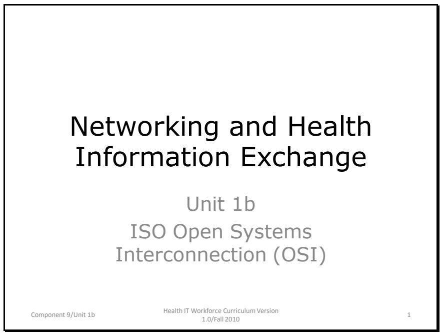
Slide 1



Networking and Health Information Exchange

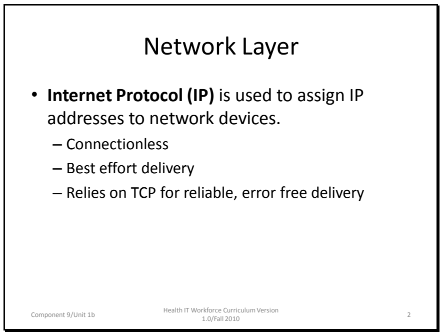
Unit 1b

ISO Open Systems Interconnection (OSI)

Component 9/Unit 1b — Health IT Workforce Curriculum Version 1.0/Fall 2010 — 1

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

Slide 2



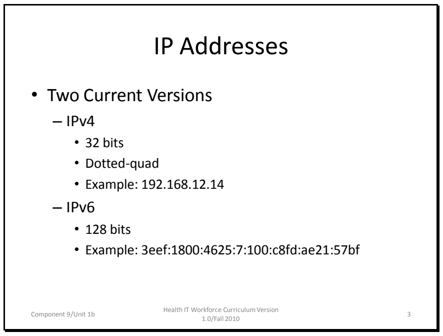
Network Layer

- **Internet Protocol (IP)** is used to assign IP addresses to network devices.
  - Connectionless
  - Best effort delivery
  - Relies on TCP for reliable, error free delivery

Component 9/Unit 1b — Health IT Workforce Curriculum Version 1.0/Fall 2010 — 2

The network layer routes packets through the network using network addresses. **Internet Protocol (IP)** is used to assign IP addresses to network devices. These addresses are used to identify the network devices so that packets can be delivered to the correct device. IP is a connectionless, best effort delivery protocol. It relies on TCP for reliable, error free delivery.

Slide 3



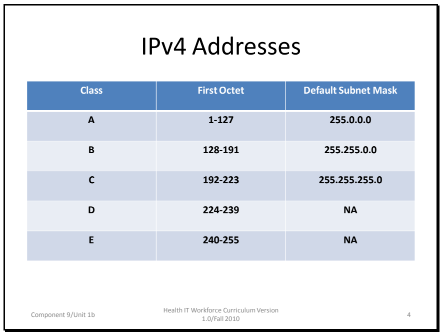
IP Addresses

- Two Current Versions
  - IPv4
    - 32 bits
    - Dotted-quad
    - Example: 192.168.12.14
  - IPv6
    - 128 bits
    - Example: 3eef:1800:4625:7:100:c8fd:ae21:57bf

Component 9/Unit 1b — Health IT Workforce Curriculum Version 1.0/Fall 2010 — 3

There are two current versions of IP addresses, version 4 and version 6. IPv4 is the most popular version in use but IPv6 is starting to be implemented. IPv4 addresses use 32 bits and IPv6 uses 128 bits. Version 4 addresses are referred to as a dotted-quad address because the 32 bits are broken down into 4 – 8 bit groups called octets separated by a dot. An example would be 192.168.12.14. An example of a IPv6 address would be 3eef:1800:4625:7:100:c8fd:ae21:57bf. Remember that computers use binary numbers, just 0s and 1s. The IPv4 examples shown in the rest of the presentation are in decimal format because they are easier for us to deal with.

Slide 4



IPv4 Addresses

Class	First Octet	Default Subnet Mask
A	1-127	255.0.0.0
B	128-191	255.255.0.0
C	192-223	255.255.255.0
D	224-239	NA
E	240-255	NA

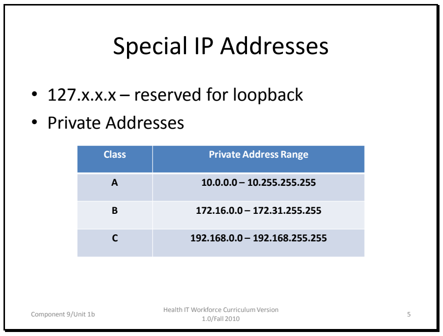
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

4

The first octet determines what class of address an IPv4 address is. If the 1st octet falls between 0-127, it is a class A address. If it falls between 128-191 it is a class B address, 192-223, class C, 224-239, class D and 240-255, class E. Class A, B and C are assigned to networks. Class D addresses are used for multicasting and class E is for experimental purposes. We don't know what's going on on those addresses!

Slide 5



Special IP Addresses

- 127.x.x.x – reserved for loopback
- Private Addresses

Class	Private Address Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

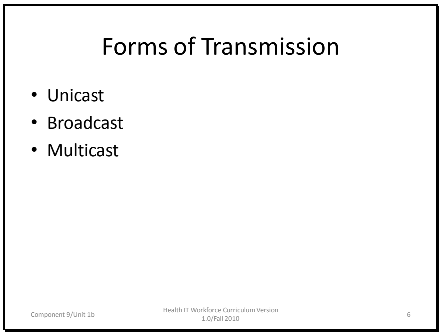
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

5

Address that have 127 in the 1st octet are reserved for testing and can not be assigned to devices. In particular 127.0.0.1 is reserved for loopback test. This allows a user to test the TCP/IP settings on a device. Private addresses are addresses that can be used in home, office, or LANs where the packets do not have to be sent out across the Internet. The Internet uses public addresses. If such a private network needs to connect to the Internet, it must use either network address translation (NAT) or a proxy server.

Slide 6



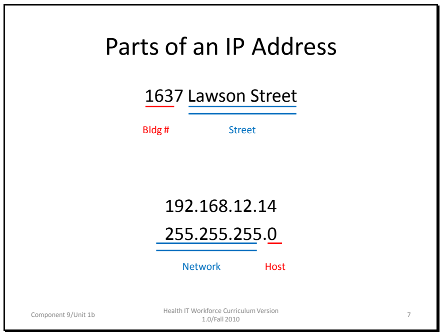
Forms of Transmission

- Unicast
- Broadcast
- Multicast

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 6

As mentioned Class D addresses are for multicast. We can classify transmission in one of three ways, unicast, broadcast or multicast. Unicast transmissions are from one source to one receiver. An example would be if you were having a one-on-one conversation with another person. Broadcast is one source sending out a transmission to all devices that are on the same network. For example a teacher in a classroom is broadcasting their lecture to all the students in the classroom. Multicast transmission is when one sender sends out a message to a group of devices and that group is identified by a class D address. For example is an announcement was made at your college that was addressed to all students in the Networking and Health Information Exchange class you would pay attention because you are part of the group. Devices are programmed to know what multicast addresses they should respond to.

Slide 7



Parts of an IP Address

1637 Lawson Street

Bldg # Street

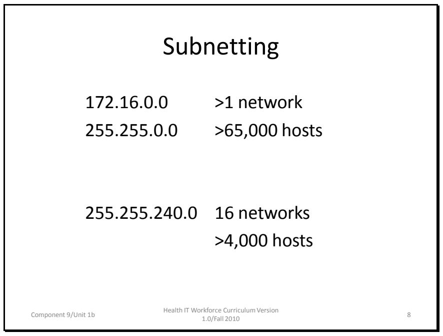
192.168.12.14
255.255.255.0

Network Host

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 7

An IP address has two parts. The first part identifies the network that the host with that IP addresses belongs to and the second part uniquely identifies that device on that network. For example if you were driving to 1637 Lawson Street you would know that the street is named Lawson and once you got to that street you would need to look for building 1637. We know the scheme for addresses because we have learned it. In networking the subnet mask is what tells us which part of the address is the network and which part is the host. Where ever there are 1s in the subnet mask that is the network portion of the address and where there are 0s that is the host portion. 255 in decimal is 8 1's or 11111111 in binary. In our example 192.168.12.14 is a class C address so the default subnet mask is 255.255.255.0. The 1st 3 octets identify the network and the last octet identifies the host.

Slide 8



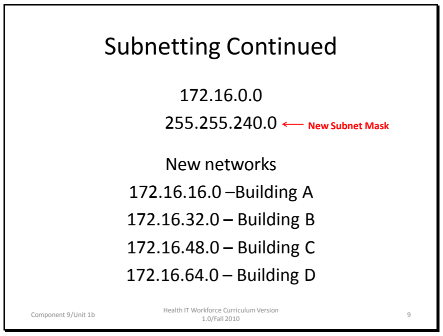
Subnetting

172.16.0.0	>1 network
255.255.0.0	>65,000 hosts
255.255.240.0	16 networks
	>4,000 hosts

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 8

172.16.0.0 is a class B address. The default subnet mask is 255.255.0.0. The first 2 octets identify the network and the last 2 octets identify the hosts on that network. There are 16 bits that can be used to identify hosts on the 172.16.0.0 network. This means we can have over 65,000 hosts on that 1 network. Not many networks need over 65 thousand hosts. We can take the 1 network and subdivide it, or subnet it, into more networks. We take some of the hosts bits (0s) and change them to network bits (1s). If we have a new subnet mask of 255.255.240 and we apply to that same address 172.16.0.0 we can create 16 networks with 4,000 hosts on each network.

Slide 9



Subnetting Continued

172.16.0.0

255.255.240.0 ← New Subnet Mask

New networks

172.16.16.0 –Building A

172.16.32.0 – Building B

172.16.48.0 – Building C

172.16.64.0 – Building D

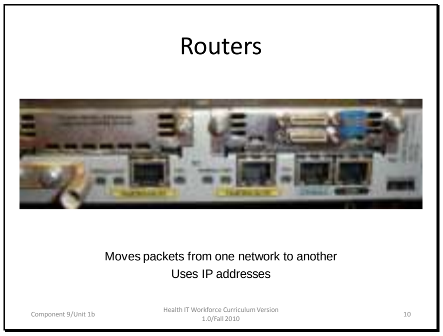
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

9

We can then take those subnets and use them for different buildings for example. If we get a virus on a computer with an IP address of 172.16.32.10 we immediately know it is on a pc in building B. We could also “cut off” that subnet from the rest of the network therefore isolating the virus to just that subnet instead of allowing it to spread to the entire network.

Slide 10



Routers

Moves packets from one network to another

Uses IP addresses

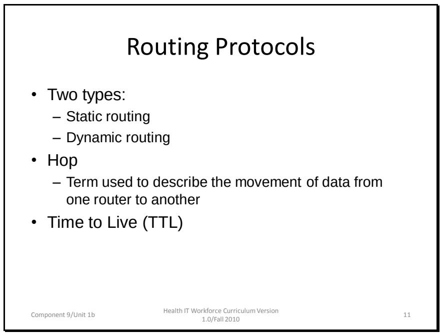
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

10

Routers operate at the Network layer of the OSI Model. Routers are multiport connectivity devices that connect different networks (LANs, WANs, different transmission speeds, media, and protocols) to each other. They move packets from one network to another (routes packets).

Slide 11



Routing Protocols

- Two types:
  - Static routing
  - Dynamic routing
- Hop
  - Term used to describe the movement of data from one router to another
- Time to Live (TTL)

Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

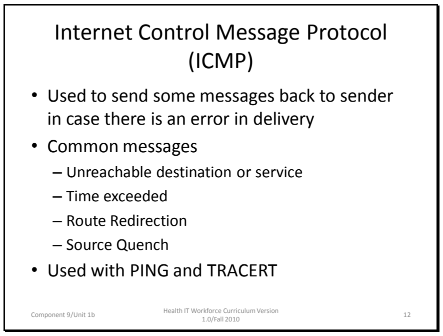
11

Routers choose the best route for a packet to take to arrive at its destination. There are two ways that the router knows what the best path is, static routing and dynamic routing. In static routing a network administrator programs a router to use a specified paths to move data between two nodes. In dynamic routing routers automatically calculate the best path between nodes and accumulates this information in a routing table. Routers share information about the routes with each other. A router will look at the destination IP address of a packet, calculate what network it is located on and based on the information in the routing table about that network, forward the packet to its next hop.

A hop is a term used to describe the movement of date from one router to another. For example if a packet travels across 3 routers from its source to its destination it is said to have taken 3 hops.

As a packet crosses across a router the Time to Live (TTL) field in the IP packet is decrease by 1. When the TTL reaches 0 that router will discard the packet and send a message to the sender to let it know that the packet was undeliverable.

Slide 12



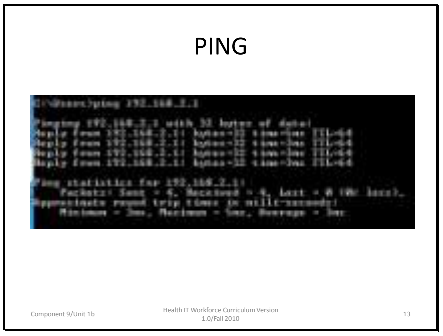
Internet Control Message Protocol (ICMP)

- Used to send some messages back to sender in case there is an error in delivery
- Common messages
  - – Unreachable destination or service
  - – Time exceeded
  - – Route Redirection
  - – Source Quench
- Used with PING and TRACERT

Component 9/Unit 1b   Health IT Workforce Curriculum Version 1.0/Fall 2010   12

Internet Control Message Protocol (ICMP) is another protocol that operates at the Network layer of the OSI model. Even though IP is an unrealiable protocol it does allow some messages to be sent back to the sender in case there is an error in delivery. Some common ICMP messages are Unreachable destination or service, Time exceeded, Route Redirection and Source Quench. ICMP is also used with the PING and TRACERT (or TRACEROUTE) utilities.

Slide 13



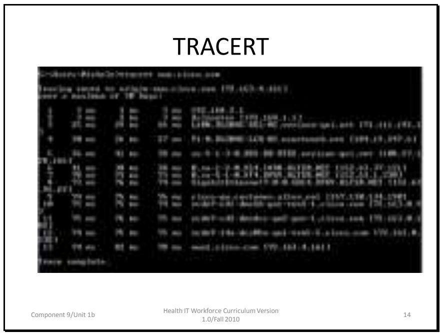
PING

```
C:\Users\[illegible]>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=5ms TTL=64
Reply from 192.168.2.1: bytes=32 time=3ms TTL=64
Reply from 192.168.2.1: bytes=32 time=3ms TTL=64
Reply from 192.168.2.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

Component 9/Unit 1b   Health IT Workforce Curriculum Version 1.0/Fall 2010   13

Ping is used to test if a particular host is reachable on a network and to measure the round trip time for packets sent from the local host to a destination computer. Ping uses ICMP Echo Request and Echo Reply packets. You can ping a device’s IP address or its host name.

Slide 14



TRACERT

[illegible]

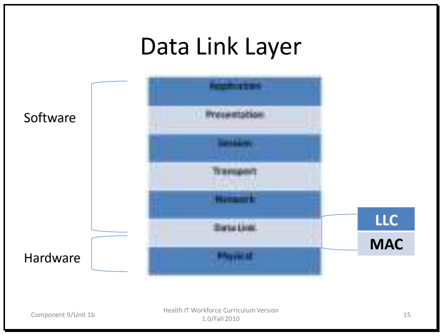
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

14

Tracert or Traceroute is a utility that is used to trace the route that a packet takes from source to destination. The destination can be referenced by its IP address or name. The output from the command shows the IP address and sometimes the host name of the routers that are traversed as the packet is sent from one device to the other.

Slide 15



Data Link Layer

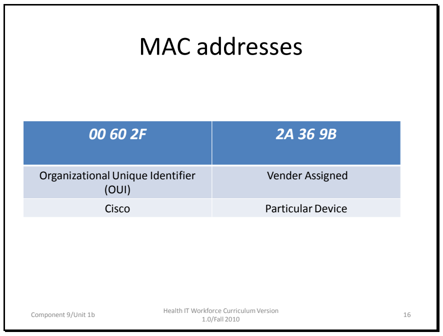
Component 9/Unit 1b

Health IT Workforce Curriculum Version 1.0/Fall 2010

15

The Data Link layer moves frames through the network using physical addresses. The Data Link layer is the layer that is the layer where the software and hardware come together. The layer contains two sublayers, the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC sublayer interacts with the Network layer and identifies what network layer protocol is being used. This information allows different network layer protocols to use the same network interface and media. The MAC sublayer interacts with the Physical layer. It provides data link layer addressing.

Slide 16

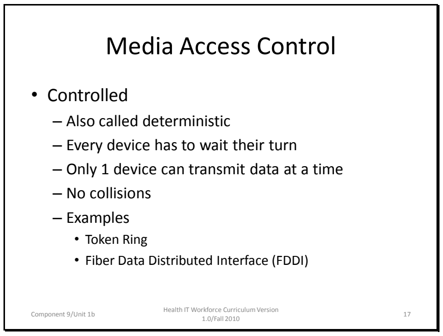


MAC addresses

00 60 2F	2A 36 9B
Organizational Unique Identifier (OUI)	Vender Assigned
Cisco	Particular Device

A MAC address is a unique address assigned to most network interface cards (NICs) by the manufacturer for identification. This is also known as the physical address. MAC address are in hexadecimal format. It contains 48 bits or 12 hex digits. The 1st 24 bits/6 hex digits is called the organizational unique identifier (OUI). Each vendor that produces NICs is assigned their OUIs by the Institute of Electrical and Electronics Engineers (IEEE). The remaining bits are unique for each OUI and is assigned by the vendor.

Slide 17

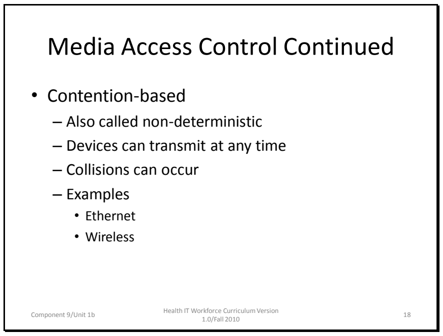


Media Access Control

- Controlled
  - Also called deterministic
  - Every device has to wait their turn
  - Only 1 device can transmit data at a time
  - No collisions
  - Examples
    - Token Ring
    - Fiber Data Distributed Interface (FDDI)

The MAC sublayer determines how data frames are placed onto the network media, in other words, which device gets to “talk”. There can be multiple devices sharing the same media and there has to be a system in place to decide which device gets to place their data on the network. The two MAC methods for allowing access to shared media are controlled and contention-based. Control access is also referred to as deterministic access There is some mechanism that determines when a device can transmit. Each device must wait its turn to transmit their data on the network. Only 1 device can communicate at a time and because of this there are no collisions. Collisions occur when multiple data transmissions interfere with each other causing none of the transmissions to be good. Token Ring and FDDI are technologies that use controlled access.

Slide 18



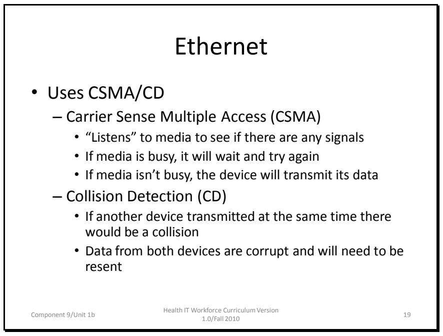
Media Access Control Continued

- Contention-based
  - Also called non-deterministic
  - Devices can transmit at any time
  - Collisions can occur
  - Examples
    - Ethernet
    - Wireless

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 18

In contention-based systems devices can transmit at any time. Collisions may occur. This method is also called non-deterministic. There is no mechanism to decide when a device can transmit data but the devices have to content with each other to access the media. Ethernet and wireless are technologies that use contention-based access.

Slide 19



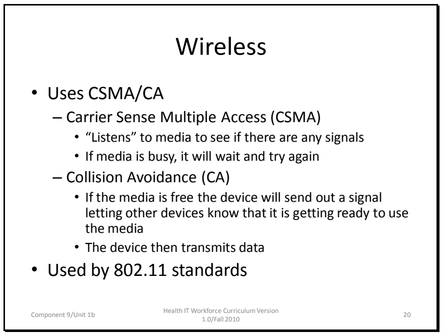
Ethernet

- Uses CSMA/CD
  - Carrier Sense Multiple Access (CSMA)
    - “Listens” to media to see if there are any signals
    - If media is busy, it will wait and try again
    - If media isn’t busy, the device will transmit its data
  - Collision Detection (CD)
    - If another device transmitted at the same time there would be a collision
    - Data from both devices are corrupt and will need to be resent

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 19

Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD). The device that has data to send will listen to the media to see if there is any signal being carried on the media. Remember media is the cable that is carrying the data. If there is a signal on the media it means that a device is already transmitting data and that device must wait and try to send its data later. If there is no signal the device can transmit the data by putting a signal on the media. It may happen that at the same time the device transmits its data, another device didn’t hear a signal on the media and it transmitted too. In that case there would be a collision causing both signals to become corrupt. The devices would detect the collision and know that they need to send the data again. They would both start the process of CSMA/CD again.

Slide 20

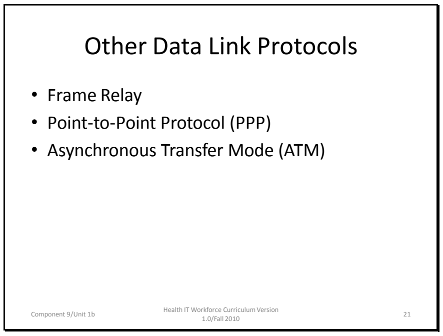


Wireless

- Uses CSMA/CA
  - – Carrier Sense Multiple Access (CSMA)
    - “Listens” to media to see if there are any signals
    - If media is busy, it will wait and try again
  - – Collision Avoidance (CA)
    - If the media is free the device will send out a signal letting other devices know that it is getting ready to use the media
    - The device then transmits data
- Used by 802.11 standards

Wireless technologies like the 802.11 standards use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). The device that has data to send will listen to the media to see if there is any signal being carried on the media. If there is a signal on the media that device must wait and try to send its data later. If there is no signal the device the device will send out a signal notifying the rest of the devices using that media that it is getting ready to send out data. This avoids a collision because other devices will not transmit. After issuing the notification the device then sends out its data.

Slide 21

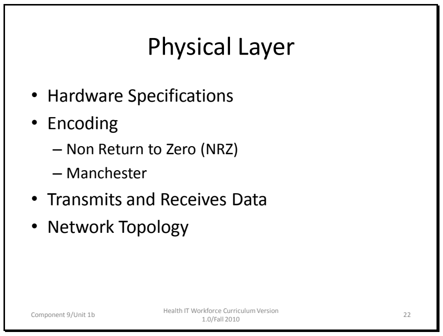


Other Data Link Protocols

- Frame Relay
- Point-to-Point Protocol (PPP)
- Asynchronous Transfer Mode (ATM)

Frame Relay, PPP and ATM are data link layer protocols that are used on WANs. Switches operate at the Data Link layer.

Slide 22



Physical Layer

- Hardware Specifications
- Encoding
  - Non Return to Zero (NRZ)
  - Manchester
- Transmits and Receives Data
- Network Topology

Component 9/Unit 1b Health IT Workforce Curriculum Version 1.0/Fall 2010 22

The physical layer transforms bits into signals to be sent across the network media. This is the layer at which data is actually transmitted across the network media. It is commonly reference as PHY. At the physical layer we have the specifications for hardware like network cables, connectors, wireless radio transceivers, etc. This layer is also responsible for data encoding. This is process of taking the data (0s and 1s) and turns it into as an electrical, optical or wireless signal that is transmitted over the media. Popular encoding methods are Non return-to-Zero and Manchester. Topologies are how network devices are connected to each other. Part of the topology involves the type of media that is used so the physical layer is concerned with this.