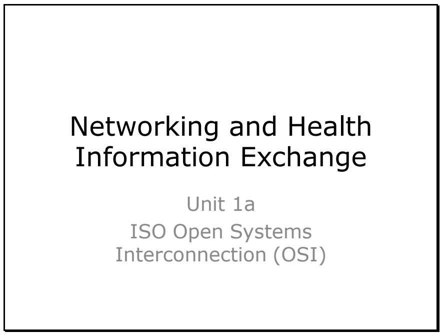
Slide 1



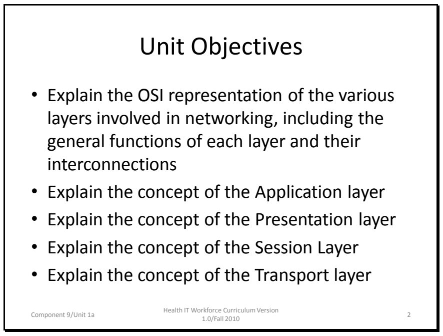
Networking and Health Information Exchange

Unit 1a

ISO Open Systems Interconnection (OSI)

Networking and Health
Information Exchange
Unit 1a
ISO Open Systems
Interconnection (OSI)

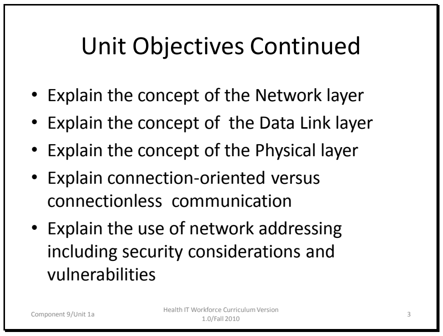
Slide 2



Unit Objectives

- Explain the OSI representation of the various layers involved in networking, including the general functions of each layer and their interconnections
- Explain the concept of the Application layer
- Explain the concept of the Presentation layer
- Explain the concept of the Session Layer
- Explain the concept of the Transport layer

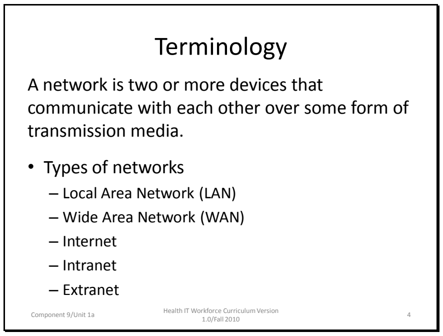
Slide 3



Unit Objectives Continued

- Explain the concept of the Network layer
- Explain the concept of the Data Link layer
- Explain the concept of the Physical layer
- Explain connection-oriented versus connectionless communication
- Explain the use of network addressing including security considerations and vulnerabilities

Slide 4



Terminology

A network is two or more devices that communicate with each other over some form of transmission media.

- Types of networks
  - Local Area Network (LAN)
  - Wide Area Network (WAN)
  - Internet
  - Intranet
  - Extranet

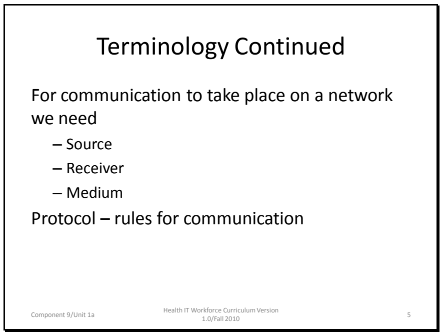
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

4

A network is two or more devices that communicate with each other over some form of transmission media. There are several different types of networks that are defined by size, who maintains the network and who has access to the network. A local area network (LAN) is a small network. It can be as small as two devices connected to each other and as big as a college campus. LANs are maintained by the organization that uses the network and it is responsible for creating and maintaining all the network hardware and software. Wide area networks (WANs) are big network. The largest and oldest WAN in existence is the Internet. WANs span large geographic areas and are typically made up of many different LANs. For example your schools' LAN is part of the Internet, your LAN at home is too. Parts of the Internet are owned by different people. Intranets make use of Internet technology but on the Internet where the web pages are available to who ever navigates to them, Intranet sites are limited to who can view the pages the make up the site. For example companies have Intranet sites that contain their human resource manuals, leave forms, employee news, etc. This information is not needed by the general public, only by employees of that company. An extranet is a combination of an Internet and intranet site. Extranets are set up so the access is limited to a company's outside resources. For example an extranet could be set up so that a retailer could use a company's extranet to see if a certain part is available and if it is, they can order it and then track the order online.

Slide 5



Terminology Continued

For communication to take place on a network we need

- – Source
- – Receiver
- – Medium

Protocol – rules for communication

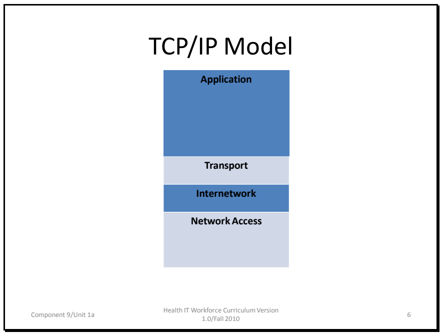
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

5

For communication to take place on a network we need a source, receiver and a medium to transmit data between the source and receiver. The source and receiver can be a desktop computer, laptop, printer, router, switch, cellphone, ATM machine, almost anything you can image! The medium or media is the wired or wireless method that is used to connect the source and receiver to each other and that carries the data from the endpoints. It is not enough for the devices to be connected to each other but they must also speak the same language. In networking we refer to this as the protocol. The protocol defines the processes and rules that devices will follow to communicate with each other. For example we follow protocols all the time. In Asian cultures the protocol may be to bow when we greet each other and in Europe it may be to kiss each other on the check where in America we shake hands. The protocols may be different but in the end we are accomplishing the same thing – greeting each other. Examples of network protocols are TCIP/IP, HTTP, NETBEUI and ICMP.

Slide 6



TCP/IP Model

Application

Transport

Internetwork

Network Access

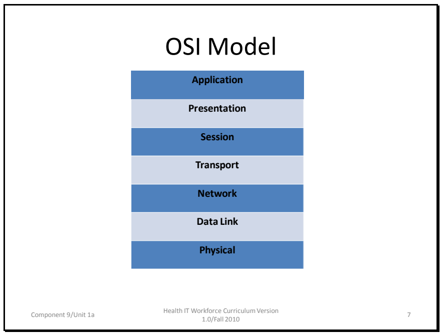
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

6

In the mid-60s the United States wanted to have a computer network connecting their military sites to each other that could withstand an attack. This means that redundant paths were needed between the sites. A protocol was created that enabled the the transmission of data to switch to another path in case one path was destroyed. This protocol was called TCP/IP – Transmission Control Protocol/Internet Protocol. The TCP/IP model, also called the Department of Defense or DoD model, was created in the 1970s as a 4 layer model that described the functions that should take place at each layer as two devices communicated with each other. The TCP/IP layers were the Application layer which is closest to the user, the Transport layer, Internetwork layer and Network Access layer.

Slide 7



OSI Model

Application

Presentation

Session

Transport

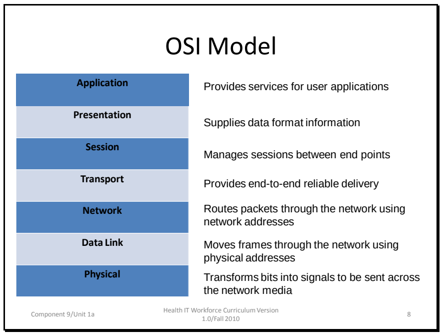
Network

Data Link

Physical

In the late 1970s the Open Systems Interconnection (OSI) model created by International Organization for Standardization. It is a 7 layer model that describes the processes should take place for communication to occur between 2 devices on a network.   The Application layer is closest to the user and the physical layer is closest to the network media (or medium). The media is the wired or wireless method that is used to connect network devices to each other. There is a mnemonic that can be used to remember the layers. Starting at the physical layer, Please Do Not Throw Sausage Pizza Away. By taking the first letter of every word in the mnemonic you will have the first letter of the 7 layers of the OSI model.

Slide 8

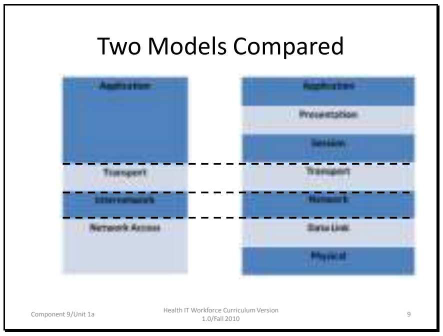


OSI Model

Application	Provides services for user applications
Presentation	Supplies data format information
Session	Manages sessions between end points
Transport	Provides end-to-end reliable delivery
Network	Routes packets through the network using network addresses
Data Link	Moves frames through the network using physical addresses
Physical	Transforms bits into signals to be sent across the network media

The application layer is the OSI layer closest to the end user. The user interacts with the application which uses services provided at the application layer. For example a user uses Internet Explorer (IE) to surf the web. HTTP (hypertext transfer protocol) is the protocol that works at the Application layer that allows IE to work. The presentation layer prepares data to be passed to the next layer. It is at this layer that data encryption and compression takes places. The session layer manages sessions between end points. An example is the network client that exists on a computer system that allows you to login to the network. The session layers establishes, maintains and ends the connection between the end points. The transport layers makes sure that data is received correctly at the destination. If it isn't the transport layers make sure that the data is resent. The network layers uses network addresses (and example is IP addresses) to move packets across a network from source to destination. The data link layer uses physical (or MAC addresses) to move data across the network. The physical layers transforms bits into signals (either electrical or optical) that are then sent across the network media (wired or wireless).

Slide 9



Two Models Compared

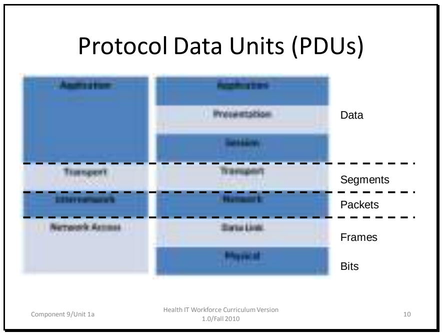
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

9

The Application layer of the TCP/IP model is equal to the Application, Presentation and Session layers of the OSI model. The Transport layer in both models are equal to each other. The Internetwork layer of the TCP/IP model is equivalent to the Network layer of the OSI model. The Network Access layer of the TCP/IP model is the same as the Data Link and Physical layers of the OSI model.

Slide 10



Protocol Data Units (PDUs)

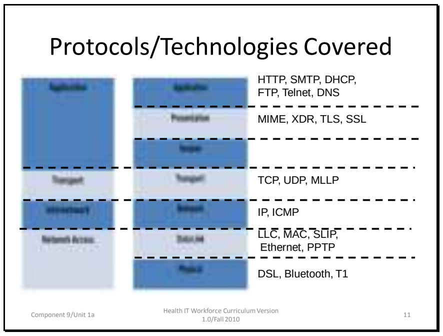
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

10

As data travels through the layers it is referred to with different names. This is known as the protocol data units (PDUs). As data travels through the Application, Presentation and Session layers it is called data. At the transport layer it is called segments, at the network layer packets. As it passes through the data link layer it is call frames and finally when it reaches the physical layer it is called bits.

Slide 11



Protocols/Technologies Covered

HTTP, SMTP, DHCP, FTP, Telnet, DNS

MIME, XDR, TLS, SSL

TCP, UDP, MLLP

IP, ICMP

LLC, MAC, SLIP, Ethernet, PPTP

DSL, Bluetooth, T1

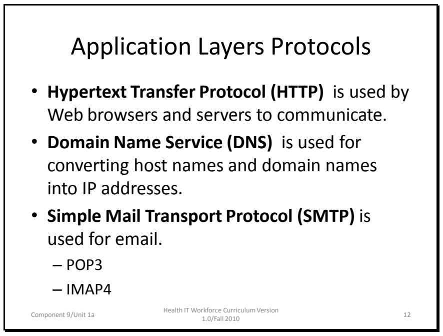
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

11

Transmission Control Protocol/Internet Protocol (TCP/IP) is actually a protocol suite. This means that it consists of multiple protocols. The 2 core protocols are TCP and IP but there are many other protocols like HTTP, DHCP and ICMP. TCP/IP is the protocol that is used by the majority of networks today. It is important to understand what these protocols do. The protocols and technologies we will cover in this unit are shown on the diagram at the layer in which they function.

Slide 12



Application Layers Protocols

- **Hypertext Transfer Protocol (HTTP)** is used by Web browsers and servers to communicate.
- **Domain Name Service (DNS)** is used for converting host names and domain names into IP addresses.
- **Simple Mail Transport Protocol (SMTP)** is used for email.
  - POP3
  - IMAP4

Component 9/Unit 1a

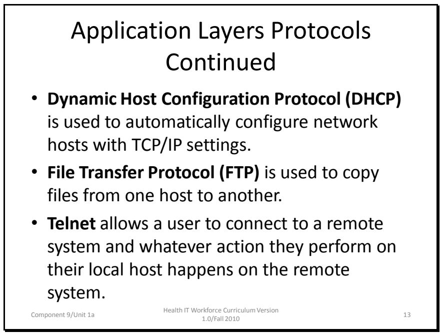
Health IT Workforce Curriculum Version 1.0/Fall 2010

12

Application layer protocols provides services for user applications. **Hypertext Transfer Protocol (HTTP)** is the standard used for Web browsers and servers to communicate. HTTP clients (Web browsers) and servers communicate using HTTP request and response messages. GET, POST, and HEAD are the three main HTTP message types. **Domain Name Service (DNS)** is a system for converting host names and domain names into IP addresses. For example if you type www.cisco.com into a web browser DNS is used to resolve the domain name (cisco.com) into an IP address. That IP address is what is used to connect to the server that hosts the web pages for cisco.com. When you are using voice activation on your cell phone and you ask it to call your mom the phone has to translate your mom into a phone number and it dials that phone number. **Simple Mail Transport Protocol (SMTP)** is used for email, specially the sending of email. SMTP is used to transport email from one email server to another. Post Office Protocol (POP, current version 3 so referred to as POP3) and Internet

Message Access Protocol (IMAP, curent version 4 so referred to as IMAP4) are the popular protocols that are used to deliver email. If you were sending an email using GMAIL to a friend that was using YAHOO, SMTP would be the protocol that would transfer the email between the GMAIL and YAHOO servers and IMAP4 would be the protocol that would deliver the email to their mailbox.

Slide 13



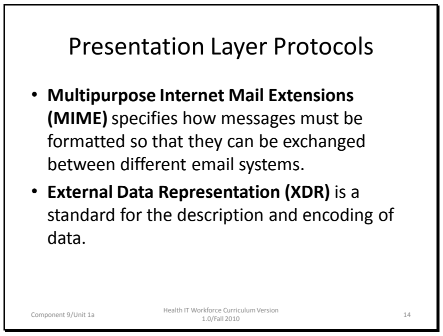
Application Layers Protocols Continued

- **Dynamic Host Configuration Protocol (DHCP)** is used to automatically configure network hosts with TCP/IP settings.
- **File Transfer Protocol (FTP)** is used to copy files from one host to another.
- **Telnet** allows a user to connect to a remote system and whatever action they perform on their local host happens on the remote system.

Dynamic Host Configuration Protocol (DHCP) is used to automatically configure network client with TCP/IP settings. The settings a device must have to get on the network are IP address, subnet mask and default gateway. Other settings are optional. When a client gets on the network it sends out a broadcast message requesting IP settings, a DHCP server will respond offering the client an IP address and other TCP/IP settings. To finalize the process the client will respond to the DHCP with a request to use those settings that were offered by the server. The server will make an entry into it's database that those settings have been leased to that client. The lease will last for an a defined period of time. When that time period has ended or the client manually breaks the lease the TCP/IP settings are put back into the pool and can be offered to another client requesting TCP/IP settings. DHCP saves times by not requiring a network administrator to go to every client and type in all TCP/IP settings. It also eliminates the possibility of more than one client getting the same IP address since it will only lease it to one client. It is very easy for an administrator to make a mistake and assign the same IP address to multiple clients. DHCP can cause a security risk because any device connected to the network could receive a IP address on that network and be able to communicate. Physical security is important on networks that use DHCP.

File Transfer Protocol (FTP) is used to copy files from one host to another. Some systems require users to login to the host that they wish to upload or download a file to. Systems that don’t require usernames and/or passwords are called anonymous FTP sites. If you have ever download an application, music or movie from the Internet then you have used FTP. **Telnet** allows a user to connect to a remote system and whatever action they perform on their local host happens on the remote system. For example you may remember the old computerized library catalogs   - the tan monitors with green or orange text. If you were searching for a book you entered the name of the book, the search was done on the server and then displayed on the terminal where you entered the name of the book. Both FTP and Telnet are unsecure by default. The data that is being transmitted between the two systems are in plain-text which means that anything or anyone that intercepts the data being transferred can read the data. If you want the data to be secure you should run FTP and Telnet using a secure shell like SSH. This would encrypt the data being transferred.

Slide 14

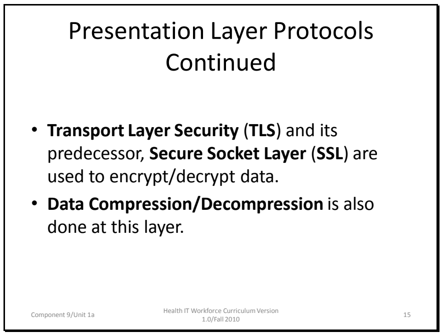


Presentation Layer Protocols

- **Multipurpose Internet Mail Extensions (MIME)** specifies how messages must be formatted so that they can be exchanged between different email systems.
- **External Data Representation (XDR)** is a standard for the description and encoding of data.

Presentation layer protocols supply data format information. **Multipurpose Internet Mail Extensions (MIME)** specifies how messages must be formatted so that they can be exchanged between different email systems. It defines mechanisms for sending other kinds of information beside just text in e-mail. These include text in languages other than English , graphics, audio, movies and application files. **External Data Representation (XDR)** is a standard for the description and encoding of data.

Slide 15



Presentation Layer Protocols Continued

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Socket Layer** (**SSL**) are used to encrypt/decrypt data.
- **Data Compression/Decompression** is also done at this layer.

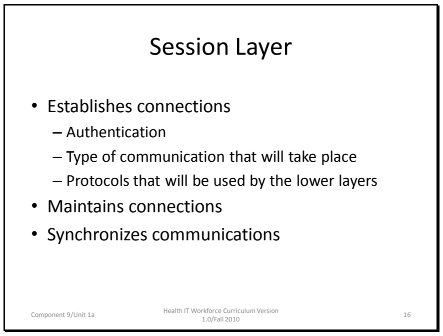
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

15

Transport Layer Security (**TLS**) and its predecessor, **Secure Socket Layer** (**SSL**) are used to encrypt/decrypt data. SSL was developed by Netscape for their web browser and was improved upon creating TLS. Today we use TLS but people still refer to it as SSL. Encryption means that the data or plaintext is encryption using an algorithm and key to create ciphertext. Ciphertext can not be read by anyone that intercepts the transmission. They would need to have the algorithm and key to decrypt the message so they could read it. When surfing the Internet, you can tell when you are using TLS when you see the "http" in the address line replaced with "https," and when you see a small padlock in the status bar at the bottom of the browser window, usually on the left-hand side. **Data Compression** is also done at this layer. This means that a device is able to transmit or store the same amount of data in fewer bits. In networking this enables the data to be sent quicker. Decompression is done by the receiving device. The same algorithm and percentage must be used to decompress the data as was used to compress the data.

Slide 16



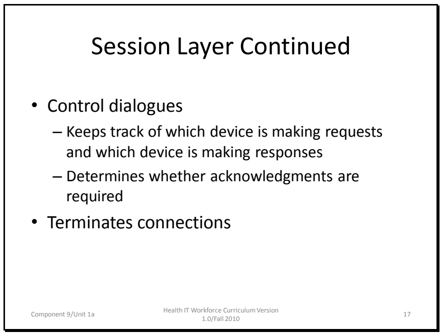
Session Layer

- Establishes connections
  - Authentication
  - Type of communication that will take place
  - Protocols that will be used by the lower layers
- Maintains connections
- Synchronizes communications

Component 9/Unit 1a Health IT Workforce Curriculum Version 1.0/Fall 2010 16

The session layer manages sessions between end points.   It is responsible for establishing connections between 2 devices. This may involve authentication. Authentication is the process in which a user/device provides some information and the information is checked against a database to ensure that the user/device should have access to that particular resource. Typically in a network this is the process of logging into a resource by providing your username and password. As part of the session establishment the type of communication and protocols that will be used by the lower layers are also determined. The session layer maintains the connections and synchronizes communications.

Slide 17



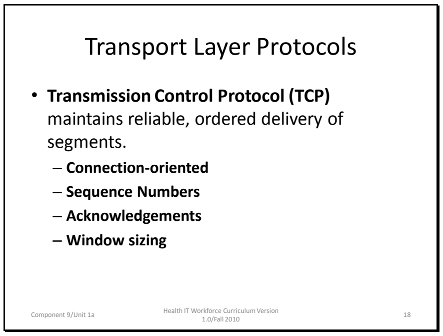
Session Layer Continued

- Control dialogues
  - Keeps track of which device is making requests and which device is making responses
  - Determines whether acknowledgments are required
- Terminates connections

Component 9/Unit 1a Health IT Workforce Curriculum Version 1.0/Fall 2010 17

The layer is also responsible for keeping track of which device is requesting services and which device is providing that service. It also determines if acknowledgements are required for data transmissions. Finally the session layer terminates the connection between two devices once the data transfer is complete.

Slide 18



Transport Layer Protocols

- **Transmission Control Protocol (TCP)** maintains reliable, ordered delivery of segments.
  - **Connection-oriented**
  - **Sequence Numbers**
  - **Acknowledgements**
  - **Window sizing**

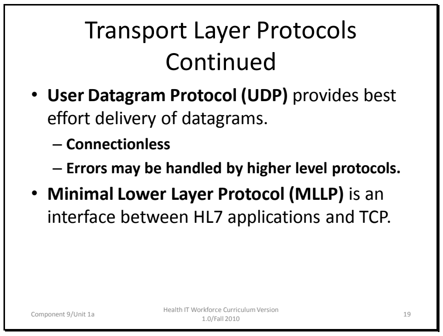
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

18

The Transport layer provides end-to-end reliable delivery of segments. **Transmission Control Protocol (TCP)** maintains reliable, ordered delivery of segments between the receiver and destination device. TCP makes a connection between the sending and receiving device before it actually transmits segments. Think about it like this. If I want to make sure you hear me telling you something. I will say your name, make sure you acknowledge me and then tell you what I want to tell you. I have created a connection with you. I will also have you acknowledge that you understood what I told you. TCP uses sequence numbers, acknowledgements and window sizing. When data is passed to the transport layer from the session layer the transport layer divides the data into chunks called segments. Each segment is given a sequence number. When the segments are send to the destination device they may take different paths and arrive in a different order than the order in which they were sent. The sequence numbers are used by receiving device's transport layer to reassemble the segments back into the correct order before they are passed back up to the session layer. Some of the segments may be lost in transmission. This is why the receiving device sends acknowledgements for the segments it receives back to the sender. If the sender doesn't receive an acknowledgment for a segment it will resend the segment. Sometimes the receiver is overwhelmed by the number of segments it is receiving at a time and has to drop some of the segments. The sender will adjust how many segments it sends to the receiver at a time. This is the process of window sizing or changing how many segments are sent at a time.   TCP is like sending a certified letter via the US Postal Service. Sequence numbers, acknowledgments and window sizing takes time and resources. Sometimes we want to send data and while we hope it gets there we don’t want to guarantee it. This is when we use **User Datagram Protocol (UDP).**

Slide 19



Transport Layer Protocols Continued

- **User Datagram Protocol (UDP)** provides best effort delivery of datagrams.
  - **Connectionless**
  - **Errors may be handled by higher level protocols.**
- **Minimal Lower Layer Protocol (MLLP)** is an interface between HL7 applications and TCP.

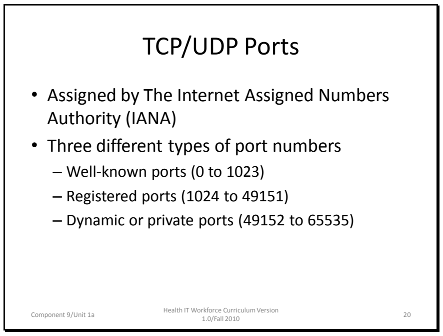
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

19

User Datagram Protocol (UDP) provides best effort delivery of datagrams. It does not create a connection between the sending and receiving devices before it sends datagrams. Errors may be handled by higher level protocols. If you are in a classroom the teacher is teaching you information and hopes that you receive that information. They can not take the time to make sure that every student understands everything they are teaching or take the time to re-teach everything that a student doesn’t understand. UDP is like sending a letter by regular postal service. We hope it gets there but we can’t be guaranteed delivery like we could with a certified letter (TCP). UDP is used for applications like streaming media, many online games and Voice over IP (VoIP). **Minimal Lower Layer Protocol (MLLP)** is an interface between HL7 Applications and TCP that uses minimal overhead.

Slide 20



TCP/UDP Ports

- Assigned by The Internet Assigned Numbers Authority (IANA)
- Three different types of port numbers
  - Well-known ports (0 to 1023)
  - Registered ports (1024 to 49151)
  - Dynamic or private ports (49152 to 65535)

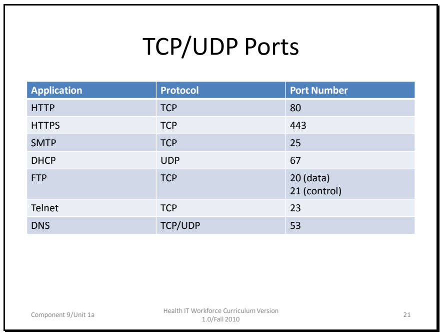
Component 9/Unit 1a

Health IT Workforce Curriculum Version 1.0/Fall 2010

20

Applications and application layer services are identified by port numbers on a specific device. Some use TCP and other use UDP. Some can use either based on the implementation. The Internet Assigned Numbers Authority (IANA) assign the port numbers. There are 3 different types of port numbers, Well-known ports (0 to 1023), Registered ports (1024 to 49151) and Dynamic or private ports (49152 to 65535).

Slide 21



TCP/UDP Ports

Application	Protocol	Port Number
HTTP	TCP	80
HTTPS	TCP	443
SMTP	TCP	25
DHCP	UDP	67
FTP	TCP	20 (data) 21 (control)
Telnet	TCP	23
DNS	TCP/UDP	53

The table shows some common applications, the protocol they use and their associated port number.