HCS 200b: Network Architecture

This lesson gives an introduction to the general architecture of health IT includes a brief overview of computer hardware, software, and network technology; Web services; and data storage. In-house architecture is contrasted with outside applications and service providers offering remote hosting. Medical and point-of-care devices that interact with information systems are discussed along with issues of connectivity and interoperability.

- HIT Computer Networks
- Networks: Intranet and Internet
- Understanding the OSI Model
- HIT Network Standards
- Flashcards
- Practice Quiz

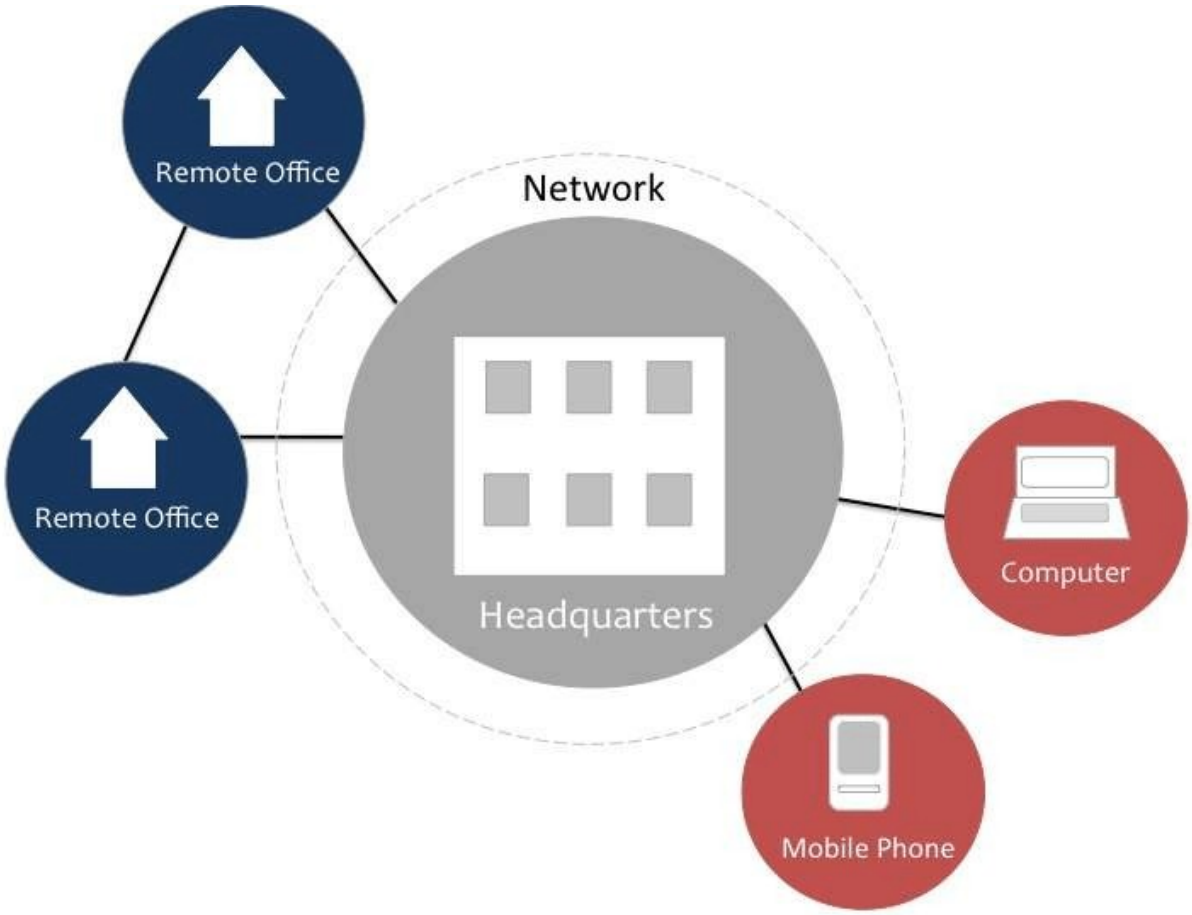
HIT Computer Networks

Computer users need a way to electronically communicate and to share computer resources with each other. A physician may want to send a prescription electronically to a pharmacy. The ofice administrator and the nurse in a physician's practice may have their own desktop computers but share a printer. A computer network makes electronic communication and resource sharing possible.

Computer Networks

A network is composed of connected computers, printers, and other devices, along with some sort of media. The term media, in a network context, refers to cabling and/or the ability to communicate wirelessly.

To visualize a network, examine the following figure. Both remote ofices shown in the figure have network connections to their headquarters and to each other. Remote users, perhaps at home or traveling, are also connected to the headquarters through network connections. Each site and each mobile device has computer hardware and software installed that supports the interface to the network.



Network Benefits

Network infrastructure supports computer applications at home and at work to provide advantages such as the following:

- Share hardware: Printer, scanner, data storage devices
- Share software: Software installed on a network server to reduce cost
- Share files: Images, spreadsheets, documents
- Communicate: Email, network phones, live chat, instant messaging

Networks decrease costs for businesses, individuals, and government in a variety of ways:

- Documents can be stored and accessed digitally on a network server (online). Users no longer need to update documents physically; instead, the user updates the single online copy and notifies other users of the changes.
- Technical support teams can access customer support documentation online. Again, if changes are needed, they can be done online, eliminating the need to reprint hundreds or perhaps thousands of copies.
- Email, which is possible only through a network, eliminates the need for interofice paper memos and mailing costs.
- Network administrators can manage and upgrade device software online, locate a device online, connect to the device, and make necessary changes. This capability eliminates the need to physically visit each computer device to perform needed upgrades.

Customer support shares these benefits and has some additional advantages that only networks can provide:

- Customers can conveniently chat or email with customer service representatives online.
- Customer satisfaction can be improved if customer service representatives have access to a common network database containing solutions to common customer requests or issues. If a representative solves a problem, the solution is immediately recorded and shared with other representatives around the world. If a recorded solution is unsuccessful, it can easily be replaced in the database with a solution that works.

Healthcare providers and patients also benefit from the availability of networks:

- Hospitals store all patient data in one common electronic medical record (EMR) network database, which improves patient safety and quality of care because the patient's medical record can be immediately updated electronically at the point of care.
- Medical staff access the EMR database online. When a nurse enters a patient's room, information can be transferred from his or her RFID badge to a screen in that room.
- The patient can see the name of the nurse on another screen. And, long after treatment is over, the patient can view his or her own medical history in a personal health record (PHR) online portal.

All of this is possible because the network technology is in place to support businesses, homes, and healthcare.

Knowledge Check

Which of these items was NOT included in the definition of network?

Media

Software

Computers

Computer devices

_____is/are cabling and/or the means for wireless communication.

Media

Software

Computers

Devices

Network Connections

An intranet network provides private communication capabilities for an organization or company. An intranet can connect users and various ofices regardless of their location. An intranet does not require an Internet connection even if the supported locations are physically separate locations.

All of the shared devices on an intranet, such as computers, scanners, and printers, require a network interface card (NIC). Each NIC has a media access control (MAC) address stamped on it, usually on a sticker.

Wired Network Connection

For wired network connections, each shared network device must have a cable-wired NIC with a port to plug in the copper network cable. The other end of the copper network cable plugs into a network switch. Switches forward trafic to devices in their network according to the MAC address of the devices.

Fiber-Optic Network Connection

For fiber-optic network connections, each shared network device must have a fiber NIC with a port to plug into a fiber-optic network cable . The other end of the fiber-optic network cable plugs into a switch or wireless access point (WAP) that has fiber-optic cable ports.

Fiber-optic technology is significantly more expensive than traditional copper cable but offers some benefits:

- Fiber-optic cable is not disturbed by high levels of nearby electricity, as is copper cable.
- One fiber-optic cable can replace thousands of copper wires and can extend well over 50 miles in length without losing signal strength.

Wireless Network Connection

For wireless network connections, each shared network device must have a wireless NIC and a WAP. If a device is moved too far away from a WAP, the network connection is likely to be lost.

A WAP is a wireless switch. Most WAPs have a few switch ports so they can support wired and wireless network switching.

Internet Network Connection

Access to the Internet network from an intranet network requires the purchase of a service plan from an Internet service provider (ISP). The ISP provides the necessary hardware, including a cable that connects to the Internet and a modem/router device.

Router~ A device that connects two networks together

Modem~ A device that makes it possible to transmit data to or from a computer or intranet network via telephone lines or ISP cable to a remote network location. [1]

The ISP modem/router has at least two ports:

- An intranet switch port where a cable from the intranet-wired switch or from the intranet WAP switch connects to the router.
- An ISP cable port where the modem plugs into the ISP Internet connection

When an intranet switch receives a destination address unknown to the switch, it sends it to the modem/router device. The router determines where that destination address is located and, if it is on the Internet, sends the message to the modem. The modem transmits the message through the ISP cable to the Internet destination address.

Network Speed

Networks measure speed in terms of bandwidth and throughput. Bandwidth is the highest number of bits that can be sent at any one time. Throughput is the amount of bandwidth that is available for actual network communications.

EXAMPLE

Bandwidth and Throughput
The bandwidth of a home network may be 100 megabits per second using copper network cabling, but the throughput is actually about 70 megabits per second. Because of the physical limitations of copper and other required network trafic and communication considerations, the network loses about one-third of its bandwidth to communication overhead.

The preceding example demonstrates that media influence network speed. Copper wire speed is commonly 100 to 1,000 megabits per second. Fiber-optic cable offers the same speeds as copper cable but can travel much longer distances.

Wireless communication speed is typically much slower. Currently, wireless speed runs at approximately 54 megabits per second. New wireless technologies, such as the Draft N wireless standard, promise improvements in speed of up to 200 megabits per second.

Knowledge Check

A wired intranet network connection must have each of the following except_____.

- media cabling
- a WAP
- a switch

A wireless intranet network connection must have_____.

media cabling

a WAP

a switch

Internet Protocol (IP) Address

An IP address is a numeric identifier used for both public Internet and private intranet purposes.

There are two versions of IP address:

IP version 4 (IPv4) has been used for nearly 50 years. There are 4,294,967,296, however, the range usually used in private natting is 192.168.10.1 through and including 192.168.10.254.

These are primarily used through a router for home use.

IP version 6 (IPv6) was created to augment IPv4. There are literally millions of IPv6 addresses. An IPv6 address might look like this:

68.12.13.14

Consider the following example during this discussion of private and public IP addresses.

EXAMPLE

Using Public and Private IP Addresses

Dr. Watanabe's practice ofice has a small EMR system supported by an intranet network with several shared devices. The intranet switch is attached to several computers and several printers.

Dr. Watanabe has also subscribed to an ISP for Internet access. His network has an Internet modem/router, which is plugged into the ISP cable and is attached to the intranet switch.

Private IP Addresses (Intranet)

Private IP addresses are used on an intranet network. A private IP address is valid only on that network. A private IP address is assigned to each shared device on the intranet.

EXAMPLE

Private IP Addresses as Sender and Receiver

Dr. Watanabe wants to print a patient's medical record. Both his computer and the printer are shared devices on the ofice intranet. The request to print goes from his computer, through the switch, to the printer, and the record is printed.

In this network request, the computer's private IP address is the sender, and the printer's private IP address is the receiver.

Because an intranet is a private network, it does not matter that separate intranet networks use the same IP addresses at the same time. That fact, coupled with some clever intranet design, allows most intranet network administrators to limit their IP addressing to the available addresses of IPv4.

Public IP Addresses (Internet)

Public IP addresses are used to communicate with sites on the Internet. All modem/routers connected to the Internet are assigned a public IP address.

EXAMPLE

Public IP Addresses as Sender and Receiver

Dr. Watanabe submits an order to the EMR system to send an e-prescription to a patient's pharmacy. The request goes from his computer to the switch. The switch does not recognize the IP address of the pharmacy, so it passes the request to the modem/router. The modem/router sends the request across the Internet. The Internet uses the pharmacy's IP address to deliver the e-prescription.

In this Internet request, the public IP address of the modem/router is the sender and the pharmacy's public IP address is the receiver.

Sites on the public Internet are growing in number, and so is the need for public IP addresses. In December 2011, IPv4 was depleted and the Internet began using IPv6. Because millions of IPv6 addresses are available, it is unlikely the Internet will run out of them in the foreseeable future.

Knowledge Check

A_____IP address is assigned to each shared device on an intranet.

private

public

A_____IP address is assigned to each shared device on the Internet.

private

public

The same IP address might be used on many different _____networks.

private

public

References/Sources

1 DifferenceBetween.netDifference between Modem and Router. http://www.differencebetween.net/object/difference-between-modem-and-router/.

This product is funded by the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program (#TC-26440-14-60-A-21).

Continue with other activities/quizzes...

Networks: Intranet and Internet

Home, business, and healthcare computer users need access to private (intranet) and public (Internet) networks. An intranet user shares internal computer resources. An Internet user communicates with outside entities and resources.

A network administrator evaluates and implements the network infrastructure and required technologies to support both intranet and Internet networks. Most home computer users act as their own network administrator without even realizing they are filling that role. Business and healthcare environments usually require a professional network administrator to handle their often extensive networks.

The professional network administrator considers many factors when designing the intranet and Internet solution to fit a business's or healthcare provider's needs, including network connections and IP addresses. Additional considerations relate to issues associated with private networks (intranet) and public networks (Internet).

Private Network: Intranet

When considering private intranet networks, size is a relative term. An intranet that services a home or a small physician ofice would probably qualify as small, whereas an intranet that supports the federal Veterans Health Administration would certainly qualify as large.

The health information technology (HIT) network administrator is the professional who evaluates and implements the appropriate intranet network on the basis of the size of the healthcare facility.

Local Area Network (LAN)

A LAN might serve a home, a physician ofice, a clinic on one floor of a building, a small hospital with one building, or a hospital with two or three buildings.

LAN Workgroup

If 10 or fewer devices are shared on a LAN, the network administrator would probably establish a workgroup to manage the network. No server is utilized, so this type of LAN is considered a peer-to-peer network.

EXAMPLE

A Peer-to-Peer LAN

Dr. Watanabe's ofice intranet is set up as a peer-to-peer LAN. His ofice administrator, Kenisha Waters, acts as network administrator.

Kenisha sets up each computer in the ofice as a member of the ofice workgroup. She specifies which devices attached to each computer are to be shared.

If Dr. Watanabe's PC is connected to a printer that the nurse needs to use, Kenisha configures the doctor's computer to share the printer on the ofice workgroup. Similarly, if Dr. Watanabe needs files that are stored on the nurse's desktop computer, Kenisha configures the nurse's computer to share them on the ofice workgroup.

Each time a request is sent to access a shared device on the network, the private IP address of the sender and the private IP address of the receiver are embedded in the message. The message travels through the network cables and switch until it finds the receiver. When the receiver completes the request, it sends back an acknowledgment to the sender.

LAN Client/Server

For LANs with more than 10 to 12 devices being shared, the network administrator would probably set up a client/server LAN. A client/server model is a computing structure that separates tasks or workloads between service providers, called servers, and service requesters, called clients. [1]

EXAMPLE

A Client/Server LAN

Adam Hospital has three separate buildings in close proximity to each other and about 100 devices to be shared.

Glenn Kelly, its network administrator, configured a network server and built server tables to identify all shared computers, devices, files and databases. He installed network software on each client computer and enabled the shared devices on each.

If a hospital laboratory technician sends a request from the desktop computer at her station to print a document, that request goes to the network server. The server forwards the request to the specified computer connected to the shared printer. The printer prints the page and sends an acknowledgment back to the server. The server forwards that acknowledgment to the laboratory technician's computer.

Metropolitan Area Network (MAN)

The larger the facility an intranet must serve, the more complex and sophisticated the infrastructure and network administration becomes. If a network comprises several geographically separate locations in the same city, it is called a MAN. A MAN usually consists of one or more LANs. The MAN may or may not have Internet access for its users.

EXAMPLE

Use of a MAN

BGR Hospital has three separate locations in the metropolitan area and several small satellite facilities that handle outpatient clinic care. Jose Stetcher, the network administrator for BGR, set up several network servers to support the large number of client devices and shared resources. Jose configured the network with fiber-optic media to support the intranet need for speed and stability.

Wide Area Network (WAN)

A network that must service a large geographical area is called a WAN. A WAN generally consists of one or more LANs. A WAN may exist within one company across multiple sites in a wide geographic area. It may or may not have Internet access.

EXAMPLE

Use of a WAN

The Better Skilled Nursing Company has facilities in Chicago and Cleveland and a shared WAN that supports all internal communication.

Evergreen Pharmacies is a nationwide company with pharmacies throughout the United States. It maintains a very large WAN network. Each location has its own LAN to support its routine in-house needs, and those individual LANs are networked across a WAN, which allows the pharmacies to quickly share patient information across locations.

Knowledge Check

If a network administrator chooses a peer-to-peer LAN intranet design, the network probably has_____shared devices.

more than 10

10 or fewer

Which answer choice best describes the needs of users on a private intranet?

The ability to communicate with outside entities and resources

The ability to share internal computer resource

Each of the following is a characteristic of the server in a client/server LAN except_____.

a computer that stores shared files, databases, and software applications.

a computer with a special network operating system.

a computer on a user's desktop or a user's mobile devices.

a computer with a high-speed CPU, large amounts of memory, and high-capacity disk drives.

Intranet Topology

The network administrator must design and implement the intranet topology that best fits the needs of the organization.

Topology~ The organization or layout of a network

Physical topology~ The layout of the network hardware components and method used when messages are sent and received by those components

Logical topology~ A diagram that illustrates the network data flow without regard for the network's physical topology

There may be some overlap between the physical and logical topologies. Following are a few of the more common topologies.

Bus Topology

In a bus topology, each shared computer is connected to every other computer by a single network cable with NIC connectors.

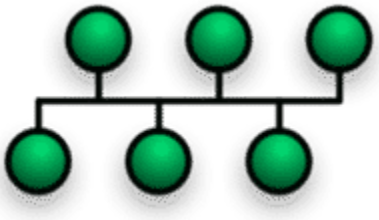


Image courtesy of Foobaz.

If a single bus cable breaks, the whole network goes down. Originally, bus networks were configured with coaxial cable, which proved to be unreliable and dificult to scale. Coaxial cable has been replaced by Ethernet cable. Ethernet is much easier to work with and is not subject to a single point of failure, as is coaxial cable. Ethernet cable is also less costly.

Ring Topology

Within a ring topology, each shared computer is connected to the network in a closed loop, or ring.

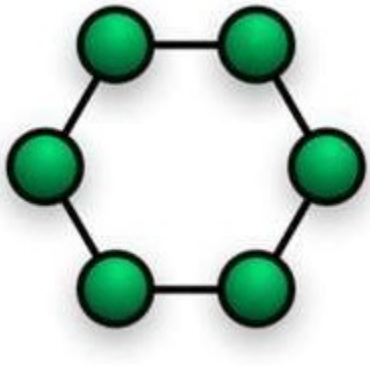


Image courtesy of Foobaz.

Ring topology is usually found in highly secure environments. Ring topologies typically use an electronic token-passing scheme, which controls access to the network. Only one machine can transmit on the network at any given time.

Star Topology

The star topology is the most commonly used topology and the easiest to set up and maintain.

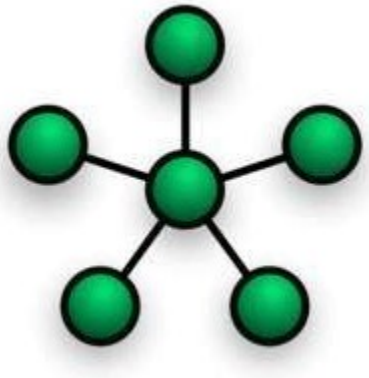


Image courtesy of Foobaz.

In a star topology, all trafic passes through the switch that is at the middle, or hub, of the network. At the outside end of each star point are end devices such as computers and printers.

An extended star topology connects a number of switches to each other.

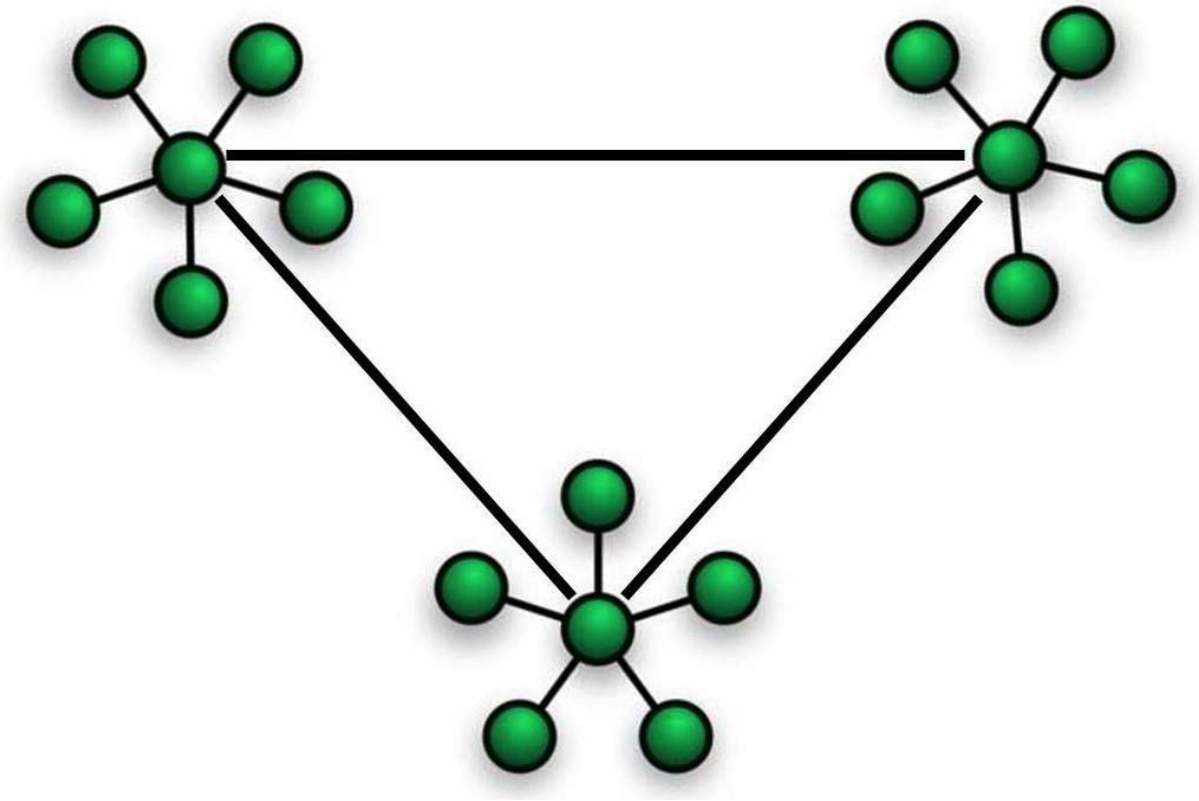


Image courtesy of Foobaz.

In an extended star topology, all shared computers can communicate with all other shared computers, assuming a proper design, IP addressing, and appropriate network permissions.

Mesh Topology

Mesh topology is slightly different from the other topologies. It describes the connections between modem/routers rather than among shared network computers or devices.

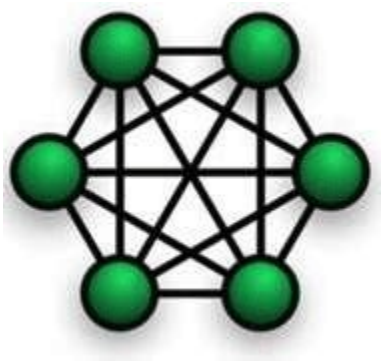


Image courtesy of Foobaz.

With mesh topologies, each modem/router in the network is connected to every other modem/router in the network.

Logical Topology

Logical topology, as opposed to physical topology, depicts the way data passes through the network from one device to the next without regard to the physical interconnection of the actual devices. In other words, in logical topology, the location of the computers, devices, or switches is not important as long as they are somehow connected. A network's logical topology is not necessarily the same as its physical topology.

If an Ethernet cable interconnects devices to a common switch, this might be referred to as a logical bus, but physically, the network may be a star layout.

Knowledge Check

When the network administrator determines how the network is organized, he or she has determined the network's_____.

physical layout

topology

logical layout

mesh design layout

Public Network: Internet

Most home computer users regularly access the Internet for shopping, surfing, email, and social networking. Most businesses and healthcare entities also find many uses for Internet access.

EXAMPLE

Tasks Requiring Internet Access

Healthcare providers must interface with entities that are not connected to their own private intranet, which requires Internet access. Here are some tasks that require Internet service:
A physician sends an e-prescription to a patient's local pharmacy.

A hospital sends quality measurement data to the Centers for Medicare and Medicaid Services (CMS) in order to benefit from the associated reimbursement incentives.

An informaticist accesses a registry database where health data has been accumulated from across the nation or even from around the world.

And what business or healthcare entity can survive without email and, increasingly, instant messaging?

The network administrator designs and implements Internet access according to the needs of the business or healthcare users.

Internet service providers (ISPs) connect users to the Internet. ISPs are organized as local, regional, and national providers and, in some cases, even international providers.

Internet users usually have a contract with an ISP that allows connection to the Internet using that ISP's services.

Internet Connections

A number of methods are available to connect to the Internet. Each has different considerations.

Dial-up Internet Connections

Dial-up connections use telephone lines to connect to an ISP's modem/router. Speed — or bandwidth — is limited to 56 kilobits per second. This is the slowest connection type.

Broadband Internet Connection

Broadband connections are of higher quality than telephone lines. They use coaxial or fiber-optic cable to connect to an ISP's modem/router. Broadband is faster than dial-up and runs in the approximate speed range of 100 megabits per second or higher.

WiFi Internet Connection

WiFi is a wireless Internet connection frequently found in hotels and public venues such as airports, libraries, college campuses, and coffee shops. The subscriber in this case is the owner of the location where the WiFi is installed.

WiFi typically connects a visitor's laptop, equipped with a wireless NIC or wireless modem, through the location's ISP modem/router to the ISP cable.

Under ideal conditions, WiFi speed ranges from 1 to 200 megabits per second. The farther away a user is from a wired access point, the lower the network speed or bandwidth.

Satellite Internet Connection

Satellite Internet connections are typically used by mobile devices such as iPads and smartphones:

- The mobile device contacts a ground satellite dish.
- The ground satellite dish sends the signal to a satellite that is orbiting the earth.
- The orbiting satellite relays the signal to a ground satellite dish closer to the destination.
- If there is a response, the return trip repeats this sequence in the opposite direction.

A satellite connection can be slow because of the round trip. The loss of speed that results from the signal bouncing around is called latency.

Third- and fourth-generation (3G and 4G) mobile devices have speeds ranging from 200 kilobits to as high as 100 megabits per second.

Internet Service Provider

An ISP purchases public IP addresses from regional organizations responsible for managing public IP addresses. The ISP then leases those public IP addresses to subscribers for business or home use.

The ISP typically leases one public IP address and a modem/router to each physical location. That modem/router is attached on one side to the ISP's cable and on the other to the subscriber's private intranet and translates between them.

Most ISP leases provide a dynamic public IP address that may change from day to day. If a subscriber needs a static public IP address, the ISP charges as much as $100 a month more for the privilege of having a public IP address that never changes.

Internet websites such as www.whitehouse.gov/ use a static IP address so that the site is reliably mapped to one public IP address.

Internet Domains

Imagine trying to navigate the Internet using IP addresses such as 68.12.13.14 rather than names such as www.whitehouse.gov. People remember names more easily than they do numbers.

Individuals and organizations can purchase a domain name from the Internet Corporation for Assigned Names and Numbers (ICANN). To own a domain name is to take administrative

responsibility and control of the name within the Internet-based domain name system (DNS).

The domain name www.whitehouse.gov suggests the White House is responsible for the administration of this Web site.

What's in a Domain Name?

Domain names are composed of three distinct parts, each separated by a dot (.) Using www.whitehouse.gov as an example:

- The www portion of the domain name indicates that this name is associated with the World Wide Web.
- The domain name, whitehouse, is a purchased domain name.
- The sufix gov indicates a government entity type.

Just because a domain name ends with .edu or .org or .gov does not prove that the entity is that type of organization. Anyone can buy any available domain name with any extension if it is not already owned. Therefore, the sufix does not necessarily indicate the type of entity that owns www.whitehouse.gov. Discovering the owner would require further investigation.

Domain Name Resolution

An Internet browser is the tool that resolves (translates) a domain name into a specific Internet IP address. When a user types in a domain name, the browser contacts a domain name server (DNS) to translate the name to the IP address. If the DNS provided by the ISP cannot resolve a domain name, the ISP connects to the global DNS servers for help.

Finally, when the browser learns the destination IP address from a DNS server, network connection to the Internet website is complete.

Knowledge Check

How might a healthcare provider use the Internet?

- sending emails to coworkers announcing policy changes
- sharing computer resources
- sending an order from a small physician office to an outside pharmacy or laboratory
- sharing patient records with physicians on staff at a hospital

Which type of Internet connection provides the slowest connection?

Dial-up

Broadband

WiFi

Where can a healthcare provider buy an Internet domain name?

From ICANN

From an ISP

From the healthcare provider's network administrator

From Amazon.com

What is an Internet domain?

A name given to a private IP address

A name given to a public IP address

A service an ISP offers to special customers

A name given to a local physical address

References/Sources

1 Health IT Workforce Curriculum, Version 3.0 (Spring 2012). Component 8, Installation and Maintenance of Health IT Systems. Unit 1a, Elements of a Typical EHR System. This material Comp8_Unit1a was developed by Duke University, funded by the Department of Health and Human Services, Ofice of the National Coordinator for Health Information Technology under Award Number IU24OC000024.

This product is funded by the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program (#TC-26440-14-60-A-21).

Continue with other activities/quizzes...

Understanding the OSI Model

The OSI model defines a networking framework in seven layers. Control of the data passes from one layer to the next, starting at the sending station's application layer, and then working down through the model, to the bottom layer. Control of the data then passes across the physical connection between each station along the path and then back up the model layers to the top layer at the receiving (destination) station. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Standardization Organization (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications. Figure 1 shows this process.

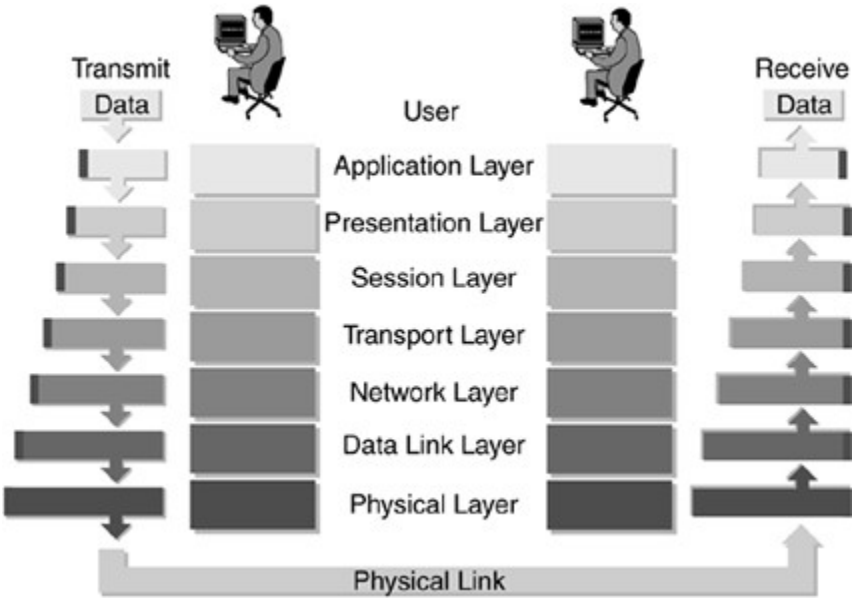


Figure 1: OSI Model

In the networking environment, the OSI is the universal model and is made up of seven layers, each layer providing a service to the layer above it and dependent on the layer below.

These seven layers are as follows:

- Layer 7 Application
- Layer 6 Presentation
- Layer 5 Session
- Layer 4 Transport
- Layer 3 Network
- Layer 2 Data link
- Layer 1 Physical

Layers 1 through 4 are referred to as the lower layers, and Layers 5 through 7 are referred to as the upper layers. Each layer performs a specific function in itself and provides a service to the layer above it. For example, Layer 2 (data link) depends on services provided to it by Layer 1 (physical) and provides services to the layer above it, Layer 3 (network). Each layer of the OSI model performs a specific function, as discussed in more detail in the following sections, starting with the uppermost?Layer 7, the application layer.

Layer 7 Application Layer

The application layer is the user-interaction layer, enabling the software and end-user processes. Everything at this layer is application specific. For example, a web browser application for surfing the Internet would use this layer. The application layer provides application services for file transfers, e-mail, and other network-based software services, such as your web browser or e-mail software.

Layer 6 Presentation Layer

The presentation layer provides for data representation to the user, such as a document (.doc)

or spreadsheet (.xls). The presentation layer also "translates" the user data into a format that can be carried by the network, such as the segments and packets required at the lower layers. The presentation layer converts your data into a form that the application layer can accept, such as converting a string of data into a recognizable file format, such as .doc (word processing document) or .jpeg (graphics format). The presentation layer formats and encrypts data (when required by the user's application) to be sent across the network.

> Encryption is the process by which original data, or plaintext, is converted into an unreadable format, or ciphertext, that can be read by only its intended recipient. The encryption process is based on a mathematical algorithm, or code, to create the ciphertext.

Layer 5 Session Layer

The session layer establishes, manages, and terminates virtual communications connections between applications. In other words, the session layer starts and stops communication sessions between network devices. When you place a telephone call, for example, you are establishing a communication session with another person. When you are finished with the call, you hang up the telephone, which terminates the session.

Layer 4 Transport Layer

The transport layer provides data transfer between end systems and is responsible for end-to-end error recovery and flow control. Flow control ensures complete data transfer and provides transparent checking for data that might have been dropped along the way from sender to receiver. Error recovery retrieves lost data if it is dropped or suffers from errors while in transit from source to destination.

Layer 3 Network Layer

The network layer provides the routing technologies, creating a forwarding table or a logical path between the source and destination. These logical paths are known as virtual circuits and are considered to be point-to-point network connections. Routing and forwarding are

functions of the network layer. Network addressing, error handling, congestion control, and packet sequencing are all functions of the network layer.

- The network layer is where routers and routing protocols operate.
- Error handling is the response to an error that advises either the user or another process that an error has occurred. Error correction is the action taken to correct the error. Examples of error correction methods include resending the data or the application, or "figuring out" the corrupted data by the use of a checksum (a mathematical operation based on the number of 1s and 0s in the data).

Layer 2 Data Link Layer

At the data link layer, data packets are placed into frames for subsequent transmission across the network. The data link layer provides the transmission protocol knowledge and management and handles physical layer errors, flow control, and frame synchronization.

The data link layer is divided into two smaller sublayers: the Media Access Control (MAC) layer and the logical link control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking.

Think of the MAC and LLC sublayers as the pilot and copilot of an aircraft. The MAC sublayer prepares the frame for physical transmission, much as the pilot focuses on the physical aspects of flying the aircraft. The LLC sublayer is concerned with the logical aspects of the transmission, not with the physical aspects of the transmission. The LLC layer acts like the copilot, who focuses on navigation, leaving the physical aspects of flying to the pilot.

> Bridges and traditional switches operate at the data link layer.

Layer 1 Physical Layer

The physical layer carries the bit stream through the network. The bit stream can be carried as an electrical, light, or radio signal. This layer provides the hardware means of sending and receiving data on a carrier, including defining the cables, cards, and physical aspects. Gigabit Ethernet, wireless, dense wavelength-division multiplexing (DWDM), Synchronous Optical Network (SONET), Electronic Industries Alliance/Telecommunications Industry Alliance 232 (EIA/TIA–232; formerly RS–232), and Asynchronous Transfer Mode (ATM) are all protocols with physical layer components.

Medium and Signal Type

Fiber Optic –light signal
Copper - electrical signal
Air - wireless, radio signal

- Hubs and repeaters operate at the physical layer.

To better understand how network switching works, it is vital to understand how the OSI model works and how data moves through the OSI model. How you move through the OSI model depends on whether you are the sender or the receiver. The sending side wraps, or encapsulates, the data, much as you enclose a letter in an envelope. The receiving side unwraps, or decapsulates, the data, much as the receiver opens an envelope to remove the contents.

Sending, or encapsulating, data requires five steps, as follows:

1. Step 1. User data (Layers 5, 6, and 7 – application, presentation, session)
2. Step 2. Segments (Layer 4 transport)
3. Step 3. Packets (Layer 3 network)
4. Step 4. Frames (Layer 2 data link)
5. Step 5. Bits (Layer 1 physical)

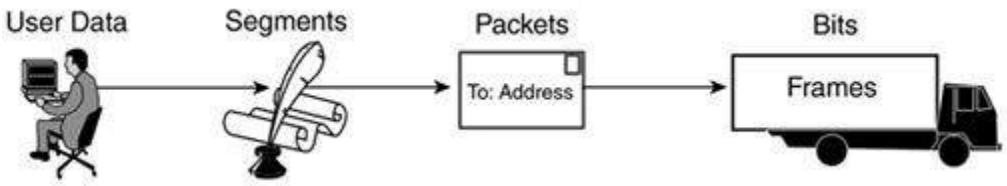


Figure 2: Data Encapsulation

Figure 2 shows data (in this case, old-fashioned mail) being sent (or encapsulated) as follows:

User data (Layers 5-7) – You write your words using a specific style, such as Roman characters or script, on a piece of paper, in a certain language, such as English.

Segments (Layer 4) – You fold the paper and place it into an envelope. If your letter is made up of multiple pages, each page, or "segment," is numbered so the letter is reassembled in the correct order by the receiver.

Packets (Layer 3) – You write the sender's and receiver's postal address on the envelope. Like an envelope, a packet contains user information and identifies the sending and receiving address.

Frames (Layer 2) – Your letter is put into a mailbag with other letters to be carried to the same destination. The mailbag here is the frame carrying multiple packets. These frames are put onto a mail truck, in which a truck driver carries the envelope to its destination.

Bits (Layer 1) – The truck is driven across the highways and other roads to reach the receiver.

1. The mail truck arrives at its destination, carrying the envelope.
2. The receiving station examines the destination address on the envelope and delivers it to that address.
3. Someone at the receiving address opens the envelope and extracts the paper.
4. The paper's recipient then reads the contents, the words and paragraphs, of the letter.

The internetworking environment is governed by two complementary rule sets: standards and models. Standards are the laws that vendors must adhere to if they are to interoperate with other vendors, in turn making themselves available and useful for the end user. Some vendors develop special features that can be configured and used only on their equipment; these are called proprietary features. Keep in mind, a proprietary implementation can limit

itself in its use and therefore is not always an attractive option when implementing a network.

The OSI model is the universal model in the networking environment and is made up of seven layers. Each of the seven layers provides services to the layer above it and depends on the layer below. The seven layers of the OSI model from top to bottom are (7) application, (6) presentation, (5) session, (4) transport, (3) network, (2) data link, and (1) physical.

The application, presentation, and session layers are known as the upper layers; the transport, network, data link, and physical layers are known as the lower layers.

The OSI model uses encapsulation and decapsulation, depending on where data is moving through the model. The sending side wraps, or encapsulates, the data, much like enclosing a letter in an envelope. The receiving side unwraps, or decapsulates, the data, much like opening an envelope and removing the contents.

The International Organization for Standardization (ISO) created the Open Systems Interconnection (OSI) reference model as a framework for defining standards for connecting computers. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model. The ISO–OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.

Which layer provides data transfer between end systems?

Layer 1

Layer 2

Layer 3

Layer 4

Layer 5

Layer 6

Layer 7

Which layer carries the bit (electrical, light, or radio signal) stream through the network?

Layer 1

Layer 2

Layer 3

Layer 4

Layer 5

Layer 6

Layer 7

Which layer enables the software and end-user processes.?

Layer 1

Layer 2

Layer 3

Layer 4

Layer 5

Layer 6

Layer 7

This product is funded by the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program (#TC-26440-14-60-A-21).

Continue with other activities/quizzes...

HIT Network Standards

A network provides a pathway for electronic communication between users and allows users to share resources such as computers, printers, and other devices. These network functions require the use of media and a variety of electronic devices such as switches, wireless access points (WAPs), routers, and modems.

Standards enable products from different vendors to work together. Protocols govern communications. Internet Protocol provides a global standard for communication on the Internet.

Standards and protocols ensure computer hardware and software devices are interoperable when communicating through an intranet network or on the Internet.

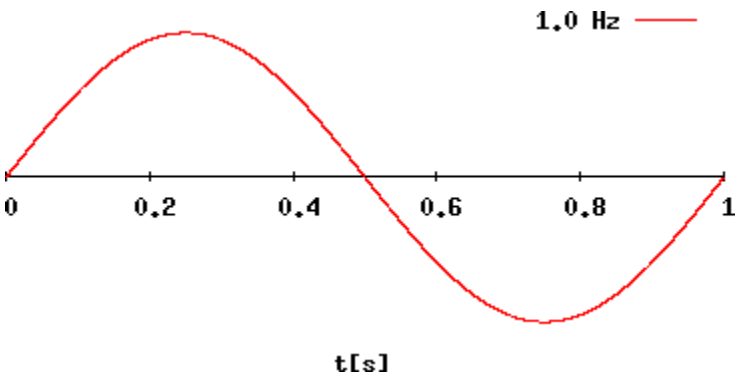
Network hardware and media must be interoperable from several perspectives. The electronic or wireless signals must be on the same wavelength, literally. The hardware must interface effectively. The format of the messages sent must be decipherable to the receiver.

Network Interoperability

Frequency

Data communicated through a wired network is transmitted in the form of electrical waves. A wireless network transmits using radio waves. Electrical and radio waves have frequencies. Both the sending and the receiving devices must be using the same frequency for the communication to succeed.

In cloud computing, users access resources (hardware, software, data storage) that are hosted on the Internet rather than physically maintained at the users' location. Cloud computing users may need nothing more than a device, such as a laptop, smartphone, or tablet PC, with Internet connection.



EXAMPLE

Frequency Mismatch

Sender A is a laptop PC transmitting on a wireless 2.4 gigahertz frequency.
Receiver B is a wireless WAP switch looking for signals on a 5.0 gigahertz frequency.
Communication fails because the sender is on a different frequency from the receiver.

Hardware and Media

The physical hardware on a network must be interoperable. If an American travels to Europe and tries to plug in an American–made hair dryer, the plug will not fit in the socket because Europe uses alternating current and America uses direct current electrical standards.

The same is true for physical hardware. Plugs must be designed and manufactured to fit into sockets. The media must be designed and manufactured to accept the electrical frequency that is transmitted. The network interface card (NIC) port on the computer must expect the same media that connects to the switch. The port on the switch must utilize the same media as the ISP connection.

EXAMPLE

Cabling Mismatch

Sender A is a laptop PC transmitting on a 2.4 gigahertz frequency through copper wire cabling.
Receiver B is a wired network switch on the same frequency but expecting fiber optic cabling.
Communication fails because the hardware and media are not interoperable.

Protocol

The network message must be decipherable by the receiver. If an American travels to the Democratic Republic of the Congo and speaks only English, the American will have a very dificult time communicating. In the same way, a network message that travels to a receiver that does not "speak" the same protocol cannot be processed by the receiver.

A network protocol is a set of rules and conventions that ensure consistent communication between network devices. Network messages are generally sent and received in the form of packets [1] , as defined by the network protocol.

EXAMPLE

Protocol Mismatch

Sender A is a laptop PC transmitting on a 2.4 gigahertz frequency through copper wire cabling but using a nonstandard network protocol.
Receiver B is a wired network switch on the same frequency and media but expects standard network protocol.
Communication fails because the network protocol cannot be interpreted by the receiver.

EXAMPLE

Successful Communication

Sender A is a laptop PC transmitting on a wireless 5.0 gigahertz frequency and using a standard network protocol.
Receiver B is a WAP switch on the same frequency and expecting the same standard network protocol.
Communication succeeds!

Knowledge Check

The network device sending messages is transmitting on 2.4 gigahertz, and the receiver is looking for messages on 5.0 gigahertz. The reason the communication will fail is that different _____are used by the sender and receiver.

- hardware and media
- network protocols
- electronic or radio frequencies
- software protocols

The network device is configured with a fiber-optic NIC. The network switch is configured to accept copper cabling. The reason the communication will fail is that different_____are used by the sender and receiver.

hardware and media

network protocols

electronic or radio frequencies

software protocols

The network device formats the message with a packet of 25 characters in length. The receiving device expects the packet to be 30 characters in length. The reason the communication will fail is that different_____are used by the sender and receiver.

hardware and media

network protocols

electronic or radio frequencies

software protocols

Network Standards

Networks achieve interoperability through adherence to industry standards and protocols. Every manufacturer who produces network devices or media and whose device transmits or receives network messages must meet these standards.

In healthcare, the HITECH Act enforces adherence to standards and protocols through the certification requirements for meaningful use. This enforcement of standards supports the healthcare network administrator's efforts to achieve interoperability.

The IP addressing standard enables any network device with network access to communicate with any other device on the network. Two versions are currently in use:

-IPv4: Original standard with limited number of IP addresses
-IPv6: Latest standard with millions of IP addresses available

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a technical standard that governs the transport of messages across the Internet for delivery to their destination.

The Hypertext Transfer Protocol (HTTP) is a technical standard used on the World Wide Web that enables any Web browser to communicate with any Web server.

The WiFi standard defines throughput and message frame formats for equipment and frequencies used for wireless communication. The standards are

-IEEE 802.11 A 5.0 gigahertz
-IEEE 802.11 B 2.4 gigahertz
-IEEE 802.11 G 2.4 gigahertz
-IEEE 802.11 N 2.4 and 5.0 gigahertz

The Wireless Application Protocol (WAP) defines a technical standard for smartphones, mobile phones, and PDAs. This protocol defines application layer, network communications, and wireless standards. This standard includes a protocol suite enabling the interoperability of WAP equipment and software with many different network technologies.

The RFID standard relates to the circuitry that stores information on the tag and to the antenna that sends and receives signals. The RFID standard is overseen by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

The Bluetooth standard addresses the open, wireless technology for exchanging data over short distances from fixed and mobile devices. Bluetooth is used in devices such as medical implants, keyboards, mouse devices, and cell phone headsets. The standard is IEEE 802.15.

Wireless Networks

The demand for wireless communication is already extensive and is growing. Network administrators must consider the qualities inherent in wireless networks to effectively establish wireless network support.

Wireless networks offer some appealing advantages:

- No cable media is needed, so the physical work environment is cleaner.
- Wireless devices are portable, which is convenient for the user. For example, a student with a laptop PC on a campus can connect to the campus WiFi for Internet access everywhere on campus.

Wireless networks also present some serious issues:

- Signal interference and other factors slow network throughput speed.
- Signal range is limited. The further a wireless device is from the WAP switch, the slower the throughput. If a campus user leaves campus, the Internet connection is lost completely.
- Security is a significant concern because wireless signals travel freely through the air on radio waves. Hackers and identity thieves use special software called sniffers to capture signals from wireless devices in the sniffer's range.

Device configuration is more complex for wireless networks than for wired, in part because of the security concerns. Some of those complexities include the following:

- Each WAP switch must be assigned a wireless channel, a service set identifier (SSID), a password, and a wireless security code in addition to its IP address.
- Wireless devices communicating with this WAP switch must match all these settings, although each device will have its own unique IP address.

Knowledge Check

A network application uses an Internet Web browser to interact with an application housed on an Internet Web server. What is the required protocol?

HTTP

RFID

Bluetooth

TCP/IP

A wireless network device must meet the same industry standard used for mobile phones and smartphones. What is the standard?

HTTP

RFID

WAP

WIMAX

The major advantage of the wireless network, of course, will be the convenience and_____for the physicians within range of the network WAP switch.

mobility

security

complexity

protocols

HIT Point of Care (POC)

Medical testing and analysis is scientific in nature, involving chemistry and medical science. Traditionally, samples for analysis were drawn at the point of patient care, but the sample analysis and findings reports were performed by accredited clinicians in an independent or hospital-based laboratory.

With the proliferation of new POC devices, it is possible to draw samples, perform analysis, and generate findings at inpatient bedside, in physician ofices, and even in a patient's own home.

Laboratory technicians in traditional settings—independent or hospital-based laboratories—also find themselves using more modern and electronic testing devices.

POC devices are getting smaller, faster, smarter, and cheaper, and POC is increasingly cost effective. Examples of POC devices include the following:

- Blood glucose meters and kits
- Nerve conduction study devices
- Test kits for use in diagnosis related to blood gas analysis, blood clotting, pregnancy, rapid strep, cardiac marker, lipid, HIV, influenza, and many other diagnostic applications [2]

Image of blood glucose kit

Fixed POC devices, such as the following, are used when a handheld device is not available:

- Small benchtop analyzers
- Inpatient bedside monitor for vital signs

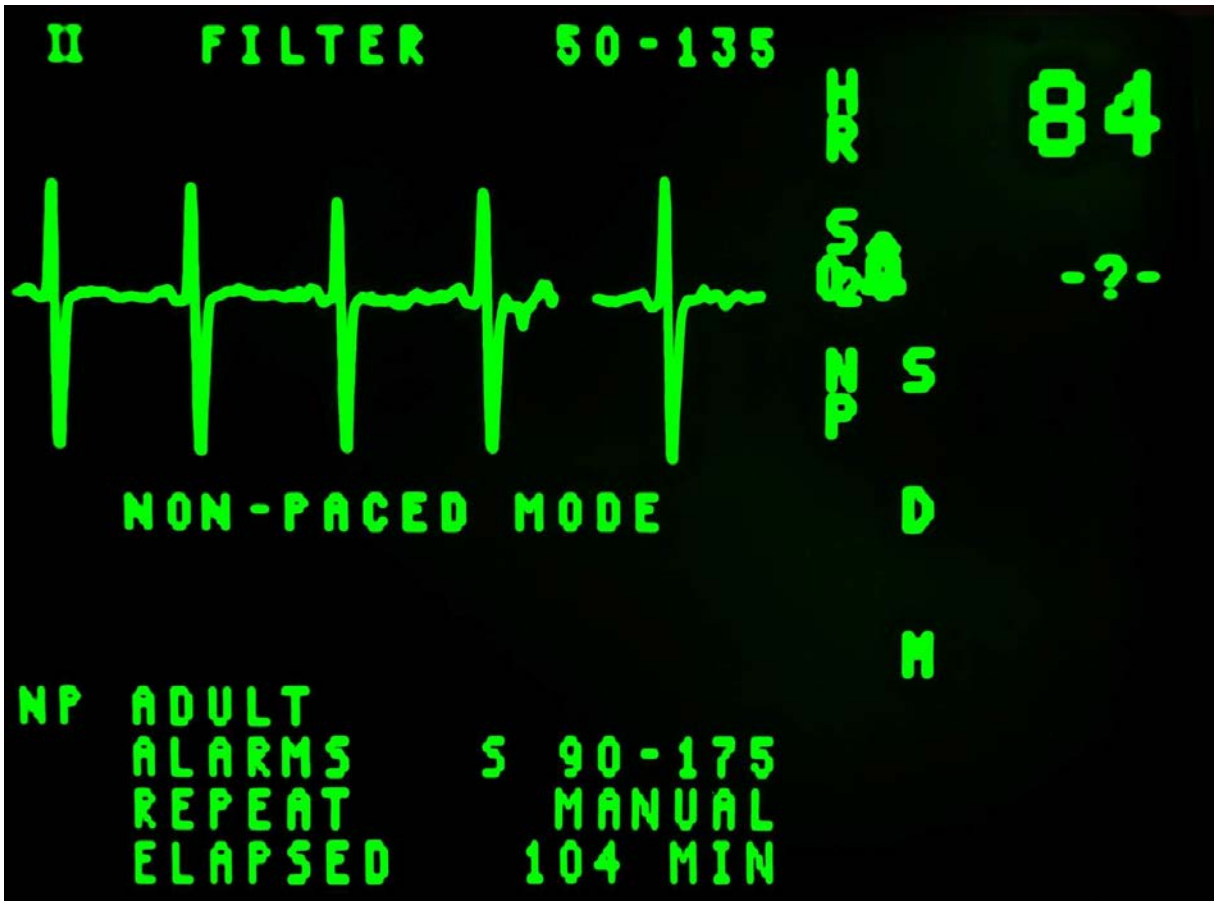


Image of a heart rate

The eficacy and accuracy of handheld POC device findings is controversial, particularly when the traditional expertise of the professional laboratory clinician is bypassed. However, the trend toward use of these devices is here to stay.

HIT POC Standards

As with any area of health IT, POC device standards are essential to safeguard patient safety and quality of care. The scientific nature of POC data and devices calls for new interoperability standards to define network access points, network protocols, and data management and to interface with clinical information systems such as laboratory and EMR.

A group of specifications was developed as the core of the POC standard by the Connectivity Industry Consortium (CIC) in a cooperative effort of providers, manufacturers, and representatives of

–Clinical and Laboratory Standards Institute (CLSI)
-Health Level Seven International (HL7)
-Institute of Electrical and Electronics Engineers (IEEE)
–College of American Pathologists (CAP)
–US Food and Drug Administration (FDA)
-Japanese Committee of Clinical Laboratory Standards (JCCLS)
-International Federation of Clinical Chemistry and Laboratory Medicine (IFCC) [3]

Healthcare systems and network administrators have very specific challenges with the interoperability and with the scientific nature of the data communicated by POC devices whether they are wired or wireless. The CIC standards set the stage for network support and POC device implementation solutions.

Knowledge Check

HIT point-of-care (POC) testing devices are getting larger, faster, smarter, and more expensive, and therefore POC is becoming less cost effective.

True

False

Which of the following is NOT an example of a wireless POC testing device?

Benchtop analyzer

Blood glucose meters and kit

Nerve conduction

Lipid test kit

References/Sources

1. Strickland, J. (2010). How Does the Internet work?. http://www.computer.howstuffworks.com/internet/basics/internet.htm.

2. Mayo Clinic and Santrach, P. J. Current & Future Applications of Point of Care Testing. http://wwwn.cdc.gov/cliac/pdf/Addenda/cliac0207/AddendumF.pdf.

3. CodeConcept and Machowska, I. (2008). Point–of–Care Overview. http://www.codeconcept.pl/doc/en/POCT%20Overview%20Presentation%20CodeConcept%20081117.ppt. PowerPoint presentation.

This product is funded by the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program (#TC-26440-14-60-A-21).

Continue with other activities/quizzes...

Flashcards

Media	In a network, media refers to the cabling and/or the ability to communicate wireless.

1 of 36

Standards	Enable products from different vendors to work together.

2 of 36

Protocols	Govern communications

3 of 36

Internet Protocol	Provides a global standard for communication on the Internet.

4 of 36

Interoperable	Means that a network meets all hardware, media, and protocol standards required to successfully exchange and make use of the transmitted information.

5 of 36

Frequency	Data communicated through a wired network is transmitted in the form of electrical waves.

6 of 36

NIC	Network Interface Card (NIC)

7 of 36

Protocol

A network protocol is a set of rules and conventions that ensure consistent communication between network devices.

8 of 36

IPv4

Original standard with limited number of IP addresses

IPv6

Latest standard with millions of IP addresses available

TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a technical standard that governs the transport of messages across the Internet for delivery to their destination.

HTTP

The Hypertext Transfer Protocol (HTTP) is a technical standard used on the World Wide Web that enables any Web browser to communicate with any Web server.

12 of 36

WiFi

The WiFi standard defines throughput and message frame formats for equipment and frequencies used for wireless communication.

13 of 36

WiFi Standards

The standards are IEEE 802.11 A 5.0 gigahertz; IEEE 802.11 B 2.4 gigahertz; IEEE 802.11 G

2.4 gigahertz; and IEEE 802.11 N 2.4 and 5.0 gigahertz.

WAP

The Wireless Application Protocol (WAP) defines a technical standard for smartphones, mobile phones, and PDAs.

RFID

The RFID standard relates to the circuitry that stores information on the tag and to the antenna that sends and receives signals.

16 of 36

Bluetooth

The Bluetooth standard addresses the open, wireless technology for exchanging data over short distances from fixed and mobile devices.

17 of 36

POC

Point of Care

18 of 36

IPv4

IP version 4 (IPv4) has been used for nearly 50 years and supports intranets.

19 of 36

IPv6

IP version 6 (IPv6) was created to augment IPv4 and supports the Internet.

20 of 36

Bandwidth

Bandwidth is the highest number of bits that can be sent

at any one time.

Throughput

Throughput is the amount of bandwidth that is available for actual network communications.

Router

A device that connects two networks together.

23 of 36

Modem

A device that makes it possible to transmit data to or from a computer or intranet network via telephone lines or ISP cable to a remote network location.

24 of 36

ISP

Internet service provider (ISP). The ISP provides the necessary hardware, including a cable that connects to the Internet and a modem/router device.

25 of 36

Intranet network

An intranet network provides private communication capabilities for an organization or company.

Network

A network is composed of connected computers, printers, and other devices, along with some sort of media.

Media

The term media, in a network context, refers to cabling and/or the ability to

communicate wirelessly.

RFID

Radio-frequency identification tags are microchips that store and transmit data needed for identification or tracking purposes.

LAN

Local Area Network (LAN). A LAN might serve a home, a physician office, a clinic on one fioor of a building, a small hospital with one building, or a hospital with two or three buildings.

30 of 36

Client/server model

A client/server model is a computing structure that separates tasks or workloads between service providers, called servers, and service requesters, called clients.

31 of 36

MAN

Metropolitan Area Network (MAN). If a network comprises several geographically separate locations in the same city, it is called a MAN.

32 of 36

WAN	Wide Area Network (WAN). A network that must service a large geographical area is called a WAN.

33 of 36

Topology	The organization or layout of a network

34 of 36

Physical Topology	The layout of the network hardware components and method used when messages are sent and

	received by those components

Logical	A diagram that illustrates the network data fiow without regard for the network's physical topology

Practice Quiz

Question

01/70

_____enable products from different vendors to work together

Standards

Protocols

Internet Protocol

Media

Question

02/70

_____govern communications.

Standards

Protocols

Interoperable

Media

Question

03/70

_____provides a global standard for communication on the Internet.

Internet Protocol

Standards

Media

Frequency

Question

04/70

In a network,_____refers to the cabling and/or the ability to communicate wireless.

Standards

Protocols

Media

Frequency

Question

05/70

A_____is a set of rules and conventions that ensure consistent communication between network devices.

---

network protocol

standard

media

frequency

Question

06/70

The network device sending messages is transmitting on 2.4 gigahertz, and the receiver is looking for messages on 5.0 gigahertz. The reason the communication will fail is that different_____are used by the sender and receiver.

---

hardware and media

network protocols

electronic or radiofrequencies

interoperability

Question

07/70

The network device is configured with a fiber-optic NIC. The network switch is configured to accept copper cabling. The reason the communication will fail is that different_____are used by the sender and receiver.

---

hardware and media

electronic or radio frequencies

network protocols

interoperability

Question

08/70

The network device formats the message with a packet of 25 characters in length. The receiving device expects the packet to be 30 characters in length. The reason the communication will fail is that different_____are used by the sender and receiver.

---

electronic or radio frequencies

hardware and media

network protocols

interoperabilty

Question

09/70

A network administrator chooses hardware and media that perform at required frequencies and with compatible network protocols to achieve successful _____.

---

electronic or radio frequencies

hardware and media

network protocols

interoperability

Question

10/70

Companies that manufacture network devices and media used in healthcare settings must follow industry_____in order to be certified as meeting HITECH requirements for network interoperability.

---

experts

guidelines

standards

protocols

Question

11/70

A network application uses an Internet Web browser to interact with an application housed on an Internet Web server. What is the required protocol?

HTTP

RFID

Bluetooth

TCP/IP

Question

12/70

If a network application transmits messages across the Internet, the message must meet_____protocol standards.

HTTP

RFID

Bluetooth

TCP/IP

Question

13/70

The ofice administrator for a small physician practice serves as the practice's network administrator. She is constantly on conference calls because the practice is upgrading to an EMR system. She would like to have a device that will leave her hands free during these phone calls. Her phone and the headset she purchases must meet _____ standards.

HTTP

WIMAX

Bluetooth

TCP/IP

Question

14/70

A small hospital asks each nurse and physician to wear a/an _____badge that transmits the clinician's name to a screen across from the patient's bed so the patient immediately knows who comes into the room.

HTTP

RFID

WAP

TCP/IP

Question

15/70

A wireless network device must meet the same industry standard used for mobile phones and smartphones. What is the standard?

HTTP

WAP

RFID

WIMAX

Question

16/70

A hospital is considering distributing wireless tablet PCs to each physician who practices at the hospital. The physicians have been pushing for some better solution than the computer on wheels (COWs) and fixed wired PCs at strategic locations throughout the hospital.

The network administrator has been asked to consider the ramifications of this decision. He explains he would need to set up a_____network and he worries about how the hospital will maintain its HIPAA standards.

---

wired

wireless

cloud

mobile

Question

17/70

A hospital is considering distributing wireless tablet PCs to each physician who practices at the hospital. The physicians have been pushing for some better solution than the computer on wheels (COWs) and fixed wired PCs at strategic locations throughout the hospital.

The network administrator's major and quite significant concern is that the wireless network will have serious_____issues, and he worries about how the hospital will maintain its HIPAA standards.

---

mobility

security

complexity

contextual

Question

18/70

A hospital is considering distributing wireless tablet PCs to each physician who practices at the hospital. The physicians have been pushing for some better solution than the computer on wheels (COWs) and fixed wired PCs at strategic locations throughout the hospital.

The major advantage of the wireless network, of course, will be the convenience and_____for the physicians within range of the network WAP switch.

---

mobility

security

complexity

contextual

Question

19/70

A hospital is considering distributing wireless tablet PCs to each physician who practices at the hospital. The physicians have been pushing for some better solution than the computer on wheels (COWs) and fixed wired PCs at strategic locations throughout the hospital.

The administrator is also concerned about the _____ associated with the network device setup. He explains that with all the electronic equipment used in a hospital setting, there is a fear that wireless devices might interfere with existing hard-wired, medically necessary technology.

---

wireless

security

mobility

complexity

Question

20/70

HIT point-of-care (POC) testing devices are getting larger, faster, smarter, and more expensive, and therefore POC is becoming less cost effective. True or False.

True

False

Question

21/70

As point-of-care (POC) testing devices proliferate, there are concerns with how to maintain patient safety and quality of care, particularly given the scientific nature of the process, analysis, and associated message content. True or False.

True

False

Question

22/70

Which of the following is NOT an example of a wireless POC testing device?

Benchtop analyzer

Blood glucose meters and kit

Nerve conduction study device

Inpatient bedside monitor for vital signs

Question

23/70

Which of the following is an example of a wired POC testing device?

Benchtop analyzer

Inpatient bedside monitor for vital signs

Nerve conductor study device

Lipid test kit

Question

24/70

If a network administrator chooses a peer-to-peer LAN intranet design, the network probably has_____shared devices.

---

10 or fewer

More than 10

Question

25/70

Which answer choice best describes the needs of users on a private intranet?

The ability to communicate with outside entities and resources

The ability to share internal computer resources

A computer with a high-speed CPU

A stand alone computer with security access.

Question

26/70

Each of the following is a characteristic of the server in a client/server LAN except:

a computer that stores shared files, databases, and software applications.

a computer with a special network operating system.

a computer on a user's desktop or a user's mobile devices.

a computer with a high-speed CPU, large amounts of memory, and high-capacity disk drives.

Question

27/70

A relatively large private network that consists of more than one LAN and supports a healthcare organization that has several geographically dispersed locations in the same community is called a_____.

WAN

MAN

WAP

LAN

Question

28/70

A peer-to-peer LAN network is usually controlled through a

server.

workgroup.

client.

desktop.

Question

29/70

A diagram that illustrates the network data flow without regard for the network's physical topology

---

Physical topology

Logical topology

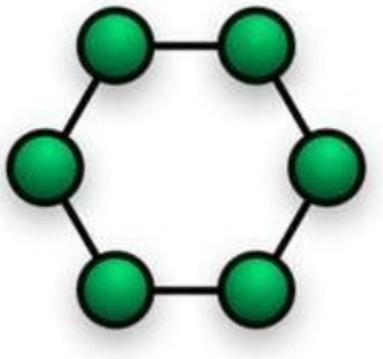
Bus topology

Mesh topology

Question

30/70

What kind of topology does this image represent?



Bus topology

Ring topology

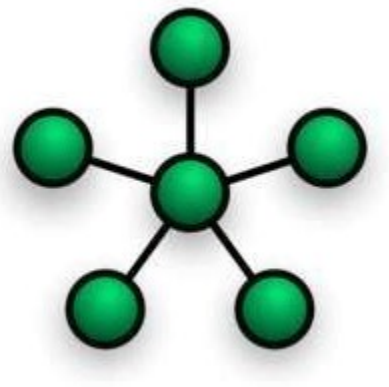
Mesh topology

Star topology

Question

31/70

What kind of topology does this image represent?



Bus topology

Ring topology

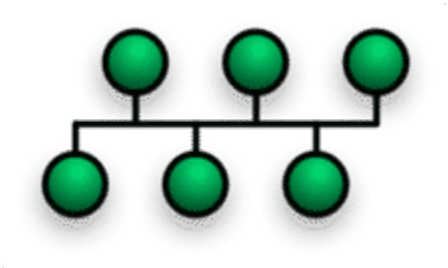
Mesh topology

Star topology

Question

32/70

What kind of topology does this image represent?



Bus topology

Ring topology

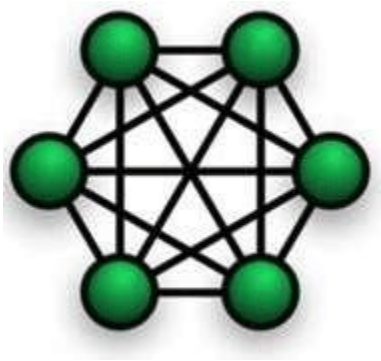
Mesh topology

Star topology

Question

33/70

What kind of topology does this image represent?



Bus topology

Ring topology

Mesh topology

Star topology

Question

34/70

When the network administrator determines how the network is organized, he or she has determined the network's_____.

---

physical layout

logical layout

computer map

topology

Question

35/70

Each shared computer is connected to every other computer by a single network cable. This is the least reliable topology.

Bus topology

Star topology

Ring topology

Logical topology

Question

36/70

All trafic passes through the switch at the hub of the network. This is the most common topology.

Bus topology

Star topology

Ring topology

Logical topology

Question

37/70

Each shared computer is connected to the network in a closed loop. This topology is used in very secured environments.

Bus topology

Star topology

Ring topology

Logical topology

Question

38/70

Data passes through the network from one device to the next without regard to the physical interconnection of the actual devices.

Bus topology

Star topology

Ring topology

Logical topology

Question

39/70

Uses telephone lines to connect to an ISP's modem/router. Speed—or bandwidth—is limited to 56 kilobits per second.

Dial-up

Broadband

Satellite

Wifi

Question

40/70

Uses coaxial or fiber-optic cable to connect to an ISP's modem/router.

Dial-up

Broadband

Satellite

Wifi

Question

41/70

Wireless Internet connection frequently found in hotels and public venues such as airports, libraries, college campuses, and coffee shops.

Dial-up

Broadband

Satellite

WiFi

Question

42/70

The loss of speed that results from the signal bouncing around is called _____.

---

frequency loss

latency

connectionless

service device shortness

Question

43/70

Using http://www.whitehouse.gov as an example, the www portion of the domain name indicates_____.

a name is associated with world wide web

is a purchased domain

indicates a government entitytype

indicates a non secure site

Question

44/70

Using http://www.whitehouse.gov as an example, the whitehouse portion of the domain name indicates_____.

---

is associated with the world wide web

is a purchased domain name

indicates a government site

indicates a non secure site

Question

45/70

Using http://www.whitehouse.gov as an example, the gov portion of the domain name indicates_____.

---

is associated with the world wide web

is a purchased domain name

indicates a government entitytype

indicates a non secure site

Question

46/70

The tool that resolves (translates) a domain name into a specific Internet IP address.

Internet Browser

File Browser

Domain Browser

Domain name

Question

47/70

How might a healthcare provider use the Internet?

sending emails to coworkers announcing policy changes

sharing computer resources

sending an order from a small physician office to an outside pharmacy or laboratory

sharing patient records with physicians on staff at a hospital

Question

48/70

If a healthcare organization owns an Internet domain,_____.

it has to pay a lot of money for it

it takes responsibility and control of the name within the internet-based domain name system (DNS)

it can use the name on its intranet

it must be renewed every month

Question

49/70

Where can a healthcare provider buy an Internet domain name?

From ICANN

From an ISP

From the healthcare provider's network administrator

From the local DMV

Question

50/70

A_____is composed of connected computers, printers, and other devices, along with somesort of media.

---

media

server

network

desktop

Question

51/70

Which of these items was NOT included in the definition of network?

media

software

computers

computer devices

Question

52/70

_____is/are cabling and/or the means for wireless communication.

Media

Software

Computers

Computer devices

Question

53/70

Certain expectations come with the installation and use of a computer network. Which of these is NOT a valid expectation?

Customer services may suffer.

Better communications result from the use of email.

Computer resources can be shared.

Software can be installed more efficiently.

Question

54/70

Choose the item that demonstrates an improvement in healthcare that results from a network installation.

Barcodes on hospital medication bottles can be scanned and compared to the scanned barcode on a patient's wristband to ensure the right patient received the right medication.

If a doctor updates a patient's EMR at the hospital bedside, the update is immediately available to all provider's anywhere in a hospital.

E-prescriptions are available at a faster rate.

Workflow efficiency is increased at a dramatic rate.

Question

55/70

Since Adam Hospital installed a network, it has saved money by purchasing fewer printers because multiple users now have access to_____.

---

improved communications

shared devices

shared files

shared office locations

Question

56/70

The hospital now has email and can broadcast policy changes immediately. This capability has resulted in_____.

---

improved communications

shared devices

shared files

shared locations

Question

57/70

The quality of care has also improved because each time a patient's record is updated in the EMR system, the update is available to all healthcare providers through the use of_____.

---

improved communications

shared communications

shared files

shared locations

Question

58/70

_____provides private communication capabilities for an organization or company.

Intranet network

Internet network

Physical network

Logical network

Question

59/70

A device that connects two networks together.

Router

Modem

Meter

RFID

Question

60/70

A device that makes it possible to transmit data to or from a computer or intranet network via telephone lines or ISP cable to a remote network location.

Router

Modem

Meter

RFID

Question

61/70

A wired intranet network connection must have each of the following except _____.

media cabling

a WAP

a switch

a connector

Question

62/70

_____is the highest number of bits that can be sent at any one time.

Bandwidth

Throughput

Communication overhead

Frequency

Question

63/70

_____is the amount of bandwidth that is available for actual network communications.

Bandwidth

Throughput

Communication overhead

Frequency

Question

64/70

_____ are factors that can reduce network speed.

Bandwidth

Throughput

Communication overhead

Frequency

Question

65/70

Which of these intranet media currently provides the lowest network speed?

Cooper cable

Fiber optic cable

Wireless

Fabric cable

Question

66/70

A_____IP address is assigned to each shared device onan intranet.

Private

Public

Internal

External

Question

67/70

A_____IP address is assigned to each shared device on the Internet.

Private

Public

Internal

External

Question

68/70

The same IP address might be used on many different _____ networks.

Private

Public

Internal

External

Question

69/70

IP Version 4 support a_____network.

Intranet

Internal

External

Internet

Question

70/70

IP Version 6 support a_____network.

Intranet

Internet

Internal

External