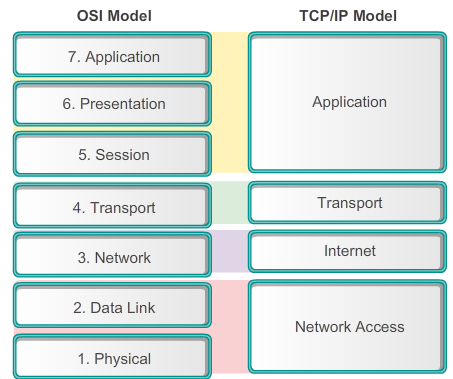
You have just completed the Chapter 3 content regarding network protocols and standards.

Assuming you resolved the beginning of this chapter’s modeling activity, how would you compare the following steps taken to design a communications system to the networking models used for communications?

* Establishing a language to communicate
* Dividing the message into small steps, delivered a little at a time, to facilitate understanding of the problem
* Checking to see if the data has been delivered fully and correctly
* Timing needed to ensure quality data communication and delivery

[Class Activity Guaranteed to work! Instructions](http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/3.4.1.1_Class_Activity_Guaranteed_to_Work_Instructor_Planning_Document.pdf)

**3.4.1.2 Summary**



# Summary

## Summary

Data networks are systems of end devices, intermediary devices, and the media connecting the devices. For communication to occur, these devices must know how to communicate.

These devices must comply with communication rules and protocols. TCP/IP is an example of a protocol suite. Most protocols are created by a standards organization such as the IETF or IEEE. The Institute of Electrical and Electronics Engineers is a professional organization for those in the electrical engineering and electronics fields. ISO, the International Organization for Standardization, is the world’s largest developer of international standards for a wide variety of products and services.

The most widely-used networking models are the OSI and TCP/IP models. Associating the protocols that set the rules of data communications with the different layers of these models is useful in determining which devices and services are applied at specific points as data passes across LANs and WANs.

Data that passes down the stack of the OSI model is segmented into pieces and encapsulated with addresses and other labels. The process is reversed as the pieces are de-encapsulated and passed up the destination protocol stack. The OSI model describes the processes of encoding, formatting, segmenting, and encapsulating data for transmission over the network.

The TCP/IP protocol suite is an open standard protocol that has been endorsed by the networking industry and ratified, or approved, by a standards organization. The Internet Protocol Suite is a suite of protocols required for transmitting and receiving information using the Internet.

Protocol Data Units (PDUs) are named according to the protocols of the TCP/IP suite: data, segment, packet, frame, and bits.

Applying models allows individuals, companies, and trade associations to analyze current networks and plan the networks of the future.