CCNA Exploration - Network Fundamentals

2 Communicating over the Network

2.0 Chapter Introduction

2.0.1 Chapter Introduction

Page 1:
More and more, it is networks that connect us. People communicate online from everywhere. Efficient, dependable technology enables networks to be available whenever and wherever we need them. As our human network continues to expand, the platform that connects and supports it must also grow.

Rather than developing unique and separate systems for the delivery of each new service, the network industry as a whole has developed the means to both analyze the existing platform and enhance it incrementally. This ensures that existing communications are maintained while new services are introduced that are both cost effective and technologically sound.

In this course, we focus on these aspects of the information network:

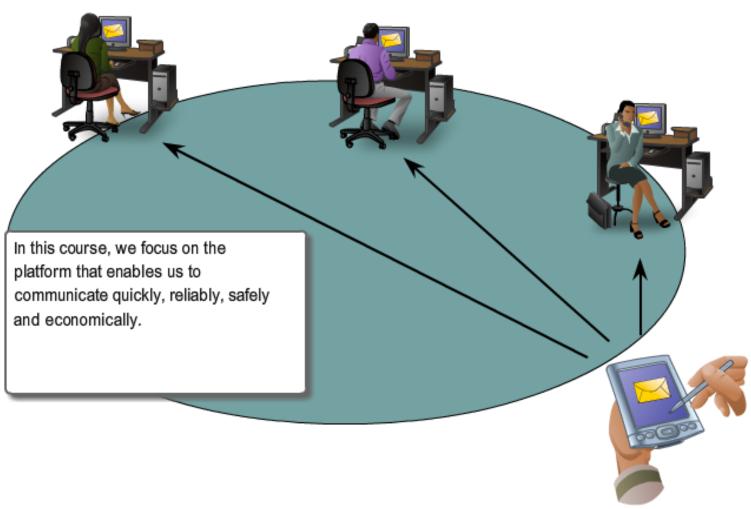
- Devices that make up the network
- Media that connect the devices
- Messages that are carried across the network
- Rules and processes that govern network communications
- Tools and commands for constructing and maintaining networks

Central to the study of networks is the use of generally-accepted models that describe network functions. These models provide a framework for understanding current networks and for facilitating the development of new technologies to support future communications needs.

Within this course, we use these models, as well as tools designed to analyze and simulate network functionality. Two of the tools that will enable you to build and interact with simulated networks are Packet Tracer 4.1 software and Wireshark network protocol analyzer.

This chapter prepares you to:

- Describe the structure of a network, including the devices and media that are necessary for successful communications.
- Explain the function of protocols in network communications.
- Explain the advantages of using a layered model to describe network functionality.
- Describe the role of each layer in two recognized network models: The TCP/IP model and the OSI model.
- Describe the importance of addressing and naming schemes in network communications.



CCNA Exploration - Network Fundamentals

2 Communicating over the Network

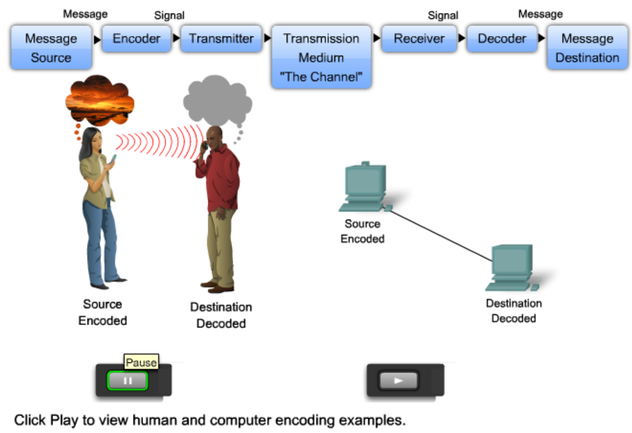
2.1 The Platform for Communications

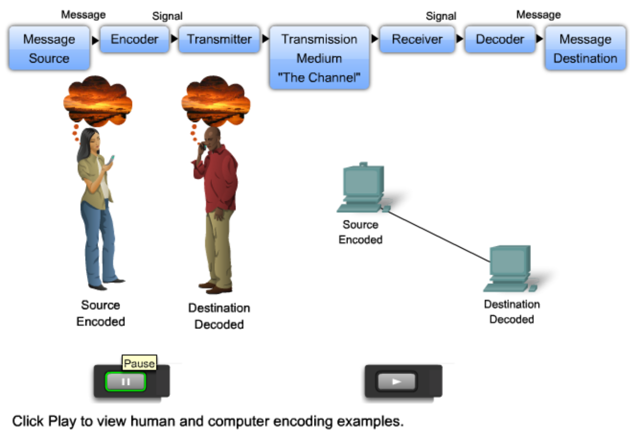
2.1.1 The Elements of Communication

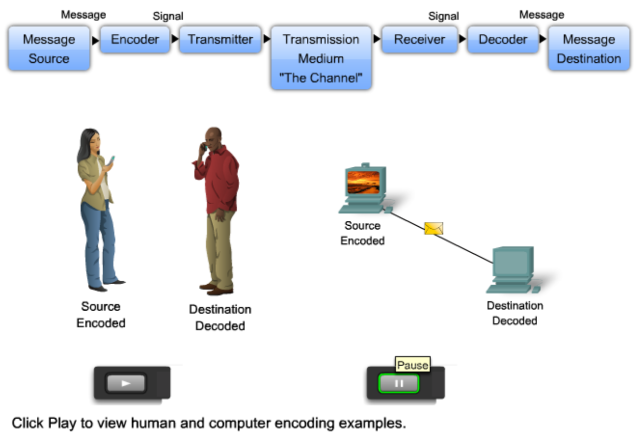
Page 1:
Communication begins with a message, or information, that must be sent from one individual or device to another. People exchange ideas using many different communication methods. All of these methods have three elements in common. The first of these elements is the message source, or sender. 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 can travel from source to destination.

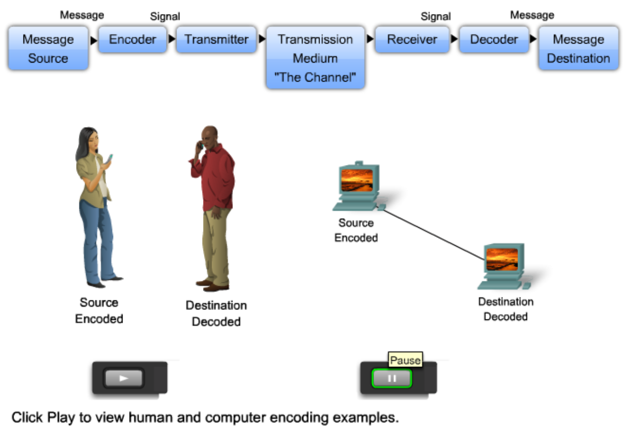
Consider, for example, the desire to communicate using words, pictures, and sounds. Each of these messages can be sent across a data or information network by first converting them into binary digits, or bits. These bits are then encoded into a signal that can be transmitted over the appropriate medium. In computer networks, the media is usually a type of cable, or a wireless transmission.

The term *network* in this course will refer to data or information networks capable of carrying many different types of communications, including traditional computer data, interactive voice, video, and entertainment products.









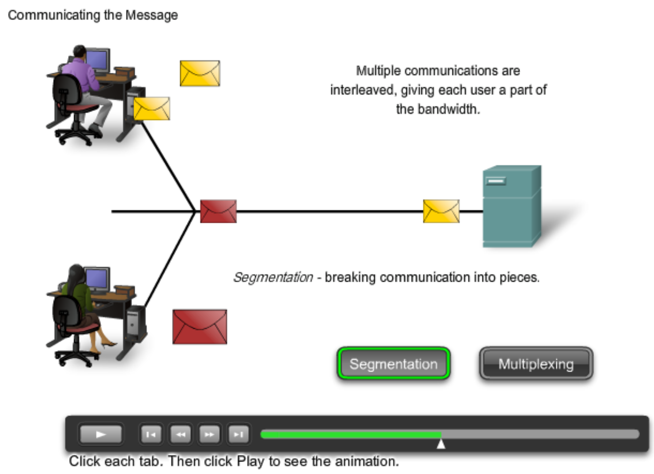
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.2 Communicating the Messages

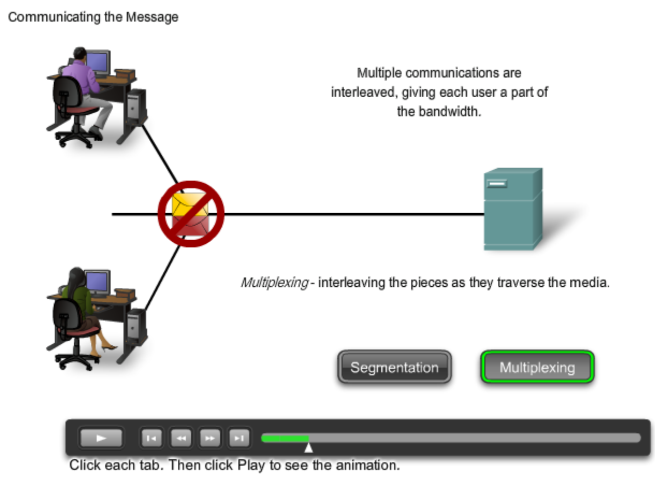
Page 1:
In theory, a single communication, such as a music video or an e-mail message, could be sent across a network from a source to a destination as one massive continuous stream of bits. If messages were actually transmitted in this manner, it would mean that no other device would be able to send 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.

First, 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.

Second, 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.



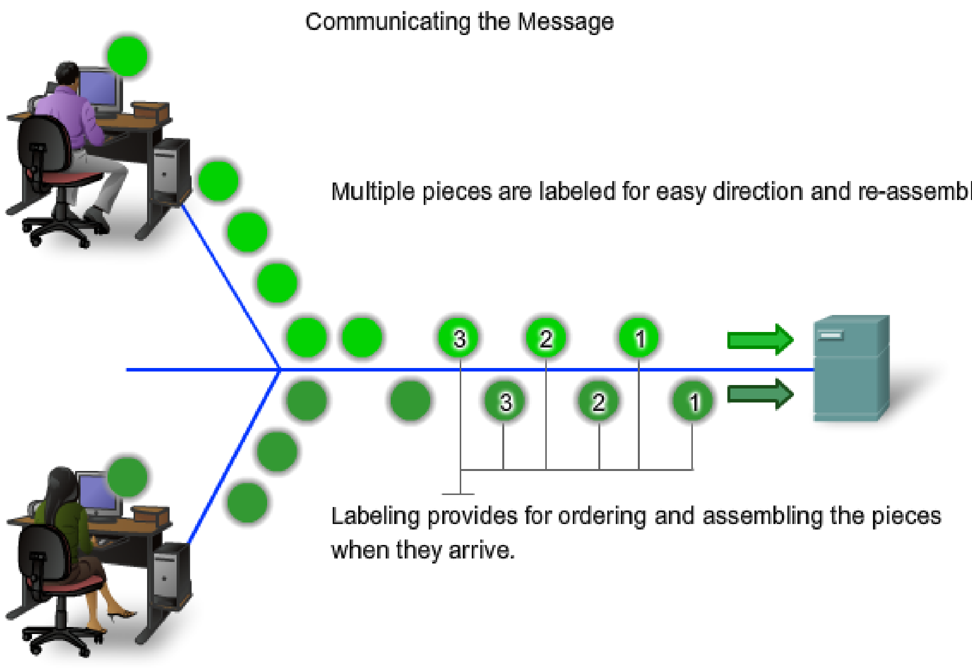


CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.2 Communicating the Messages

Page 2:
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 hundred 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.

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

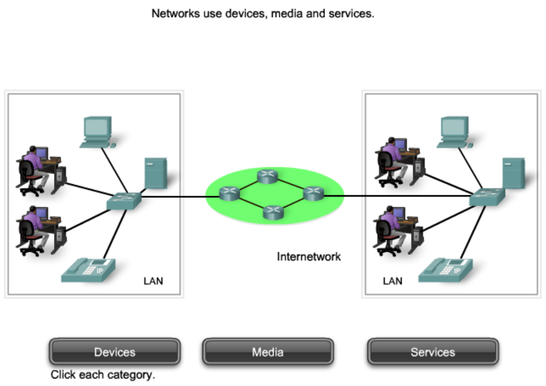


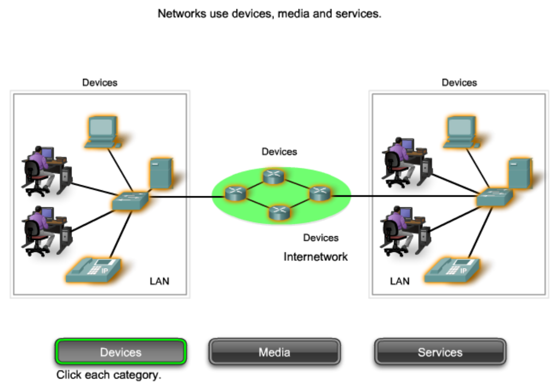
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.3 Components of the Network

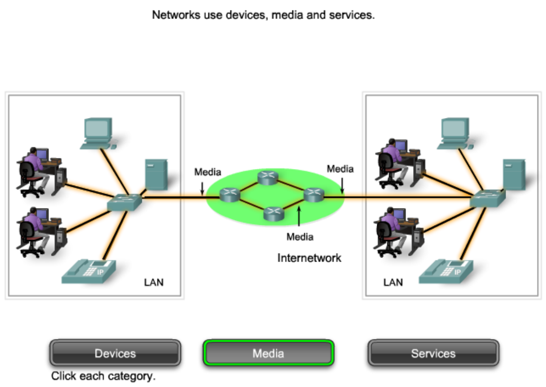
Page 1:
The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports our human network. It provides the stable and reliable channel over which our communications can occur.

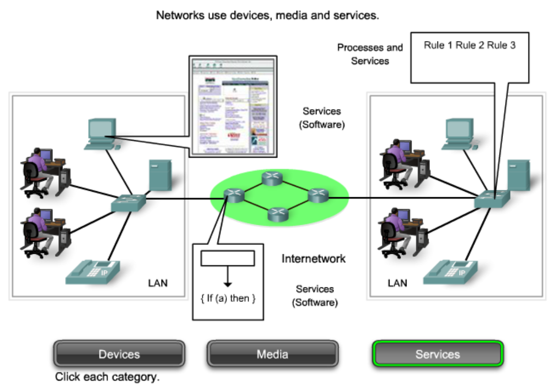
Devices and media are the physical elements or hardware of the network. Hardware is often the visible components of the network platform such as a laptop, a PC, a switch, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.

Services and processes are the communication programs, called software, that run on the networked devices. A network service provides information in response to a request. Services include many of the common network applications people use every day, like e-mail hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.









CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.4 End Devices and their Role on the Network

Page 1:
The network devices that people are most familiar with are called end devices. These devices form the interface between the human network and the underlying communication network. Some examples of end devices are:

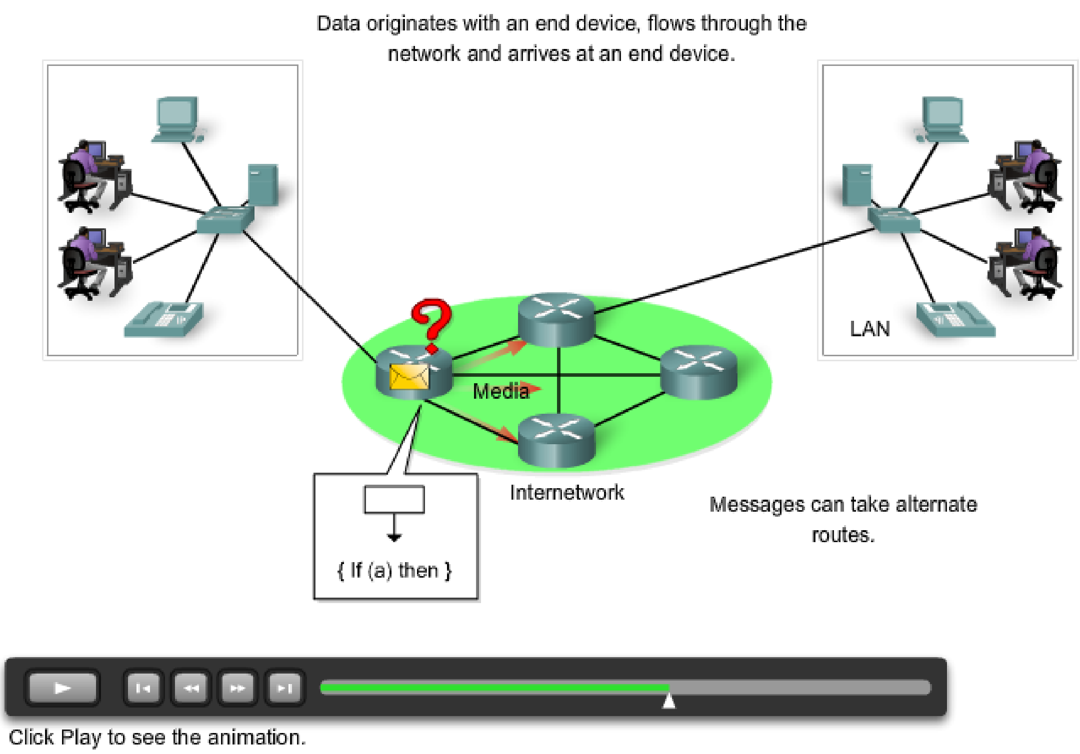
- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Mobile handheld devices (such as wireless barcode scanners, PDAs)

In the context of a network, end devices are referred to as hosts. A host device is either the source or destination of a message transmitted over the network. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

In modern networks, a host can act as a client, a server, or both. Software installed on the host determines which role it plays on the network.

Servers are hosts that have software installed that enables them to provide information and services, like e-mail or web pages, to other hosts on the network.

Clients are hosts that have software installed that enables them to request and display the information obtained from the server.



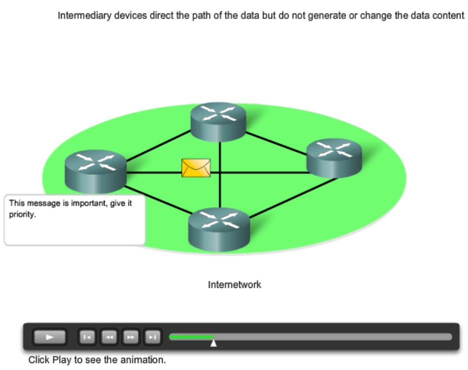
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.5 Intermediary Devices and their Role on the Network

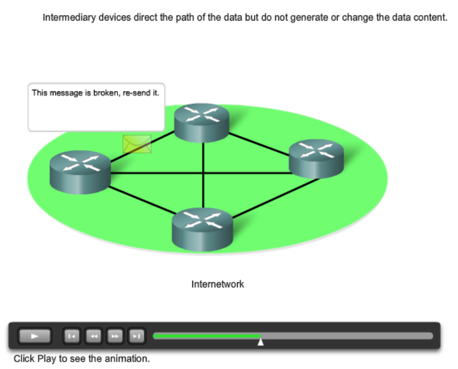
Page 1:
In addition to the end devices that people are familiar with, networks rely on intermediary devices to provide connectivity and to work behind the scenes to ensure that data flows across the network. These devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork. Examples of intermediary network devices are:

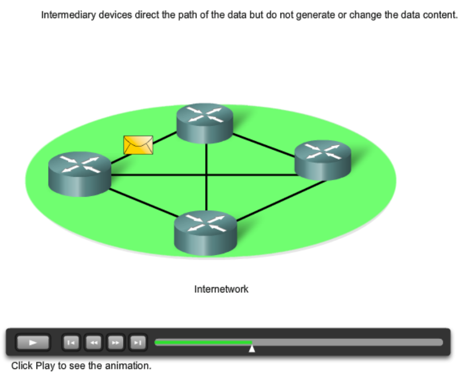
- Network Access Devices (Hubs, switches, and wireless access points)
- Internetworking Devices (routers)
- Communication Servers and Modems
- Security Devices (firewalls)

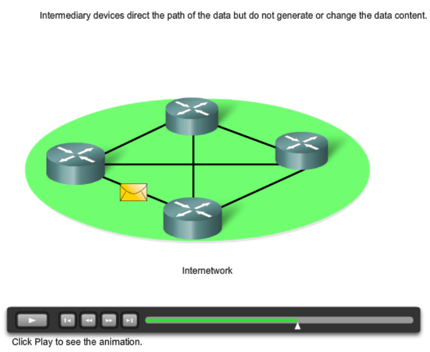
The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. Processes running on the intermediary network devices perform these functions:

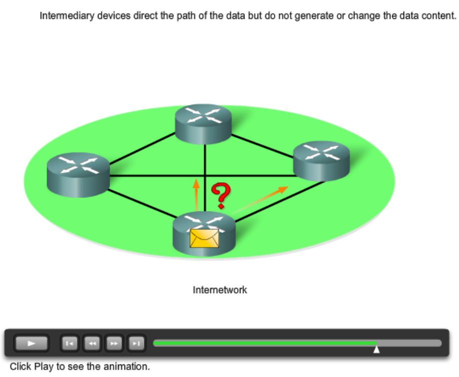
- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to QoS priorities
- Permit or deny the flow of data, based on security settings

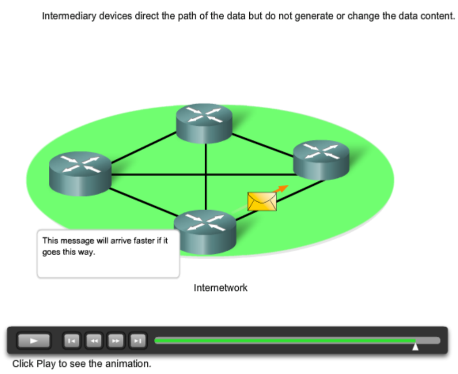












CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.1 The Platform for Communications
2.1.6 Network Media

Page 1:
Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination.

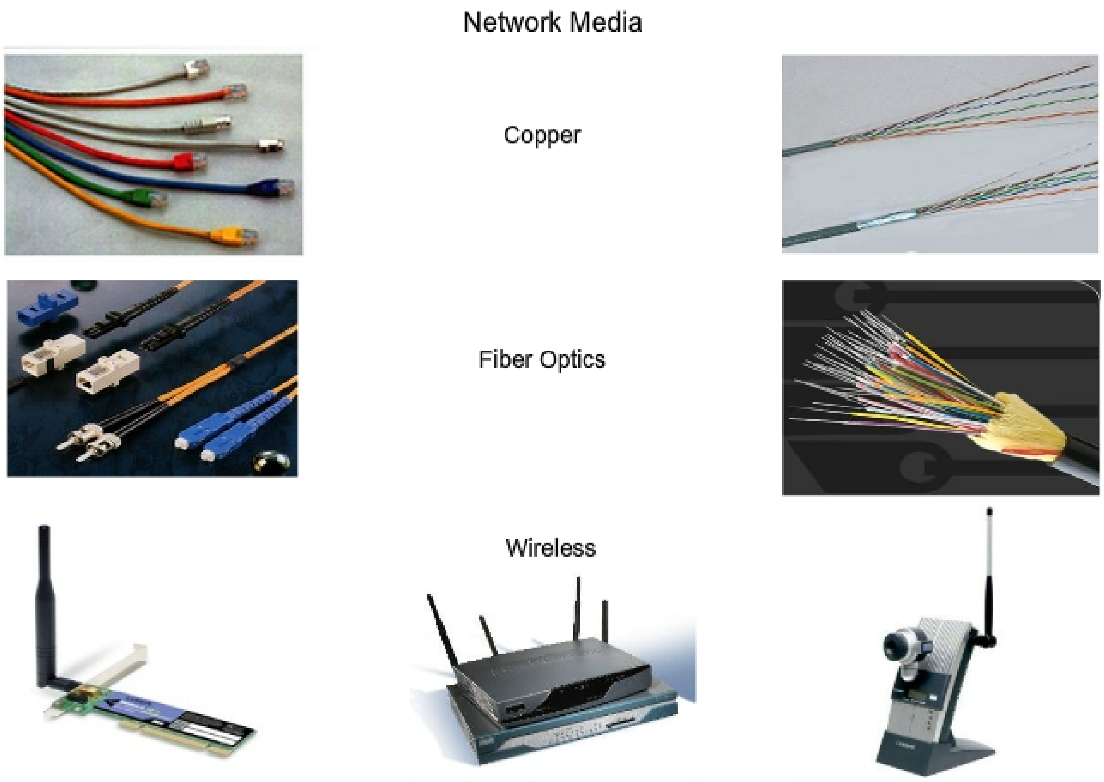
Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted. These media are:

- Metallic wires within cables
- Glass or plastic fibers (fiber optic cable)
- Wireless transmission

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media has the same characteristics and is appropriate for the same purpose. Criteria for choosing a network media are:

- The distance the media can successfully carry a signal.
- The environment in which the media is to be installed.
- The amount of data and the speed at which it must be transmitted.
- The cost of the media and installation



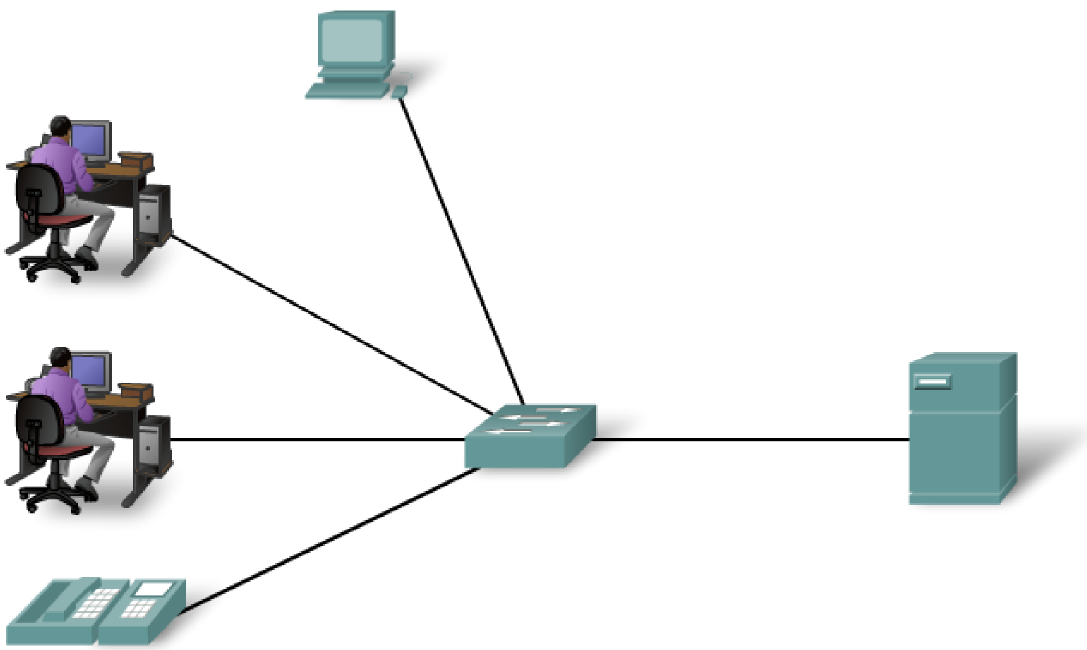
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.2 LANs, WANs, and Internetworks
2.2.1 Local Area Networks

Page 1:
Networks infrastructures can vary greatly in terms of:

- The size of the area covered
- The number of users connected
- The number and types of services available

An individual network usually spans a single geographical area, providing services and applications to people within a common organizational structure, such as a single business, campus or region. This type of network is called a Local Area Network (LAN). A LAN is usually administered by a single organization. The administrative control that governs the security and access control policies are enforced on the network level.

A network serving a home, building or campus is considered a Local Area Network (LAN).



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.2 LANs, WANs, and Internetworks
2.2.2 Wide Area Networks

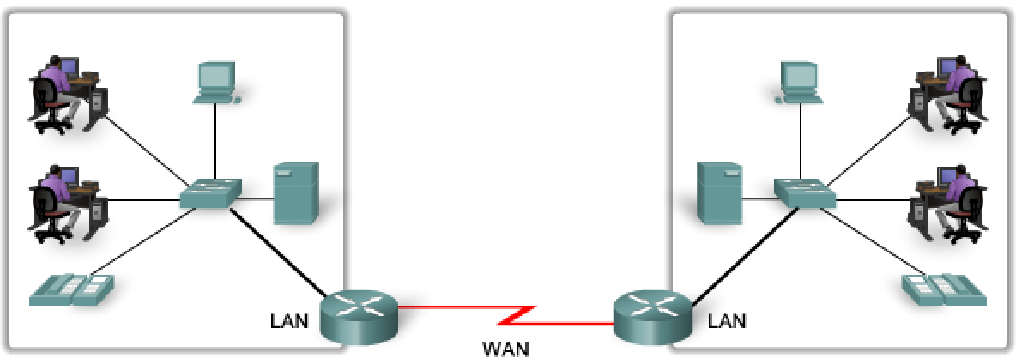
Page 1:
When a company or organization has locations that are separated by large geographical distances, it may be necessary to use a telecommunications service provider (TSP) to interconnect the LANs at the different locations. Telecommunications service providers operate large regional networks that can span long distances. Traditionally, TSPs transported voice and data communications on separate networks. Increasingly, these providers are offering converged information network services to their subscribers.

Individual organizations usually lease connections through a telecommunications service provider network. These networks that connect LANs in geographically separated locations are referred to as Wide Area Networks (WANs). Although the organization maintains all of the policies and administration of the LANs at both ends of the connection, the policies within the communications service provider network are controlled by the TSP.

WANs use specifically designed network devices to make the interconnections between LANs. Because of the importance of these devices to the network, configuring, installing and maintaining these devices are skills that are integral to the function of an organization's network.

LANs and WANs are very useful to individual organizations. They connect the users within the organization. They allow many forms of communication including exchange e-mails, corporate training, and other resource sharing.

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.2 LANs, WANs, and Internetworks
2.2.3 The Internet - A Network of Networks

Page 1:
Although there are benefits to using a LAN or WAN, most of us need to communicate with a resource on another network, outside of our local organization.

Examples of this type of communication include:
- Sending an e-mail to a friend in another country
- Accessing news or products on a website
- Getting a file from a neighbor's computer
- Instant messaging with a relative in another city
- Following a favorite sporting team's performance on a cell phone

Internetwork

A global mesh of interconnected networks (internetworks) meets these human communication needs. Some of these interconnected networks are owned by large public and private organizations, such as government agencies or industrial enterprises, and are reserved for their exclusive use. The most well-known and widely used publicly-accessible internetwork is the Internet.

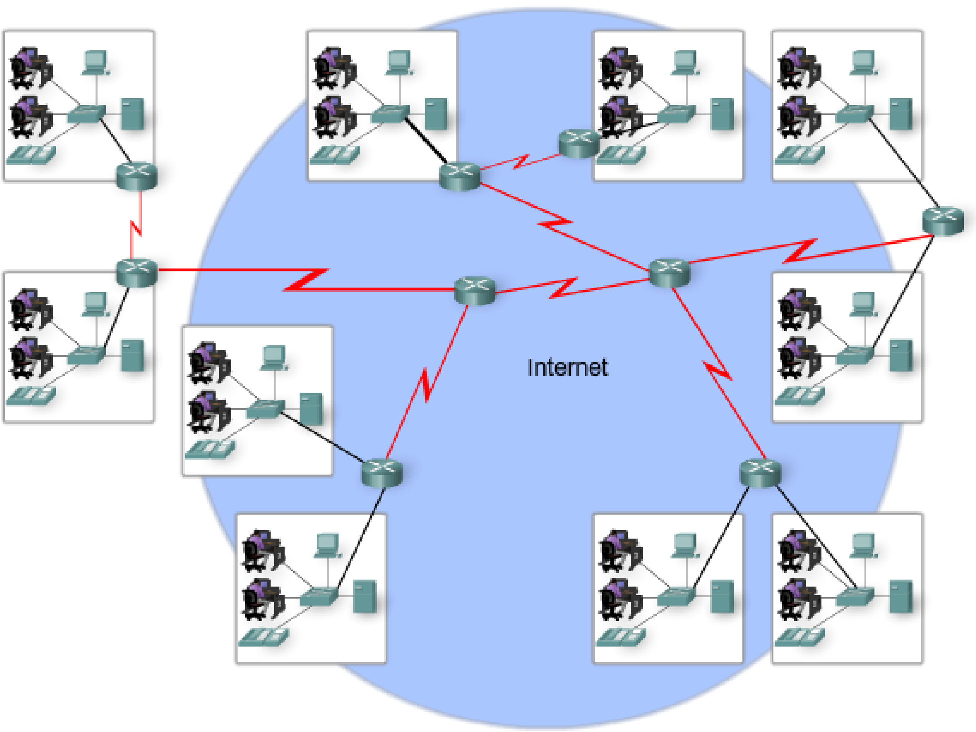
The Internet is created by the interconnection of networks belonging to Internet Service Providers (ISPs). These ISP networks connect to each other to provide access for millions of users all over the world. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and protocols as well as the cooperation of many network administration agencies.

Intranet

The term intranet is often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.

Note: The following terms may be interchangeable: internetwork, data network, and network. A connection of two or more data networks forms an internetwork - a network of networks. It is also common to refer to an internetwork as a data network - or simply as a network - when considering communications at a high level. The usage of terms depends on the context at the time and terms may often be interchanged.

LANs and WANs may be connected into internetworks.



CCNA Exploration - Network Fundamentals

2 Communicating over the Network

2.2 LANs, WANs, and Internetworks

2.2.4 Network Representations

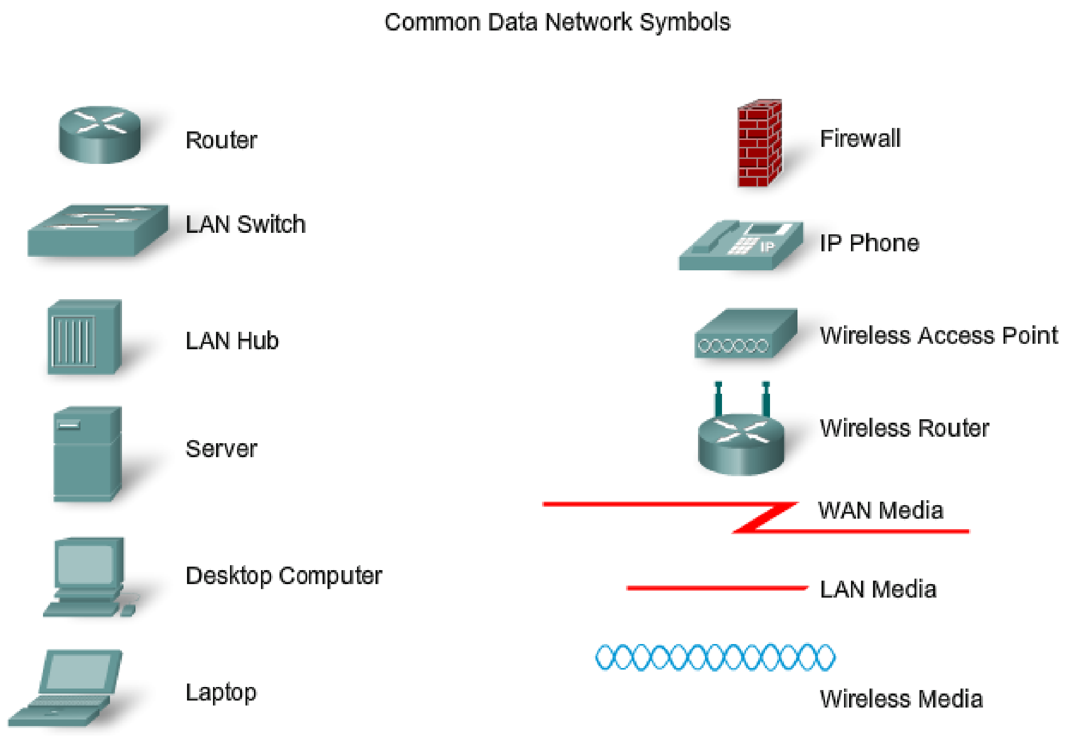
Page 1:
When conveying complex information such as the network connectivity and operation of a large internetwork, it is helpful to use visual representations and graphics. Like any other language, the language of networking uses a common set of symbols to represent the different end devices, network devices and media. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network. Throughout this course and labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are:

Network Interface Card - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC.

Physical Port - A connector or outlet on a networking device where the media is connected to a host or other networking device.

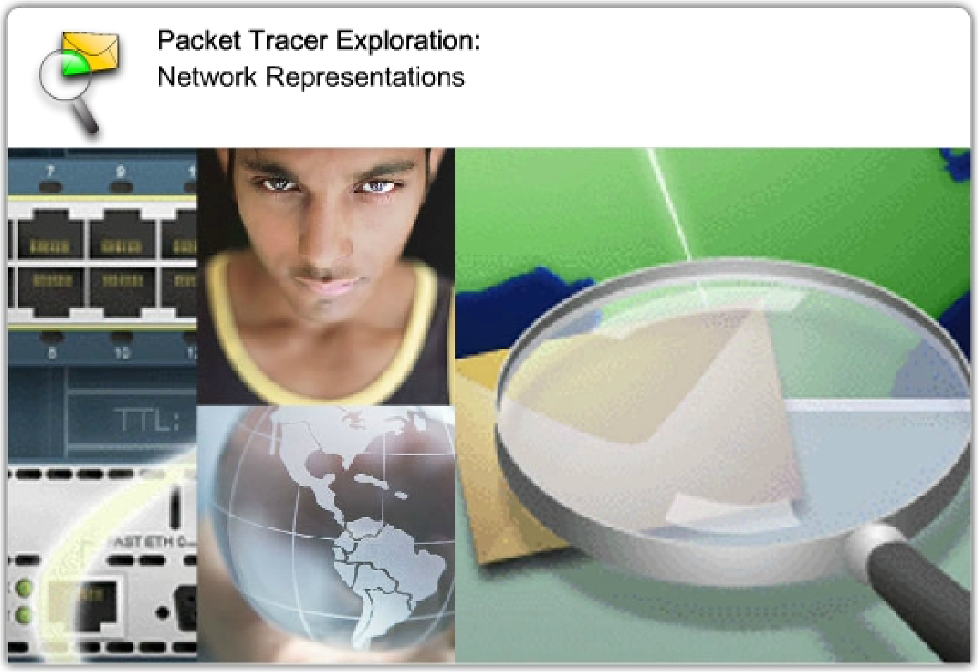
Interface - Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.2 LANs, WANs, and Internetworks
2.2.4 Network Representations

Page 2:
In this activity, you will gain experience with data network symbols by creating a simple logical topology.

Click the Packet Tracer icon for more details.



File: 2.2.4 – pka.pka

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.2 LANs, WANs, and Internetworks
2.2.5 Activity - Using NeoTrace™ to View Internetworks

Page 1:
In this activity, you will observe the flow of information across the Internet. This activity should be performed on a computer that has Internet access and access to a command line. You will use the Windows embedded **tracert** utility and then the more enhanced NeoTrace program. This lab also assumes the installation of NeoTrace.

Click the Lab Icon for more details.

File: 2.2.5 - lab - Using NoeTrace to view Internetworks.pdf

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.3 Protocols
2.3.1 Rules that Govern Communications

Page 1:
All communication, whether face-to-face or over a network, is governed by predetermined rules called protocols. These protocols are specific to the characteristics of the conversation. 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.

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

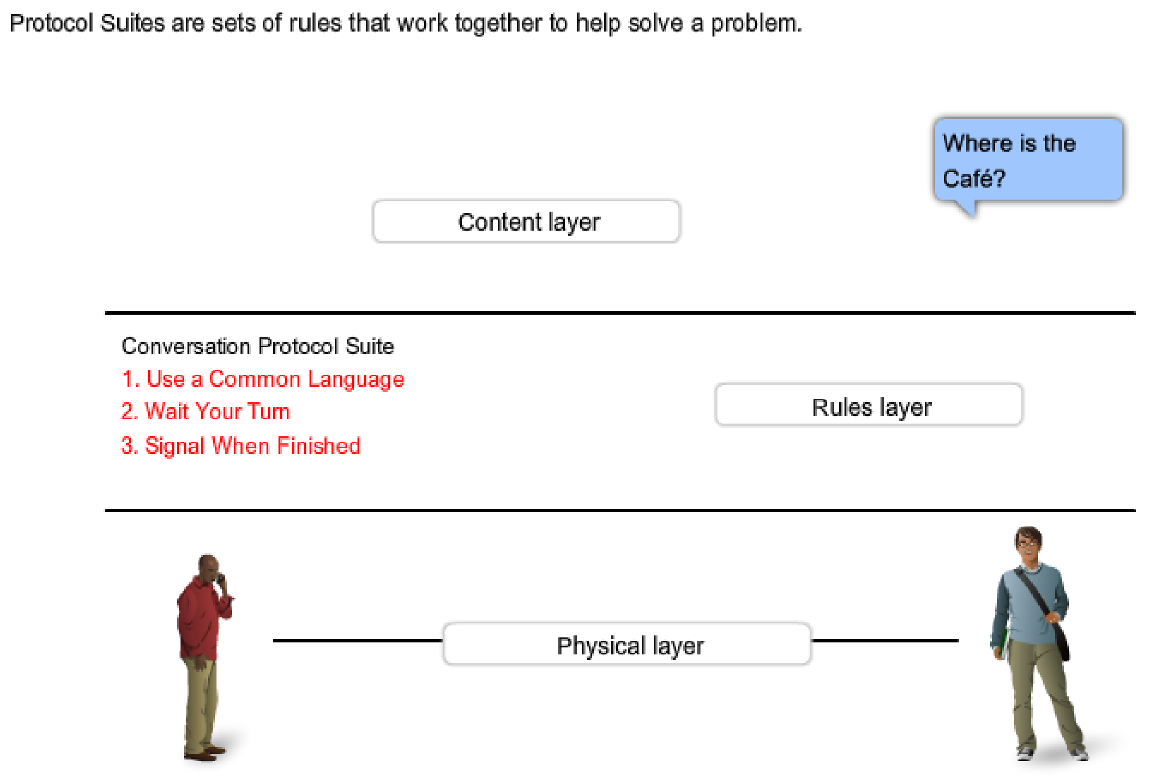
Successful communication between hosts on a network requires the interaction of many different protocols. A group of inter-related protocols that are necessary to perform a communication function is called a protocol suite. These protocols are implemented in software and hardware that is loaded on each host and network device.

One of the best ways to visualize how all of the protocols interact on a particular host is to view it as a stack. A protocol stack shows how the individual protocols within the suite are implemented on the host. The protocols are viewed as a layered hierarchy, 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 and the user interface.

Using layers to describe face-to-face communication

For example, consider two people communicating face-to-face. As the figure shows, we can use three layers to describe this activity. At the bottom layer, the Physical layer, we have two people, each with a voice that can utter words aloud. At the second layer, the Rules layer, we have an agreement to speak in a common language. At the top layer, the Content layer, we have the words actually spoken-the content of the communication.

Were we to witness this conversation, we would not actually see "layers" floating in space. It is important to understand that the use of layers is a model and, as such, it provides a way to conveniently break a complex task into parts and describe how they work.

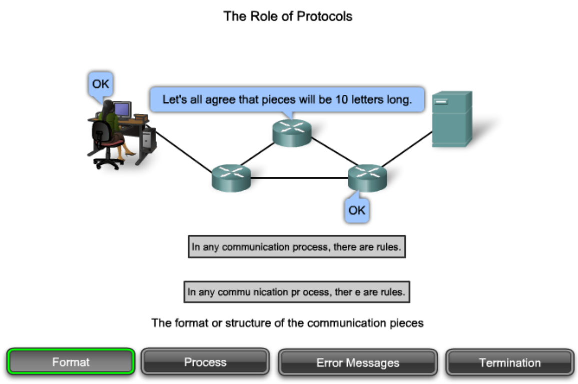


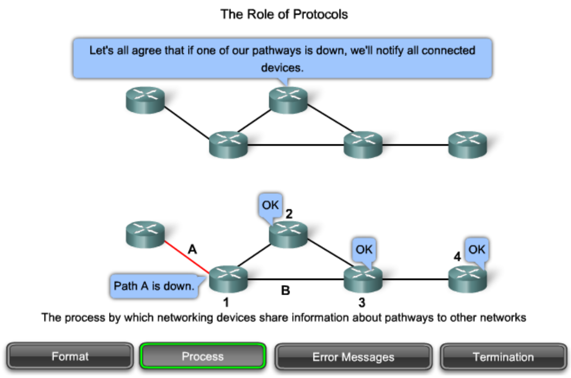
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.3 Protocols
2.3.2 Network Protocols

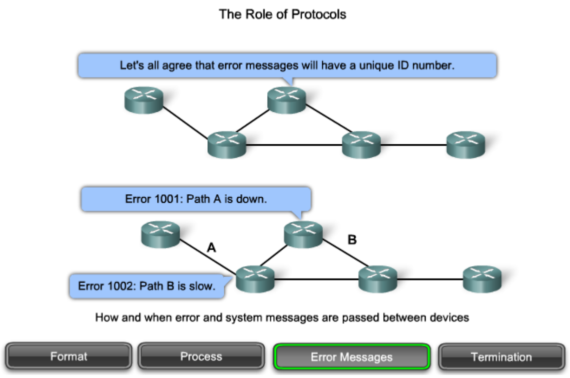
Page 1:
At the human level, some communication rules are formal and others are simply understood, or implicit, based on custom and practice. For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions.

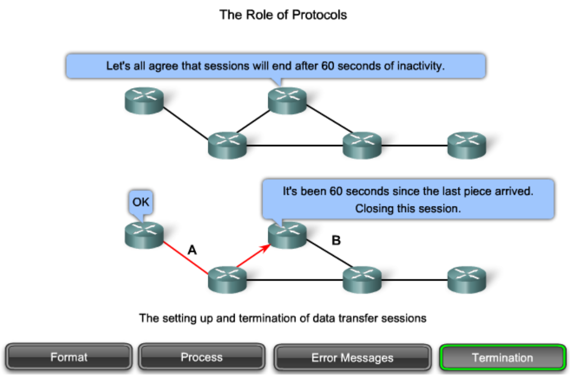
Networking protocol suites describe processes such as:
- The format or structure of the message
- The method by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions

Individual protocols in a protocol suite may be vendor-specific and 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.







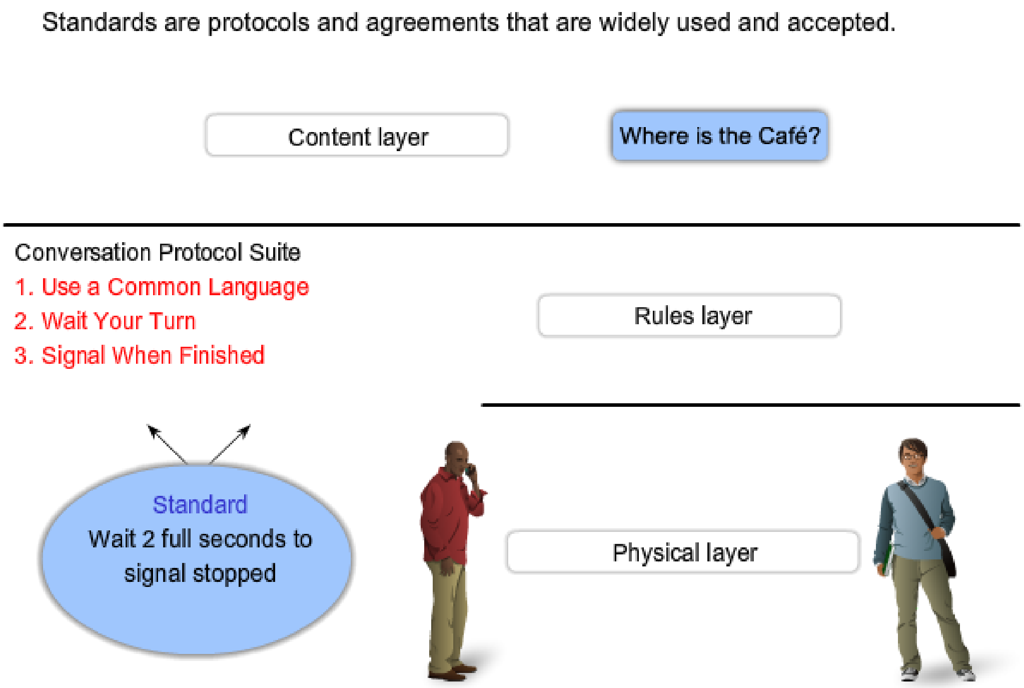


CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.3 Protocols
2.3.3 Protocol Suites and Industry Standards

Page 1:
Often, many of the protocols that comprise a protocol suite reference other widely utilized protocols or industry standards. A standard is a process or protocol that has been endorsed by the networking industry and ratified by a standards organization, such as the Institute of Electrical and Electronics Engineers (IEEE) or the Internet Engineering Task Force (IETF).

The use of standards in developing and implementing protocols ensures that products from different manufacturers can work together for efficient communications. 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 information will be exchanged.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.3 Protocols
2.3.4 The Interaction of Protocols

Page 1:
An example of the use of a protocol suite in network communications is the interaction between a web server and a web browser. 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 common protocol that governs the way that a web server and a web client interact. HTTP defines the content and formatting of the requests and responses exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. The HTTP protocol relies on other protocols to govern how the messages are transported between 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, to be sent to the destination client. It is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.

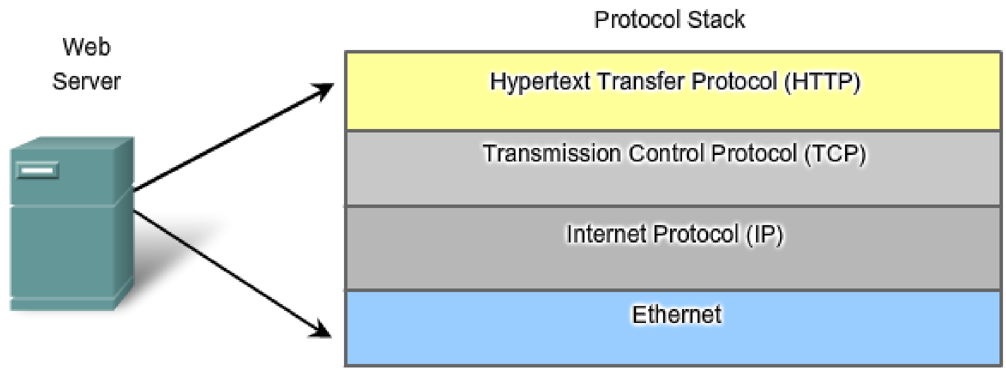
Internetwork Protocol:

The most common internetwork protocol is Internet Protocol (IP). IP is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning the appropriate addresses, and selecting the best path to the destination host.

Network Access Protocols:

Network access protocols describe two primary functions, data link management and the physical transmission of data on the 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 over the media and how they are interpreted by the receiving clients. Transceivers on the network interface cards implement the appropriate standards for the media that is being used.

Interaction



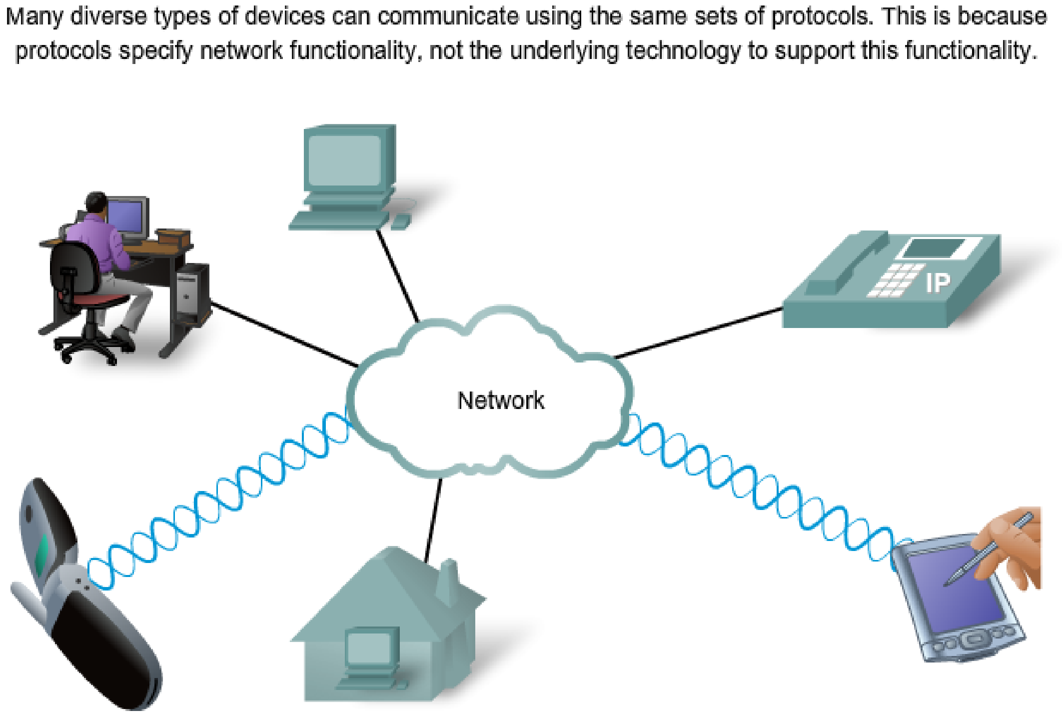
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.3 Protocols
2.3.5 Technology Independent Protocols

Page 1:
Networking protocols describe the functions that occur during network communications. In the face-to-face conversation example, a protocol for communicating might state that in order to signal that the conversation is complete, the sender must remain silent for two full seconds. However, this protocol does not specify *how* the sender is to remain silent for the two seconds.

Protocols generally do not describe *how* to accomplish a particular function. By describing only *what* functions are required of a particular communication rule but not *how* they are to be carried out, the implementation of a particular protocol can be technology-independent.

Looking at the web server example, HTTP does not specify what programming language is used to create the browser, which web server software should be used to serve the web pages, what operating system the software runs on, or the hardware requirements necessary to display the browser. It also does not describe how the server should detect errors, although it does describe what the server should do if an error occurs.

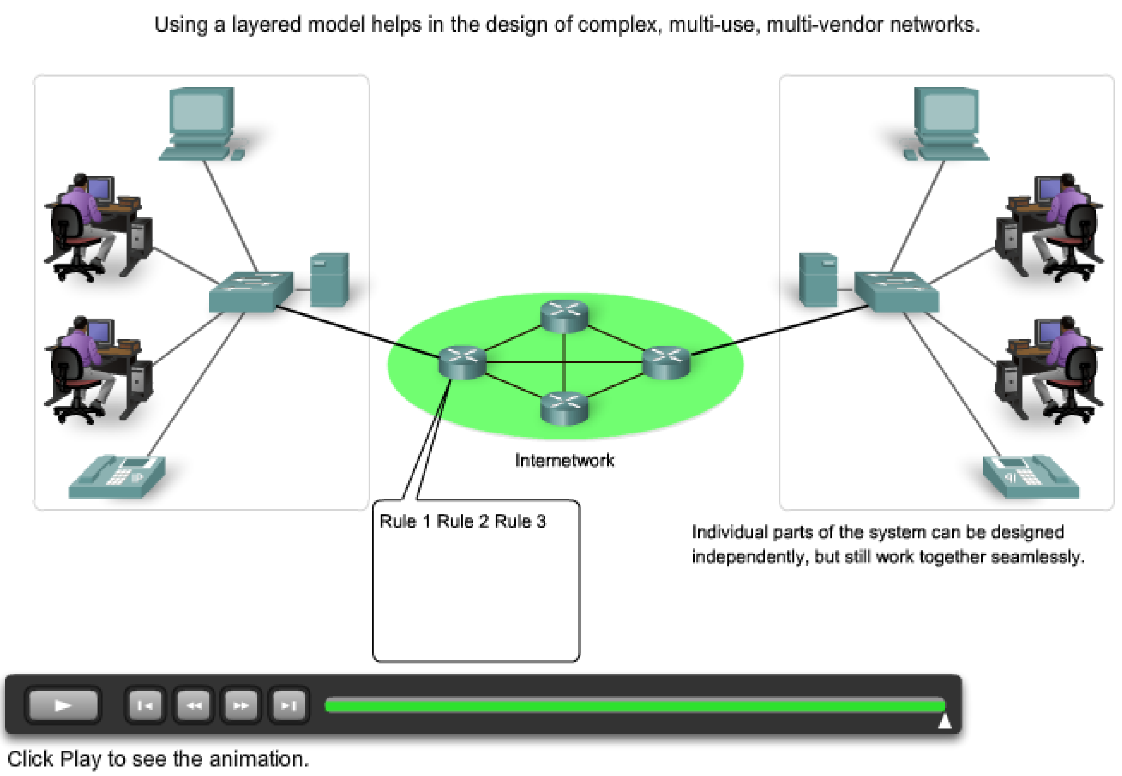
This means that a computer - and other devices, like mobile phones or PDAs - can access a web page stored on any type of web server that uses any form of operating system from anywhere on the Internet.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.1 The Benefits of Using a Layered Model

Page 1:
To visualize the interaction between various protocols, it is common to use a layered model. A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction with the layers above and below it.

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.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.2 Protocol and Reference Models

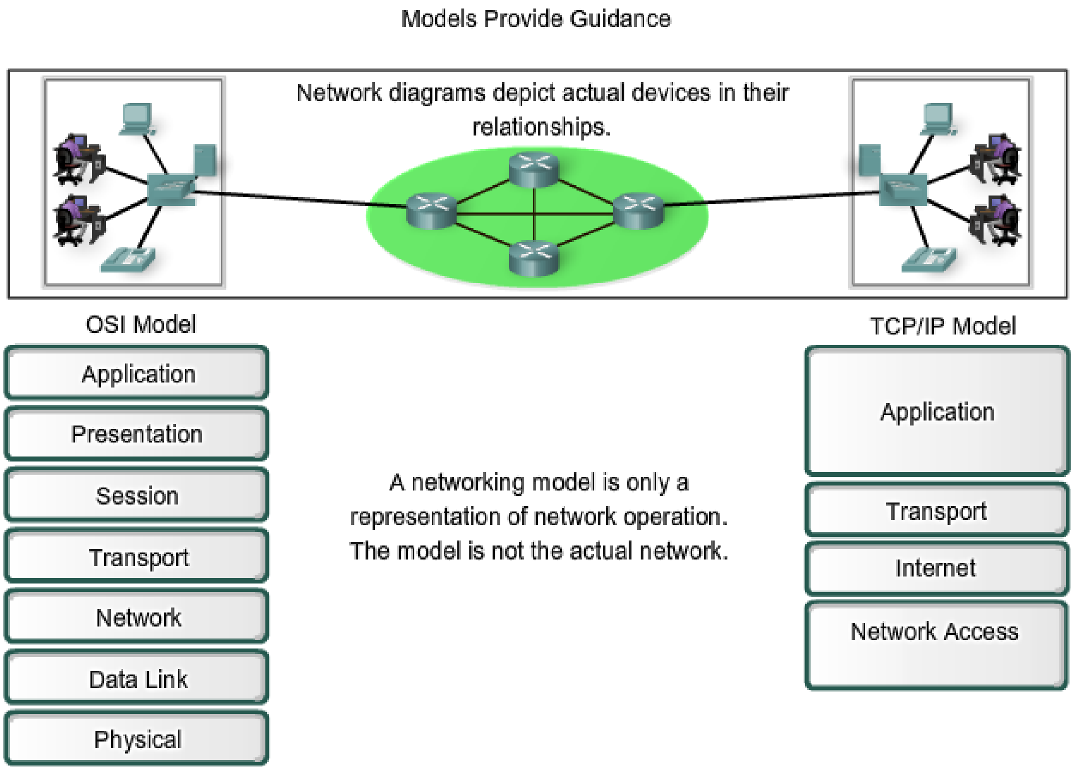
Page 1:
There are two basic types of networking models: protocol models and reference models.

A protocol model provides a model that 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.

A reference model provides a common reference for maintaining consistency within all types of network protocols and services. 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 process involved.

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

Although 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.



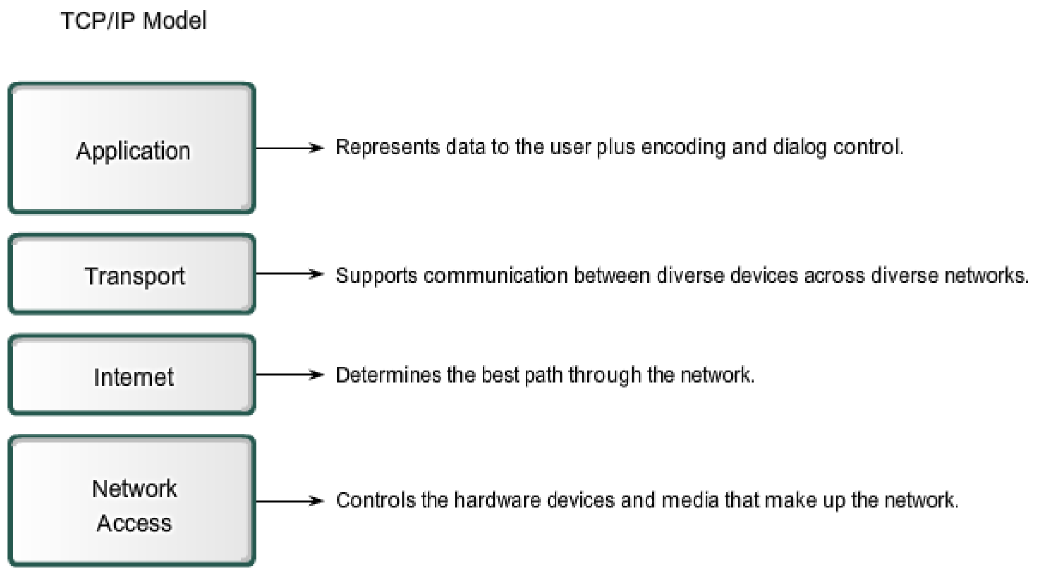
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.3 The TCP/IP Model

Page 1:
The first layered protocol model for internetwork communications was created in the early 1970s and is referred to as the Internet model. 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, since 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 documents. These documents are called Requests for Comments (RFCs). They 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 Internet Engineering Task Force (IETF).

TCP/IP model



CCNA Exploration - Network Fundamentals

2 Communicating over the Network

2.4 Using Layered Models

2.4.4 The Communication Process

Page 1:
The TCP/IP model describes the functionality of the protocols that make up the TCP/IP protocol suite. These protocols, which are implemented on both the sending and receiving hosts, interact to provide end-to-end delivery of applications over a network.

A complete communication process includes these steps:

1. Creation of data at the Application layer of the originating source end device

2. Segmentation and encapsulation of data as it passes down the protocol stack in the source end device

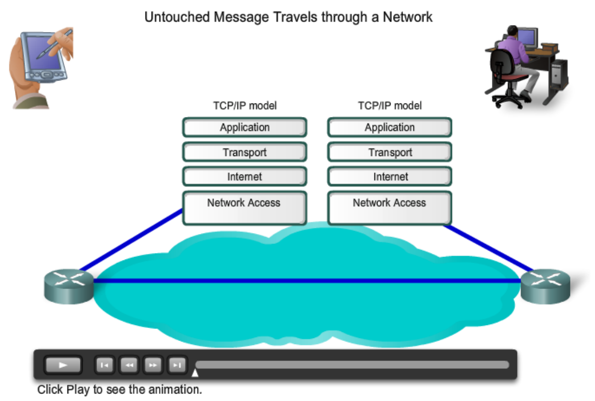
3. Generation of the data onto the media at the Network Access layer of the stack

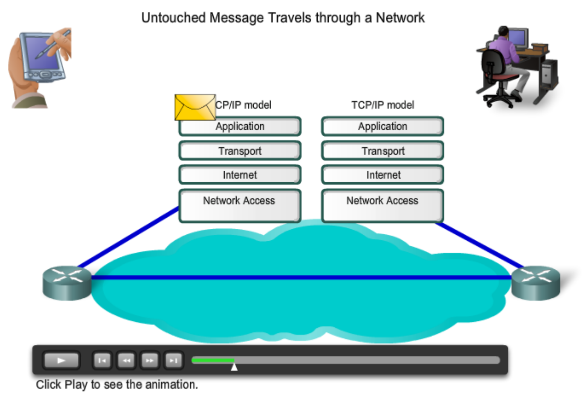
4. Transportation of the data through the internetwork, which consists of media and any intermediary devices

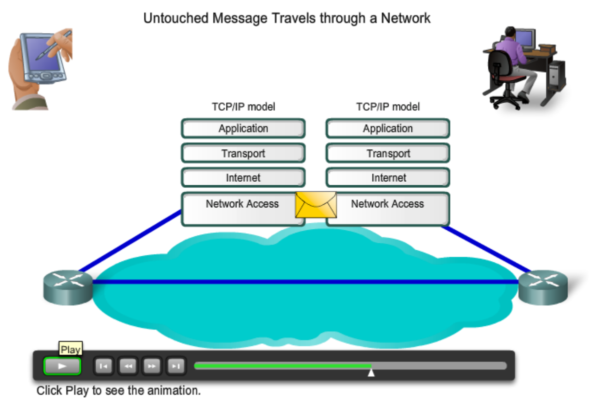
5. Reception of the data at the Network Access layer of the destination end device

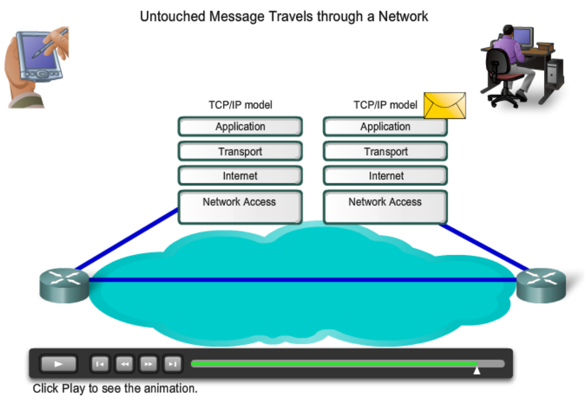
6. Decapsulation and reassembly of the data as it passes up the stack in the destination device

7. Passing this data to the destination application at the Application layer of the destination end device







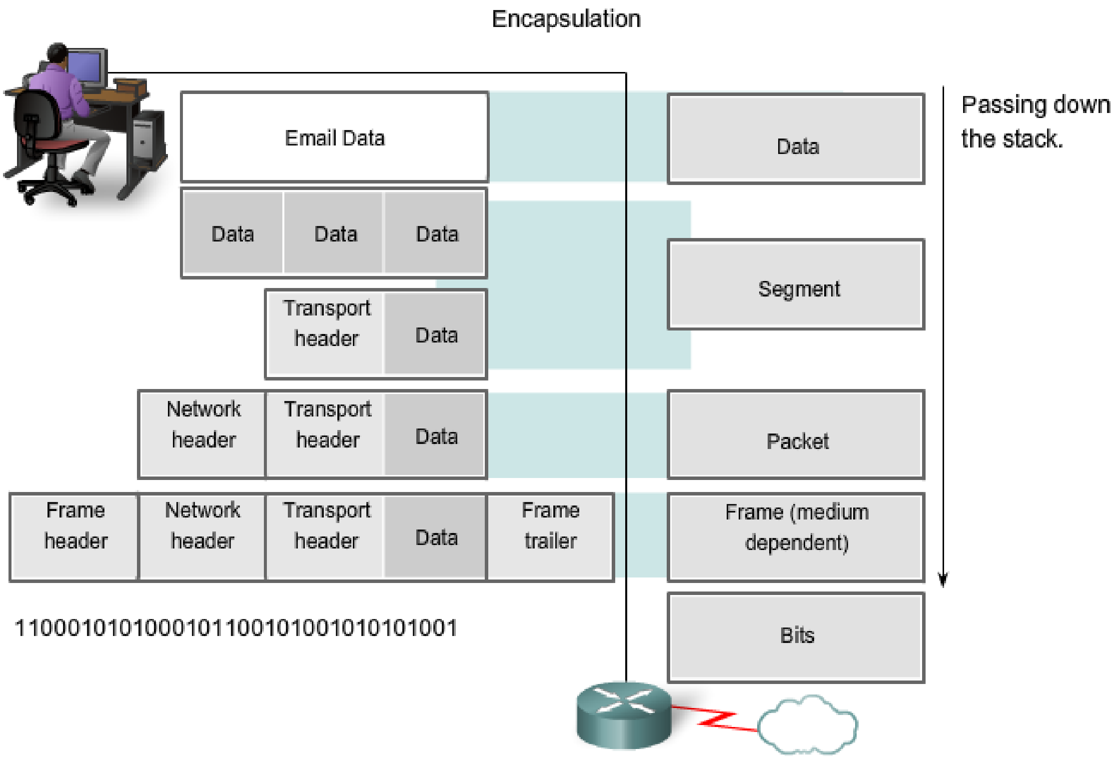


CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.5 Protocol Data Units and Encapsulation

Page 1:
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 appearance. 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.

- Data - The general term for the PDU used at the Application layer
- Segment - Transport Layer PDU
- Packet - Internetwork Layer PDU
- Frame - Network Access Layer PDU
- Bits - A PDU used when physically transmitting data over the medium



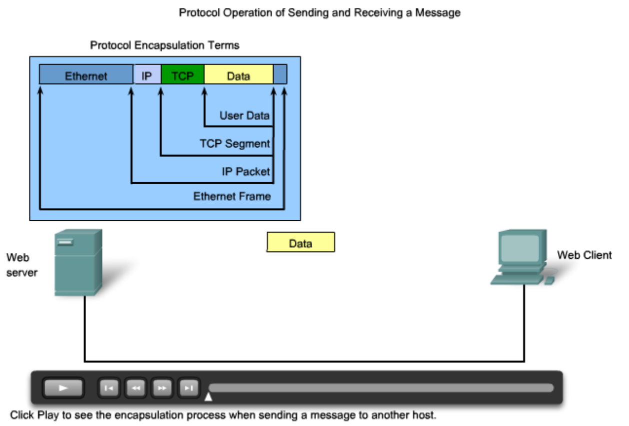
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.6 The Sending and Receiving Process

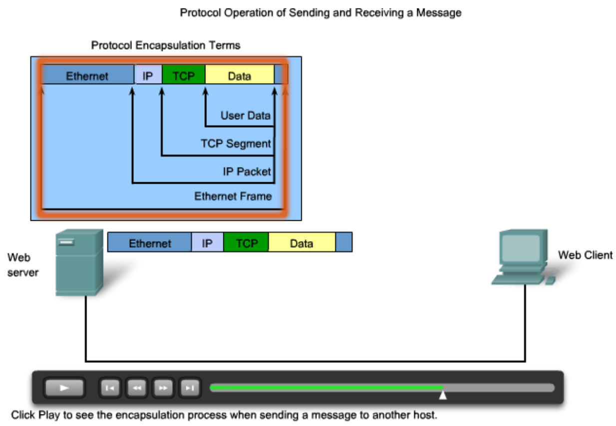
Page 1:
When sending messages on a network, the protocol stack on a host operates from top to bottom. In the web server example, we can use the TCP/IP model to illustrate the process of sending an HTML web page to a client.

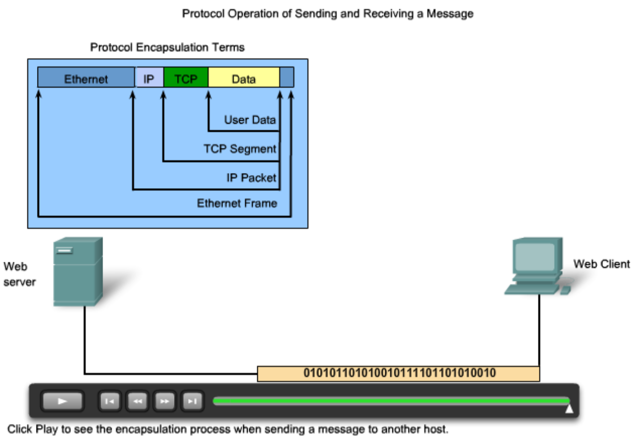
The Application layer protocol, HTTP, begins the process by delivering the HTML formatted web page data to the Transport layer. There the application data is broken into TCP segments. Each TCP segment is given a label, called a header, containing information about which process running on the destination computer should receive the message. It also contains the information to enable 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 Ethernet protocol 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 Ethernet media by the server NIC.

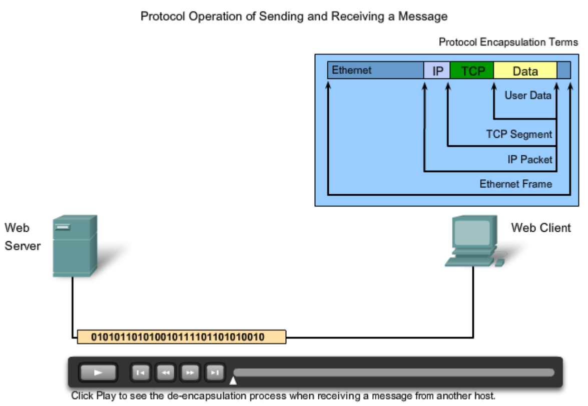


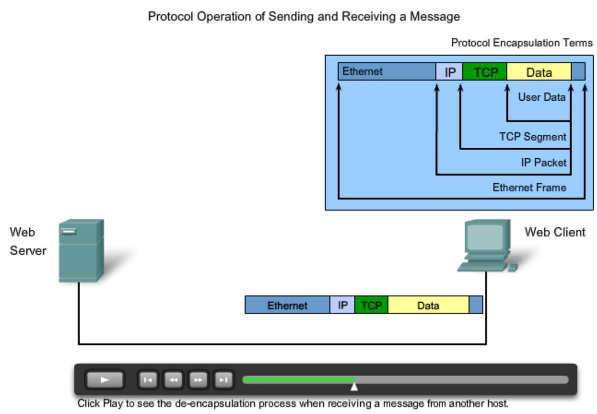


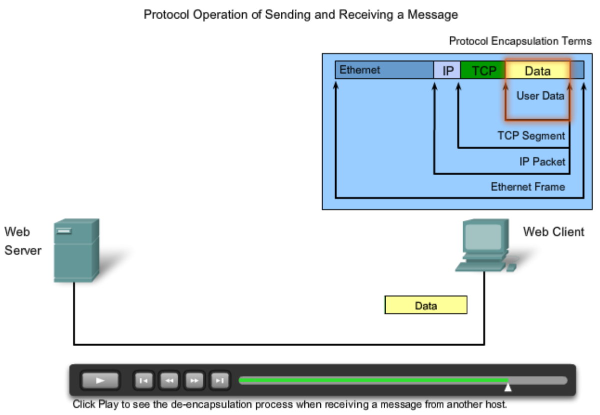


CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.6 The Sending and Receiving Process

Page 2:
This process is reversed at the receiving host. The data is decapsulated as it moves up the stack toward the end user application.







CCNA Exploration - Network Fundamentals

2 Communicating over the Network

2.4 Using Layered Models

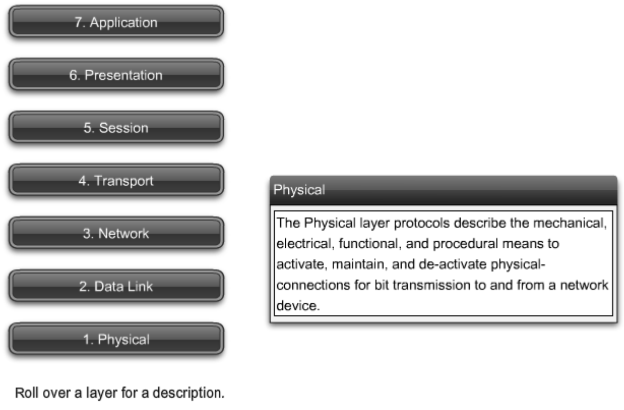
2.4.7 The OSI Model

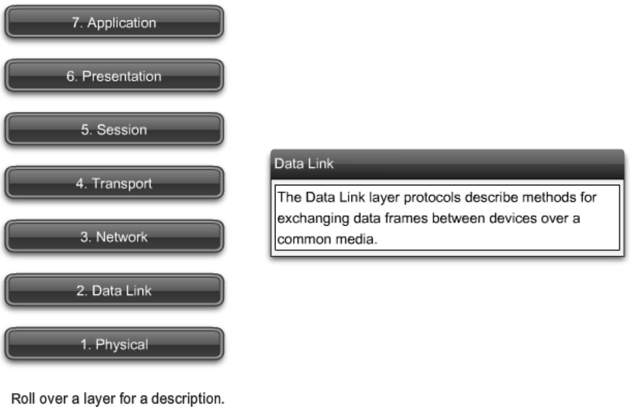
Page 1:
Initially the OSI model was designed by the International Organization for Standardization (ISO) to provide a framework on which to build a suite of open systems protocols. The vision was that this set of protocols would be used to develop an international network that would not be dependent on proprietary systems.

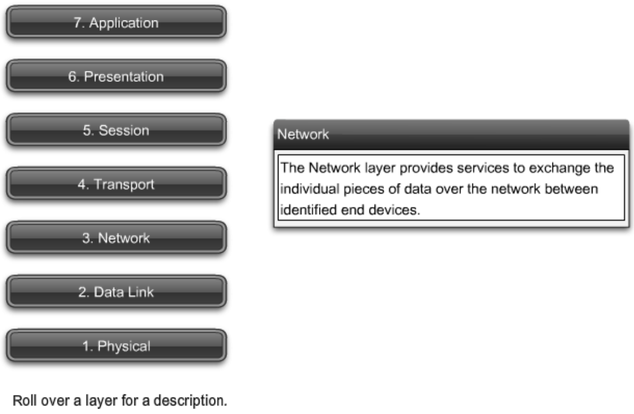
Unfortunately, the speed at which the TCP/IP based Internet was adopted, and the rate at which it expanded, caused the OSI Protocol Suite development and acceptance to lag behind. Although few of the protocols developed using the OSI specifications are in widespread use today, the seven-layer OSI model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

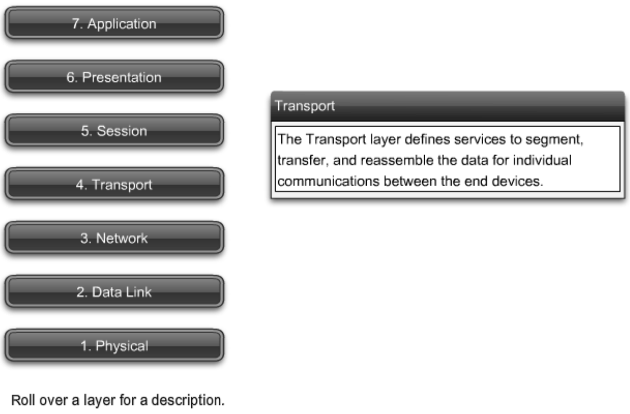
As a reference model, the OSI model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below it. Although the content of this course will be structured around the OSI Model the focus of discussion will be the protocols identified in the TCP/IP protocol stack.

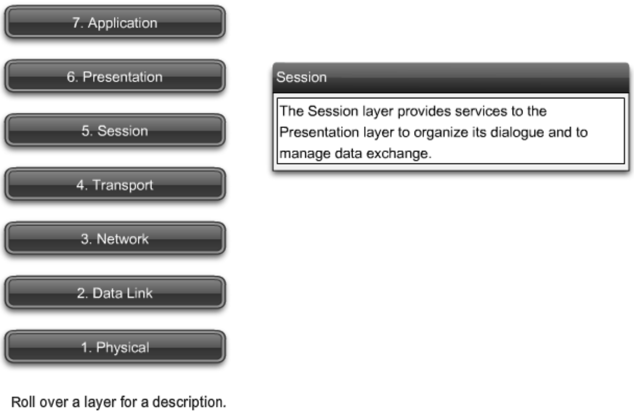
Note that whereas the TCP/IP model layers are referred to only by name, the seven OSI model layers are more often referred to by number than by name.



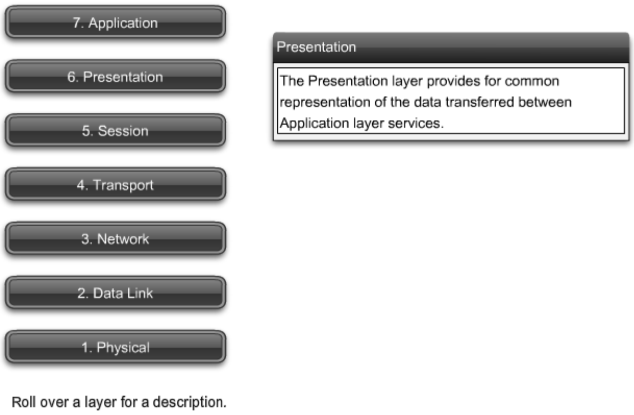




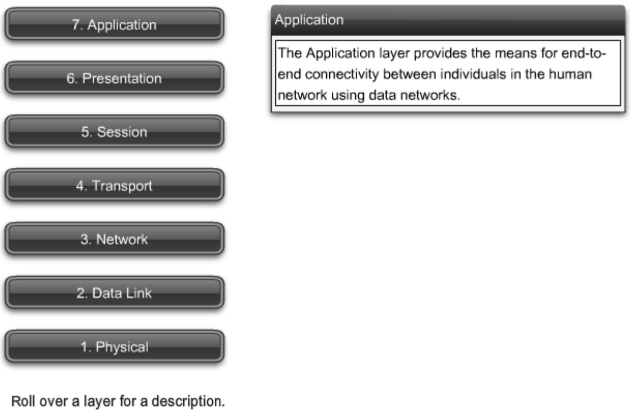




7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Roll over a layer for a description.
Session
The Session layer provides services to the Presentation layer to organize its dialogue and to manage data exchange.



7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Roll over a layer for a description.
Presentation
The Presentation layer provides for common representation of the data transferred between Application layer services.



7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Roll over a layer for a description.
Application
The Application layer provides the means for end-to-end connectivity between individuals in the human network using data networks.

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.8 Comparing the OSI Model with the TCP/IP Model

Page 1:
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 discreet functions that need to occur at these layers.

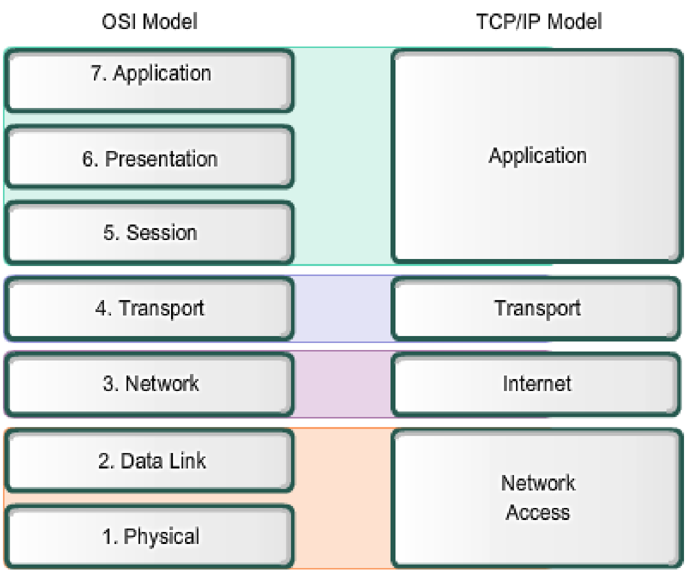
At the Network Access Layer, the TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium; it only describes the handoff from the Internet Layer to the physical network protocols. The OSI Layers 1 and 2 discuss the necessary procedures to access the media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

The key parallels between the two network models occur at the OSI model Layers 3 and 4. OSI Model Layer 3, the Network layer, almost universally is used to discuss and document the range of processes that occur in all data networks to address and route messages through an internetwork. The Internet Protocol (IP) is the TCP/IP suite protocol that includes the functionality described at Layer 3.

Layer 4, the Transport layer of the OSI model, is often used to describe general services or functions that manage individual conversations between source and destination hosts. These functions include acknowledgement, error recovery, and sequencing. At this layer, the TCP/IP protocols Transmission Control Protocol (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 need to access networks for communications.

Comparing the OSI and TCP/IP models

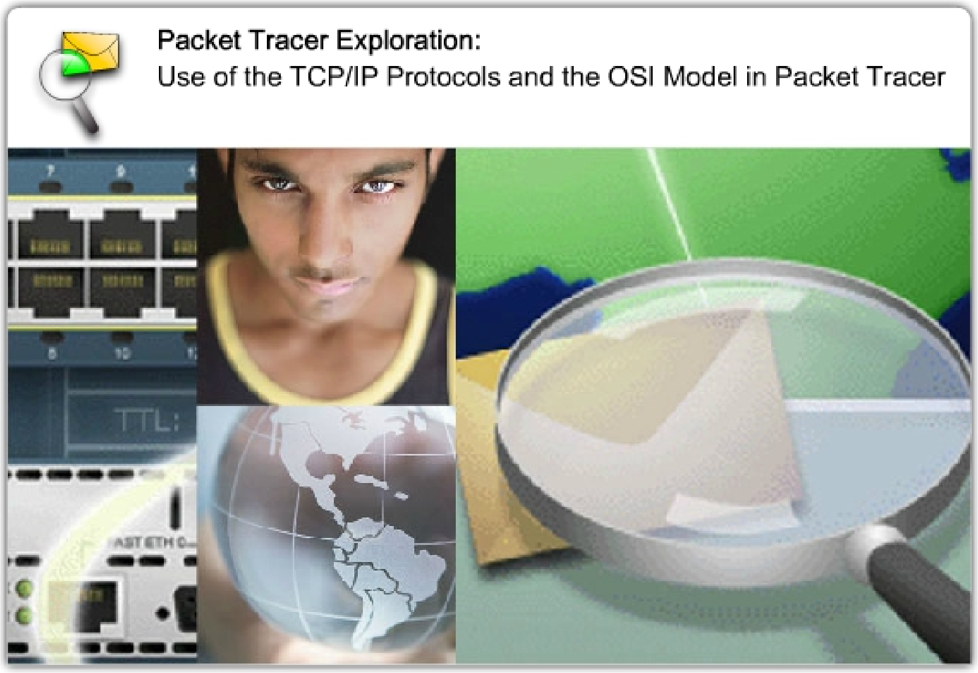


The key parallels are in the Transport and Network layers.

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.4 Using Layered Models
2.4.8 Comparing the OSI Model with the TCP/IP Model

Page 2:
In this activity, you will see how Packet Tracer uses the OSI Model as a reference to display the encapsulation details of a variety of the TCP/IP protocols.

Click the Packet Tracer icon for more details.

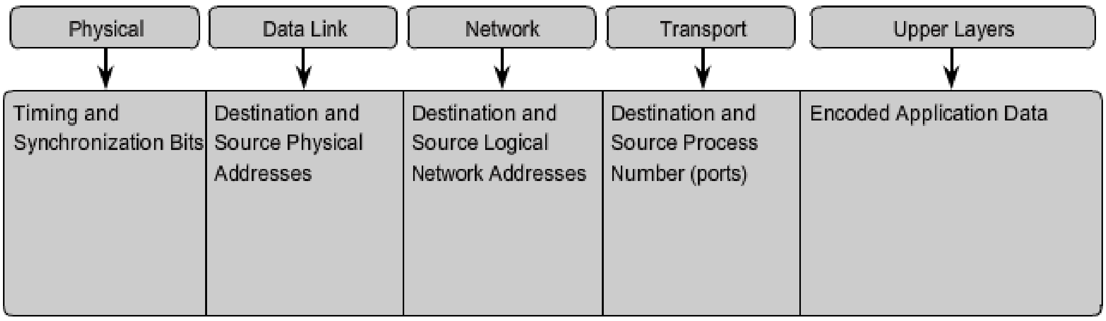


File: 2.4.8 - pka.pka

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.5 Network Addressing
2.5.1 Addressing in the Network

Page 1:
The OSI model describes the processes of encoding, formatting, segmenting, and encapsulating data for transmission over the network. A data stream that is sent from a source to a destination can be divided into pieces and interleaved with messages traveling from other hosts to other destinations. Billions of these pieces of information are traveling over a network at any given time. It is critical for each piece of data to contain enough identifying information to get it to the correct destination.

There are various types of addresses that must be included to successfully deliver the data from a source application running on one host to the correct destination application running on another. Using the OSI model as a guide, we can see the different addresses and identifiers that are necessary at each layer.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network

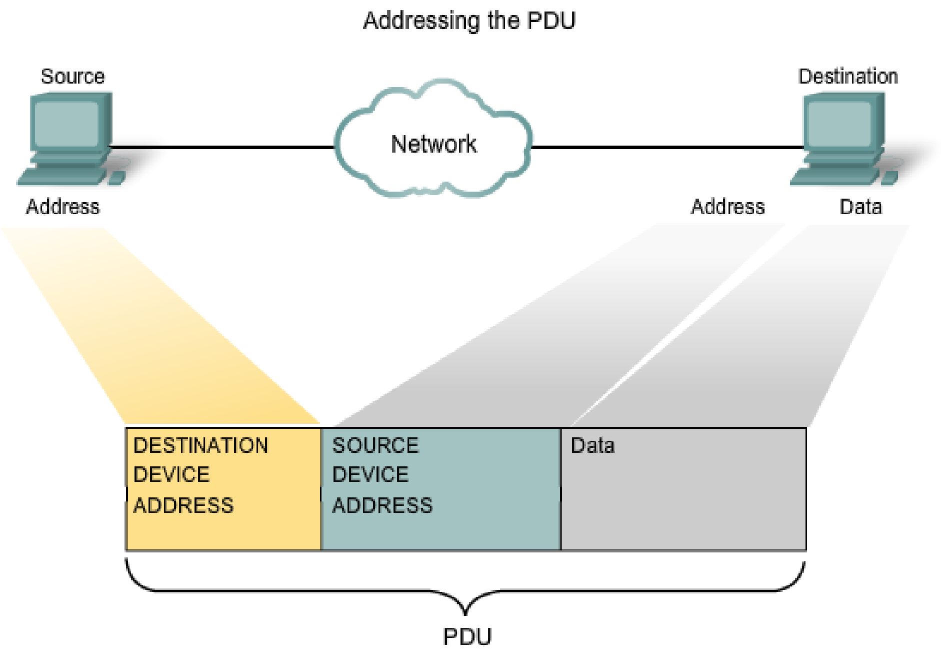
2.5 Network Addressing

2.5.2 Getting the Data to the End Device

Page 1:

During the process of encapsulation, address identifiers are added to the data as it travels down the protocol stack on the source host. Just as there are multiple layers of protocols that prepare the data for transmission to its destination, there are multiple layers of addressing to ensure its delivery.

The first identifier, the host physical address, is contained in the header of the Layer 2 PDU, called a frame. Layer 2 is concerned with the delivery of messages on a single local network. The Layer 2 address is unique on the local network and represents the address of the end device on the physical media. In a LAN using Ethernet, this address is called the Media Access Control (MAC) address. When two end devices communicate on the local Ethernet network, the frames that are exchanged between them contain the destination and source MAC addresses. Once a frame is successfully received by the destination host, the Layer 2 address information is removed as the data is decapsulated and moved up the protocol stack to Layer 3.



The Protocol Data Unit header contains device address fields.

CCNA Exploration - Network Fundamentals
2 Communicating over the Network

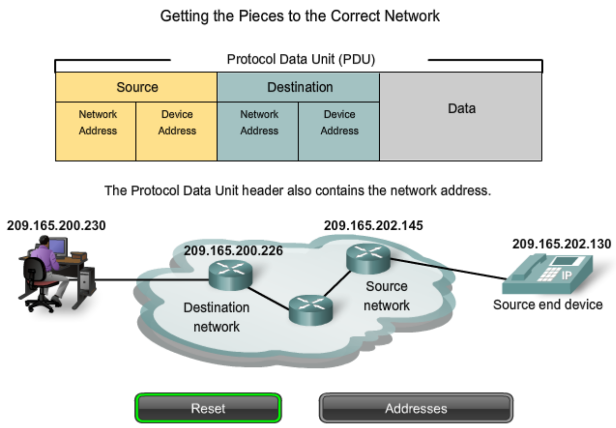
2.5 Network Addressing

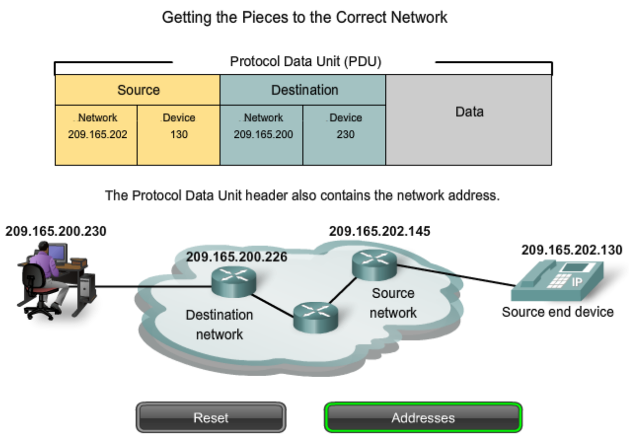
2.5.3 Getting the Data through the Internetwork

Page 1:

Layer 3 protocols are primarily designed to move data from one local network to another local network within an internetwork. Whereas Layer 2 addresses are only used to communicate between devices on a single local network, Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks. In the TCP/IP protocol suite, every IP host address contains information about the network where the host is located.

At the boundary of each local network, an intermediary network device, usually a router, decapsulates the frame to read the destination host address contained in the header of the packet, the Layer 3 PDU. Routers use the network identifier portion of this address to determine which path to use to reach the destination host. Once the path is determined, the router encapsulates the packet in a new frame and sends it on its way toward the destination end device. When the frame reaches its final destination, the frame and packet headers are removed and the data moved up to Layer 4.





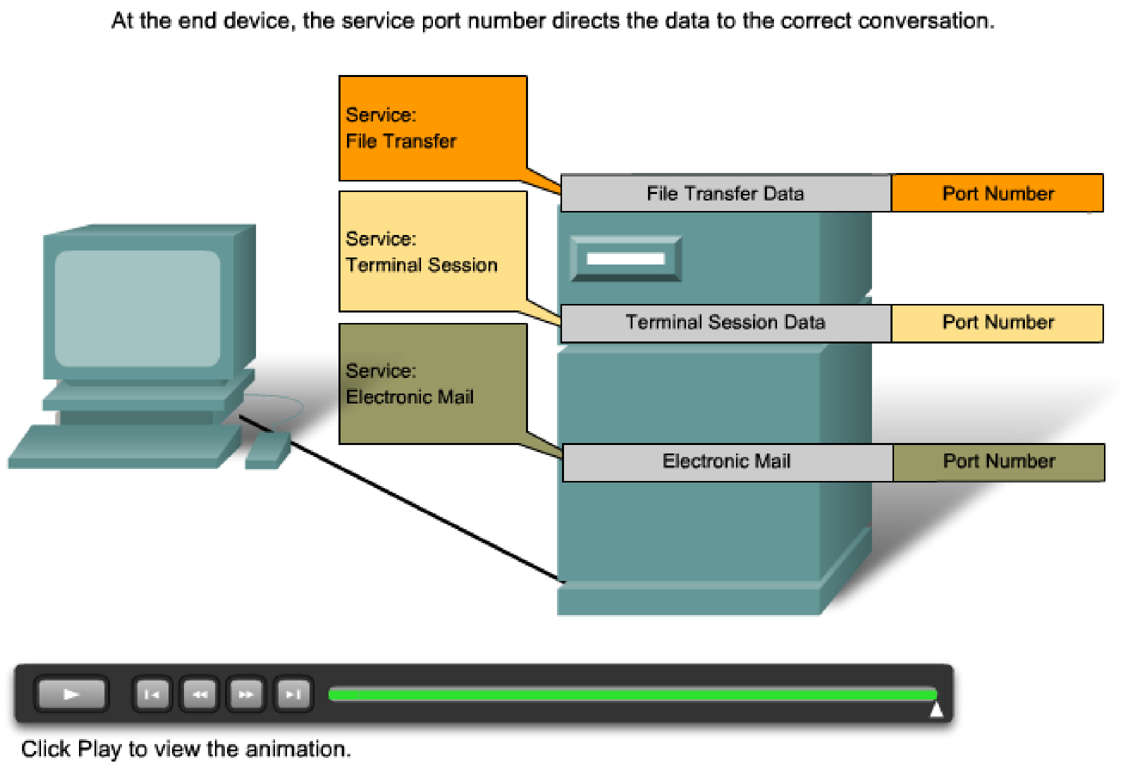
CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.5 Network Addressing
2.5.4 Getting the Data to the Right Application

Page 1:
At Layer 4, information contained in the PDU header does not identify a destination host or a destination network. What it does identify is the specific process or service running on the destination host device that will act on the data being delivered. Hosts, whether they are clients or servers on the Internet, can run multiple network applications simultaneously. People using PCs often have an e-mail client running at the same time as a web browser, an instant messaging program, some streaming media, and perhaps even a game. All these separately running programs are examples of individual processes.

Viewing a web page invokes at least one network process. Clicking a hyperlink causes a web browser to communicate with a web server. At the same time, in the background, an e-mail client may be sending and receiving email, and a colleague or friend may be sending an instant message.

Think about a computer that has only one network interface on it. All the data streams created by the applications that are running on the PC enter and leave through that one interface, yet instant messages do not popup in the middle of word processor document or e-mail showing up in a game.

This is because the individual processes running on the source and destination hosts communicate with each other. Each application or service is represented at Layer 4 by a port number. A unique dialogue between devices is identified with a pair of Layer 4 source and destination port numbers that are representative of the two communicating applications. When the data is received at the host, the port number is examined to determine which application or process is the correct destination for the data.



CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.5 Network Addressing
2.5.5 Warriors of the Net

Page 1:
An entertaining resource to help you visualize networking concepts is the animated movie "Warriors of the Net" by TNG Media Lab. Before viewing the video, there are a few things to consider. First, in terms of concepts you have learned in this chapter, think about when in the video you are on the LAN, on WAN, on intranet, on Internet; and what are end devices versus intermediate devices; how the OSI and TCP/IP models apply; what protocols are involved.

Second, some terms are mentioned in the video which may not be familiar. The types of packets mentioned refers to the type of upper level data (TCP, UDP, ICMP Ping, PING of death) that is encapsulated in the IP Packets (everything is eventually converted into IP Packets). The devices the packet encounters on its journey are router, proxy server, router switch, corporate intranet, the proxy, URL, firewall, bandwidth, hosts, web server.

Third, while port numbers 21, 23, 25, 53, and 80 are referred to explicitly in the video, IP addresses are referred to only implicitly - can you see where? Where in the video might MAC addresses have been involved?

Finally, though all animations often have simplifications in them, there is one outright error in the video. About 5 minutes in, the statement is made "What happens when Mr. IP doesn't receive an acknowledgement, he simply sends a replacement packet." As you will find out in later chapters, this is not a function of the Layer 3 Internet Protocol, which is an "unreliable", best effort delivery protocol, but rather a function of the Transport Layer TCP Protocol.

By the end of this course you will have a much better understanding of the breadth and depth of the concepts depicted in the video. We hope you enjoy it.

Download the movie from http://www.warriorsofthe.net

File: Warriors of the Net (Italian).mp4

CCNA Exploration - Network Fundamentals

2 Communicating over the Network

2.6 Chapter Labs

2.6.1 Lab: Topology Orientation and Building a Small Network

Page 1:
This lab begins by having you construct two small networks. It then shows how they are connected to the larger hands-on lab network used throughout the course. This network is a simplified model of a section of the Internet and will be used to develop your practical networking skills.

The following sequence of labs will introduce the networking terms below. This networking terminology will be studied in detail in subsequent chapters.

Straight-through Cable: Unshielded twisted pair (UTP) copper cable for connecting dissimilar networking devices

Crossover Cable: UTP copper cable for connecting similar networking devices

Serial Cable: Copper cable typical of wide area connections

Ethernet: Dominant local area network technology

MAC Address: Ethernet Layer 2, physical address

IP Address: Layer 3 logical address

Subnet Mask: Required to interpret the IP address

Default Gateway: The IP address on a router interface to which a network sends traffic leaving the local network

NIC: Network Interface Card, the port or interface that allows an end device to participate in a network

Port (hardware): An interface that allows a networking device to participate in network and to be connected via networking media

Port (software): Layer 4 protocol address in the TCP/IP suite

Interface (hardware): A port

Interface (software): A logical interaction point within software

PC: End device

Computer: End device

Workstation: End device

Switch: Intermediate device which makes decision on frames based on Layer 2 addresses (typical Ethernet MAC addresses)

Router: Layer 3, 2, and 1 device which makes decisions on packets based on Layer 3 addresses (typically IPv4 addresses)

Bit: Binary digit, logical 1 or zero, has various physical representations as electrical, optical, or microwave pulses; Layer 1 PDU

Frame: Layer 2 PDU

Packet: Layer 3 PDU

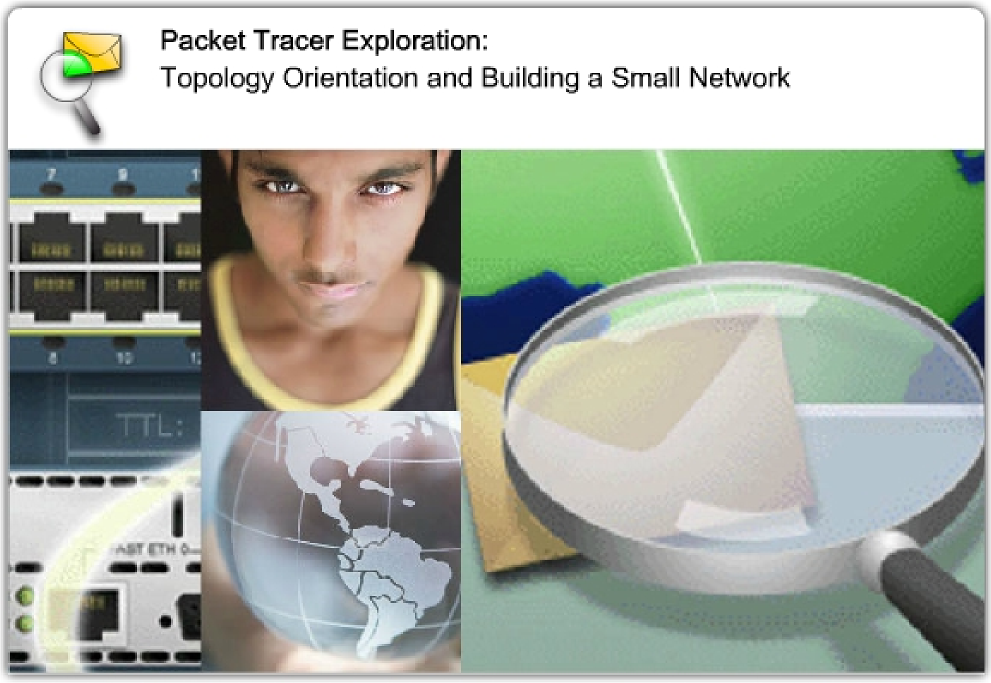
Click the Lab Icon for more details.

File: 2.6.1 - lab - Topology Orientation and Building a Small Network.pdf

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.6 Chapter Labs
2.6.1 Lab: Topology Orientation and Building a Small Network

Page 2:
In this activity, you will use Packet Tracer to complete the Topology Orientation and Building a Small Network lab.

Click the Packet Tracer icon to launch the Packet Tracer activity.



File: 2.6.1 – Pka.pka

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.6 Chapter Labs
2.6.2 Lab: Using Wireshark™ to View Protocol Data Units

Page 1:
In this lab, you will learn to use the very powerful Wireshark tool by capturing ("sniffing") traffic off of the model network.

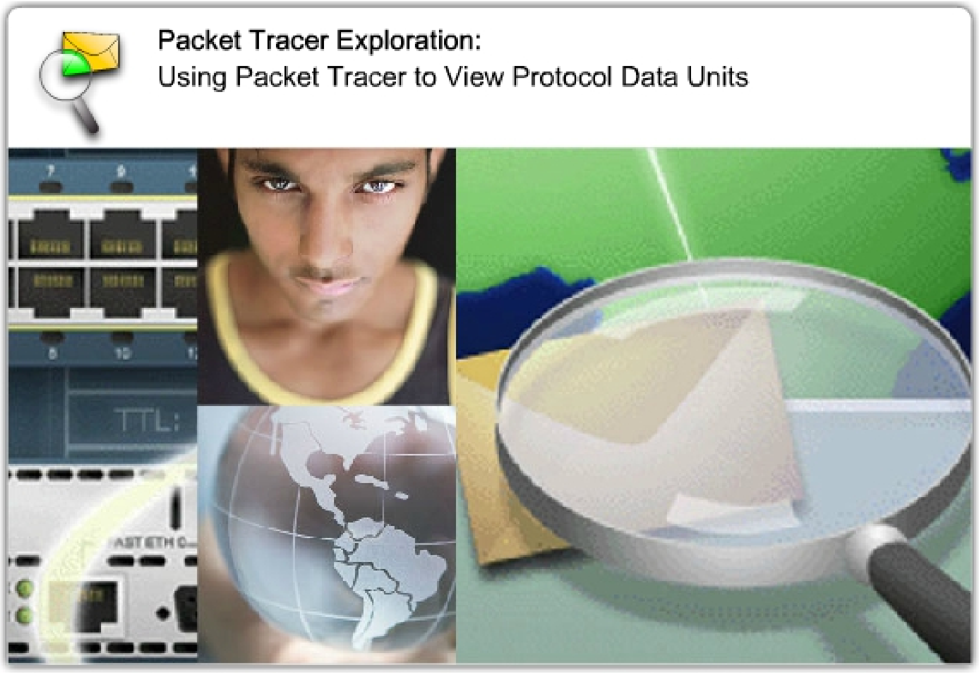
Click the Lab Icon for more details.

File: 2.6.2 - lab - Using Wireshark to View Protocol Data Units.pdf

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.6 Chapter Labs
2.6.2 Lab: Using Wireshark™ to View Protocol Data Units

Page 2:
In this activity, you will use Packet Tracer's Simulation mode to capture and analyze packets from a ping from a PC's command prompt and a web request using a URL.

Click the Packet Tracer icon to launch the Packet Tracer activity.



File: 2.6.2 – Pka.pka

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.7 Chapter Summary
2.7.1 Summary and Review

Page 1:
Data networks are systems of end devices, intermediary devices, and the media connecting the devices, which provide the platform for the human network.

These devices, and the services that operate on them, can interconnect in a global and user-transparent way because they comply with rules and protocols.

The use of layered models as abstractions means that the operations of network systems can be analyzed and developed to cater the needs of future communication services.

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

As it passes down the stack, data is segmented into pieces and encapsulated with addresses and other labels. The process is reversed as the pieces are decapsulated and passed up the destination protocol stack.

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

In this chapter, you learned to:

- Describe the structure of a network, including the devices and media that are necessary for successful communications.
- Explain the function of protocols in network communications.
- Explain the advantages of using a layered model to describe network functionality.
- Describe the role of each layer in two recognized network models: The TCP/IP model and the OSI model.
- Describe the importance of addressing and naming schemes in network communications.

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.7 Chapter Summary
2.7.1 Summary and Review

Page 2:

Use this activity to check your understanding of the main points in this chapter.

- A series of questions will be presented. This is not a quiz and your answers are not recorded.
- Click **Answer** to see the answer.
- Click **Next Question** to go to the next question in the series.

Click Here to Begin

1. List 5 end devices, 6 intermediate devices, and 3 forms of networking media.

Answer

- End devices: desktop computer, laptop computer, server, PDA, cellular mobile phone, printer, security camera, IP phone, electronic point of sale device, automatic teller machine
- Intermediate device: repeater, hub, wireless access point, switch, router, modem, and firewall
- Networking media: copper cable, fiber cable, radio (wireless)

Next Question

2. Compare and contrast the following terms: network, LAN, WAN, internetwork, and the Internet.

Answer

- **Network** – a group of interconnected devices capable of carrying many different types of communications, including traditional computer data, interactive voice, video, and entertainment products.
- **LAN** – a local network, or group of interconnected local networks that are under the same administrative control. In the past, LANs were thought of only as small networks that existed in a single physical location. While LANs can be as small as a single local network installed in a home or small office, LANs now include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations. All of the local networks within a LAN are under one administrative control group that governs the security and access control policies that are in force on the network

Next Question

2. Compare and contrast the following terms: network, LAN, WAN, internetwork, and the Internet.

Answer

- WAN – Telecommunications service providers (TSP) operate large regional networks spanning long distances. Individual organizations usually lease connections through a telecommunications service provider network. These networks that connect LANs in geographically separated locations are Wide Area Networks (WANs). Although the organization maintains all of the policies and administration of the LANs at both ends of the connection, the policies within the communications service provider network are controlled by the TSP. WANs use specifically designed network devices to make the interconnections between LANs.
- Internetwork - Al mesh of interconnected networks is used. Some of these interconnected networks are owned by large public and private organizations, such as government agencies

2. Compare and contrast the following terms: network, LAN, WAN, internetwork, and the Internet.

Answer

- Internetwork - Al mesh of interconnected networks is used. Some of these interconnected networks are owned by large public and private organizations, such as government agencies or industrial enterprises, and are reserved for their exclusive use. The most well-known and widely used publicly accessible internetwork is the Internet.
- Internet - The most well-known and widely used publicly accessible internetwork. The Internet is created by the interconnection of networks belonging to Internet Service Providers (ISPs). These ISP networks connect to each other to provide access for users all over the world. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and protocols as well as the cooperation of many network administration agencies.

3. Compare and contrast the layers of the OSI model with the TCP/IP protocol stack.

Answer

There are two basic types of networking models: protocol models and reference models.

A protocol model closely matches the structure of a particular protocol suite. The hierarchical set of related protocols in a suite t represents all the functionality required to interface the human network with the data network. The 4-layer TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

A reference model provides a common reference for maintaining consistency within all types of network protocols and services. 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

Next Question

3. Compare and contrast the layers of the OSI model with the TCP/IP protocol stack.

Answer

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 process involved. The 7-layer Open Systems Interconnection (OSI) model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

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 discreet functions that need to occur at these layers.

3. Compare and contrast the layers of the OSI model with the TCP/IP protocol stack.

Answer

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. The OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

The key parallels between the two network models occur at the OSI model Layers 3 and 4. OSI Model Layer 3, the Network layer, almost universally is used to discuss and document the range of processes that occur in all data networks to address and route messages through an internetwork. The Internet Protocol (IP) is the TCP/IP suite protocol that includes the functionality described at Layer 3.

3. Compare and contrast the layers of the OSI model with the TCP/IP protocol stack.

Answer

Layer 4, the Transport layer of the OSI model, is often used to describe general services or functions that manage individual conversations between source and destination hosts. These functions include acknowledgement, error recovery, and sequencing. At this layer, the TCP/IP protocols Transmission Control Protocol (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 need to access networks for communications.

4. Explain why networking models are used.

Answer

Although 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.

As a reference model, 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. Whereas TCP/IP model layers are referred to by name, the seven OSI model layers are usually referred to by number.

Next Question

4. Explain why networking models are used.

Answer

below it. Whereas TCP/IP model layers are referred to by name, the seven OSI model layers are usually referred to by number.

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

- 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

5. Elaborate on the following terms: protocol, PDUs, and encapsulation.

Answer

Protocol:
All communication, whether face-to-face or over a network, is governed by predetermined rules called protocols. These protocols are specific to the characteristics of the conversation. 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 a sending a letter.

Successful communication between hosts on a network requires the interaction of many different protocols. A group of interrelated protocols that are necessary to perform a communication function is called a protocol suite. These protocols are implemented in software and hardware that is on

Next Question

5. Elaborate on the following terms: protocol, PDUs, and encapsulation.

Answer

each host and network device.

PDU & 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

5. Elaborate on the following terms: protocol, PDUs, and encapsulation.

Answer

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 appearance. PDUs within the protocols of the TCP/IP suite are:

- Data – The general term for the PDU used at the Application layer
- Segment – Transport Layer PDU
- Packet – Internetwork Layer PDU
- Frame – Network Access Layer PDU

6. Explain the postal metaphor for encapsulation.

Answer

Individual pages of a letter are written and numbered sequentially. Each page is sealed in a separate envelope that is then addressed to the recipient. The letters are posted and put in a mailbag (labelled with the destination) with many other envelops each containing a page of different letters and addressed to recipients. Many mailbags are loaded into a van and transported towards the destination. Along the way the mailbags may be transferred to other vans or different modes of transport – trucks, trains, aircraft, ships. At the destination the mailbags are unloaded and emptied. The envelopes are delivered to the destination addresses. At one address all the envelopes received are opened, the page removed from each one, and the pages re-assembled into the letter.

The envelope, and then the mailbag and the vans/trucks/aircraft, each do not care what is in the

Next Question

6. Explain the postal metaphor for encapsulation.

Answer

The envelopes are delivered to the destination addresses. At one address all the envelopes received are opened, the page removed from each one, and the pages re-assembled into the letter.

The envelope, and then the mailbag and the vans/trucks/aircraft, each do not care what is in the "container" that they carry. The letter itself is not used to provide information to assist in its delivery. The address on the envelope, the label on the mailbag or the delivery instructions to the van driver are what direct the letter towards its destination.

Data encapsulation follows the same principle – it is the addresses used in each layer of encapsulation that direct the data towards its destination not the data itself.

7. What are the unique roles of Layer 2, Layer 3, and Layer 4 addresses?

Answer

- Layer 4 addresses (ports) identify the individual applications sending or receiving data.
- Layer 3 (logical) addresses identify devices and their networks.
- Layer 2 (physical) addresses identify devices on a local network.

This concludes this chapter's Problems and Discussion questions.

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.7 Chapter Summary
2.7.1 Summary and Review

Page 3:
In this activity, you will start building, testing, and analyzing a model of the Exploration lab network.

Packet Tracer Skills Integration Instructions (PDF)

Click the Packet Tracer icon to launch the Packet Tracer activity.

File: 2.7.1 - lab - Skills Integration Challenge-Examining Packets.pdf

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.7 Chapter Summary
2.7.1 Summary and Review

Page 4:
To Learn More
Reflection Questions

How are the classifications LAN, WAN, and Internet still useful, and how might they actually be problematic in classifying networks?

What are strengths and weaknesses of the OSI and TCP/IP models? Why are both models still used?

Metaphors and analogies can be powerful aids to learning but must be used with care. Consider issues of devices, protocols, and addressing in the following systems:

- Standard postal service
- Express parcel delivery service
- Traditional (analog) telephone system
- Internet telephony
- Containerized shipping services
- Terrestrial and satellite radio systems
- Broadcast and cable television

Discuss what you see as common factors among these systems. Apply any similarities to other networks.

How could you apply these common concepts to developing new communications systems and networks?

CCNA Exploration - Network Fundamentals
2 Communicating over the Network
2.8 Chapter Quiz
2.8.1 Chapter Quiz

Page 1:

CCNA Exploration - Network Fundamentals
MODULE 2 (vesion 4.0)

1. Which statements correctly identify the role of intermediary devices in the network? (Choose three.)
determine pathways for data.
initiate data communications.
retime and retransmit data signals.
originate the flow of data.
manage data flows.
final termination point for data flow.

2. Select the statements that are correct concerning network protocols. (Choose three.)
define the structure of layer specific PDU's.
dictate how to accomplish layer functions.
outline the functions necessary for communications between layers.
limit hardware compatibility.
require layer dependent encapsulations.
eliminate standardization among vendors.

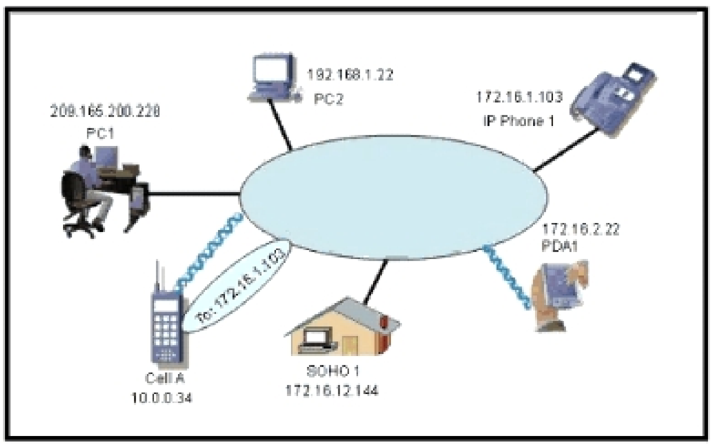
3 What are the key functions of encapsulation? (Choose three.)
tracks delay between end devices.
enables consistent network paths for communication.
allows modification of the original data before transmission.
identifies pieces of data as part of the same communication.
ensures that data pieces can be directed to the correct receiving end device.

4. Which two layers of the OSI model have the same functions as the TCP/IP model Network Access Layer? (Choose two.)
Network.
Transport.
Physical.
Data Link.
Session.

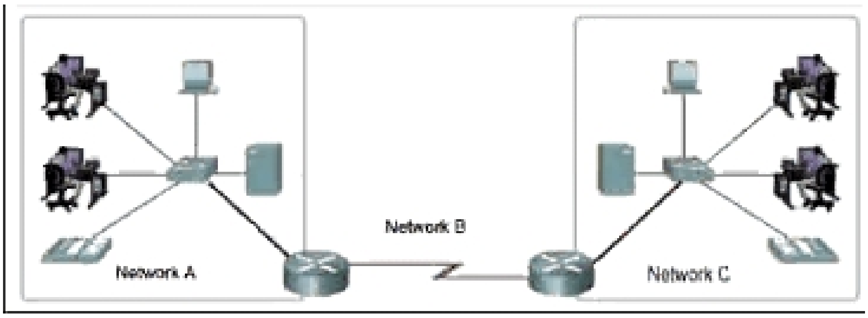
5. What is a PDU?
corruption of a frame during transmission.
data reassembled at the destination.
retransmitted packets due to lost communication.
a layer specific encapsulation.

6. Which characteristic correctly refers to end devices in a network?
manage data flows.
originate data flow.
retime and retransmit data signals.
determine pathways for data.

7. Refer to the exhibit. "Cell A" at IP address 10.0.0.34 has established an IP session with "IP Phone 1" at IP address 172.16.1.103. Based upon the graphic, which device type best describes the function of wireless device "Cell A?"
the destination device
an end device
an intermediate device
a media device

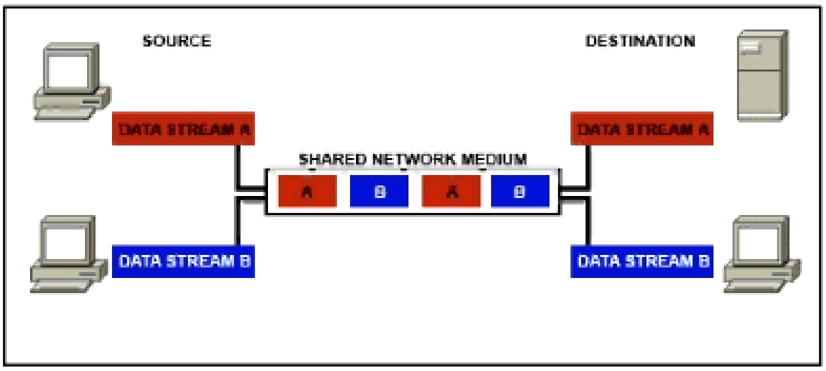


8. Refer to the exhibit. Which three labels correctly identify the network types for the network segments that are shown? (Choose three.)
Network A -- WAN
Network B -- WAN
Network C -- LAN
Network B -- MAN
Network C -- WAN
Network A – LAN



9. Which three statements best describe a Local Area Network (LAN)? (Choose three.)
A LAN is usually in a single geographical area.
The network is administered by a single organization.
The connection between segments in the LAN is usually through a leased connection.
The security and access control of the network are controlled by a service provider.
A LAN provides network services and access to applications for users within a common organization.
Each end of the network is generally connected to a Telecommunication Service Provider (TSP).

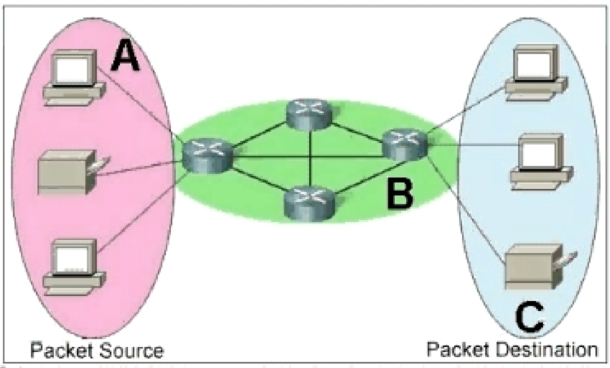
10. Refer to the exhibit. Which networking term describes the data interleaving process represented in the graphic?
piping
PDU
streaming
multiplexing
encapsulation



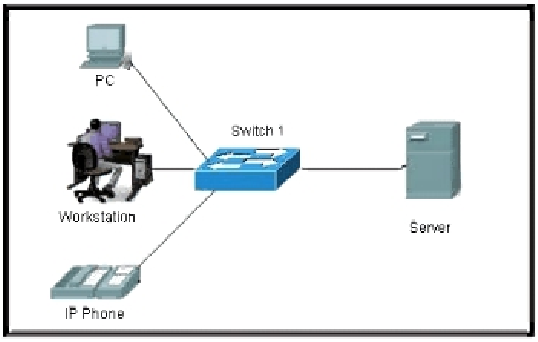
11. What is the primary purpose of Layer 4 port assignment?
to identify devices on the local media
to identify the hops between source and destination
to identify to the intermediary devices the best path through the network
to identify the source and destination end devices that are communicating
to identify the processes or services that are communicating within the end devices

12. What device is considered an intermediary device?
file server
IP phone
laptop
printer
switch

13. Refer to the exhibit. Which term correctly identifies the device type that is included in the area B?
source
end
transfer
intermediary



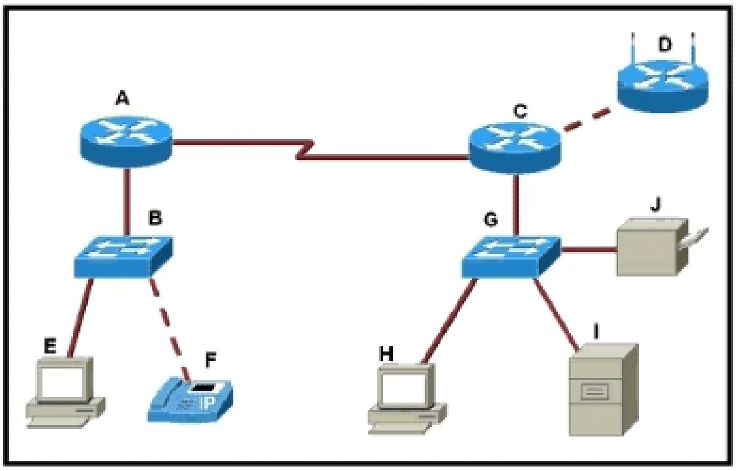
14. Refer to the exhibit. What type of network is shown?
WAN
MAN
LAN
WLAN



15. Which layer encapsulates the segment into packets?
physical
data link
network
transport

16. What can be identified by examining the network layer header?
the destination device on the local media
the destination host address
the bits that will be transferred over the media
the source application or process creating the data

17. Refer to the exhibit. Which set of devices contains only end devices?
A, C, D
B, E, G, H
C, D, G, H, I, J
D, E, F, H, I, J
E, F, H, I, J



18. During the encapsulation process, what occurs at the data link layer?
No address is added.
The logical address is added.
The physical address is added.
The process port number is added.

19. What is the purpose of the TCP/IP Network Access layer?
path determination and packet switching
data presentation
reliability, flow control, and error detection
network meia control
the division of segments into packets

20. What is the proper order of the layers of the OSI model from the highest layer to the lowest layer?
physical, network, application, data link, presentation, session, transport
application, physical, session, transport, network, data link, presentation
application, presentation, physical, session, data link, transport, network
application, presentation, session, transport, network, data link, physical
presentation, data link, session, transport, network, physical, application

21. What is a primary function of the trailer information added by the data link layer encapsulation?
supports error detection
ensures ordered arrival of data
provides delivery to correct destination
identifies the devices on the local network
assists intermediary devices with processing and path selection