Mahidol University
Faculty of Medicine Ramathibodi Hospital
Department of Clinical Epidemiology and Biostatistics

https://paginas.fe.up.pt/~acbrito/laudon/ch6/chpt6-1fulltext.htm

IT Infrastructure

RADI601 Health informatics and health information technology / RADI607 Theories in Health Informatics and Health Information Technology

Lect. Anuchate Pattanateepapon, D.Eng.

Section of Data Science for Healthcare

Department of Clinical Epidemiology and Biostatistics

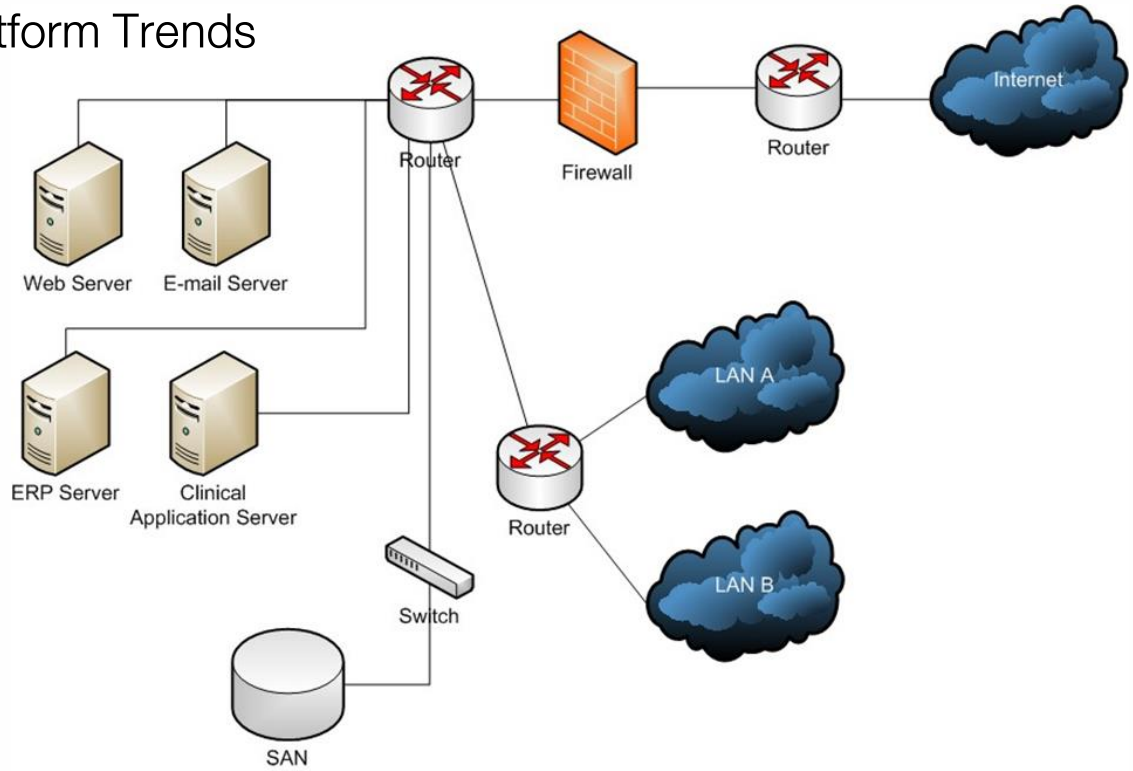
Faculty of Medicine Ramathibodi Hospital, Mahidol University

Wisdom of the Land

Reference: https://paginas.fe.up.pt/~acbrito/laudon/ch6/chpt6-1fulltext.htm

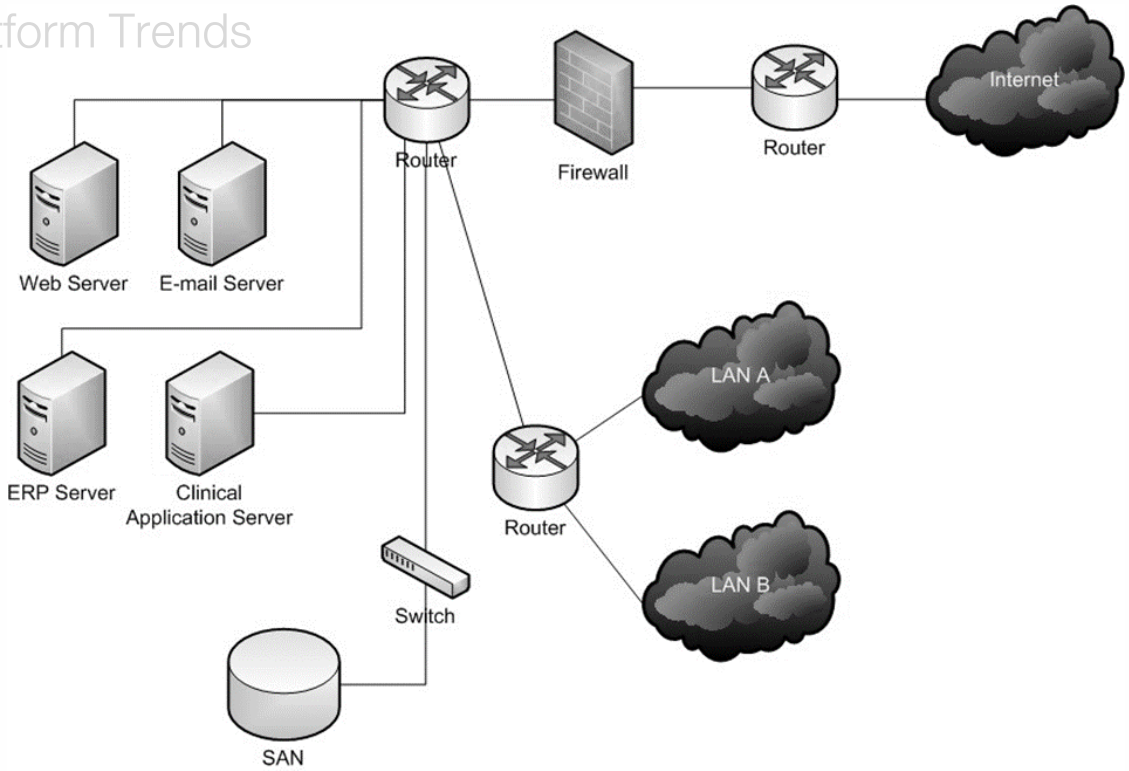
Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Hardware Platform Trends
- Security Management
- Example of Hospital IT infra.



Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Hardware Platform Trends
- Security Management
- Example of Hospital IT infra.



A traditional IT infrastructure is made up of the usual hardware and software components: facilities, data centers, servers, networking hardware desktop computers and enterprise application software solutions.

IT Infrastructure

- **Defining IT infrastructure:** IT infrastructure refers to the combined components needed for the operation and management of enterprise IT services and IT environments.

  to operate an enterprise

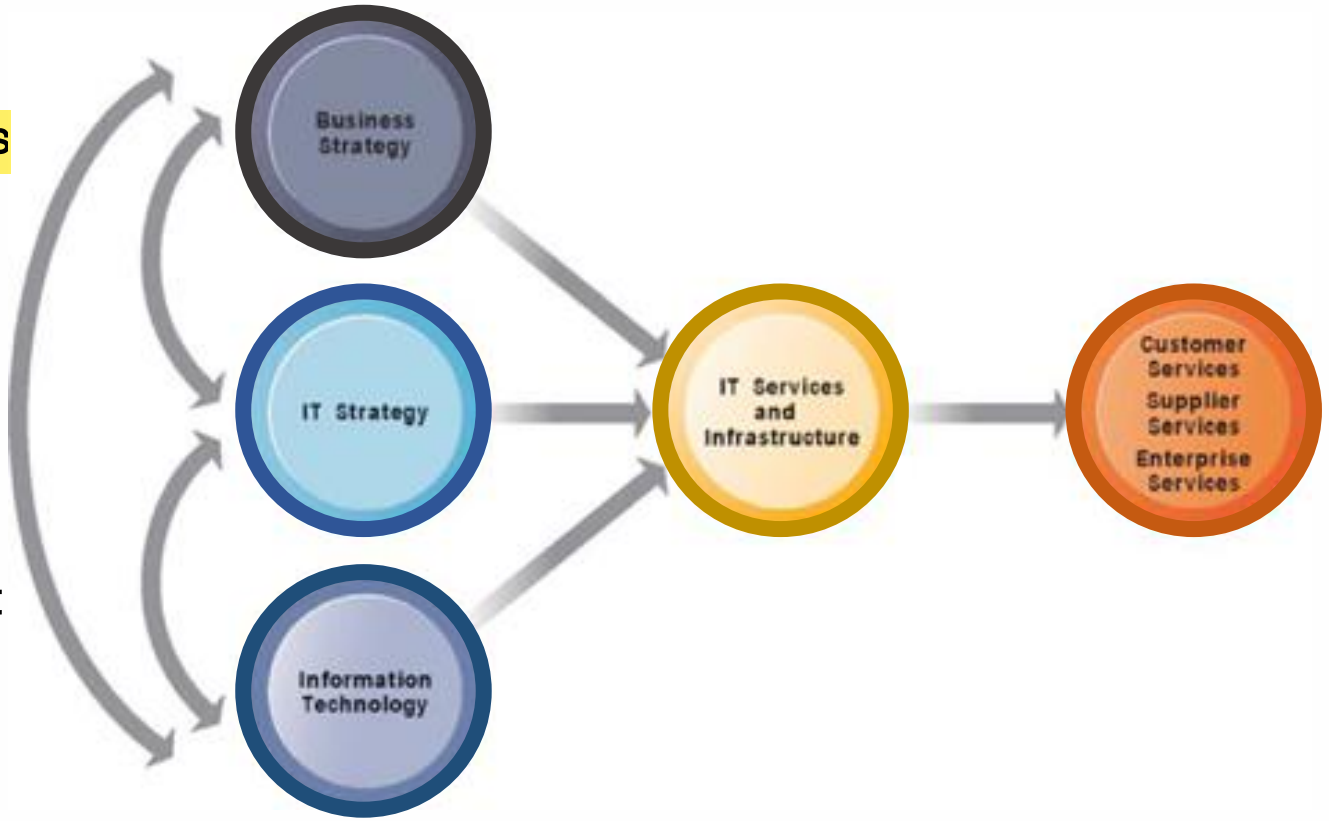
  - Set of physical devices and software required to operate enterprise
  - Set of firmwide services including:
    - Computing platforms providing computing services
    - Telecommunications services
    - Data management services
    - Application software services
    - Physical facilities management services
    - IT management, standards, education, research and development services
  - "Service platform" perspective more accurate view of value of investments

New PC increases its value to the firm to meet the enterprise's objectives

IT Infrastructure

Connection Between the Firm, IT Infrastructure, and Business Capabilities

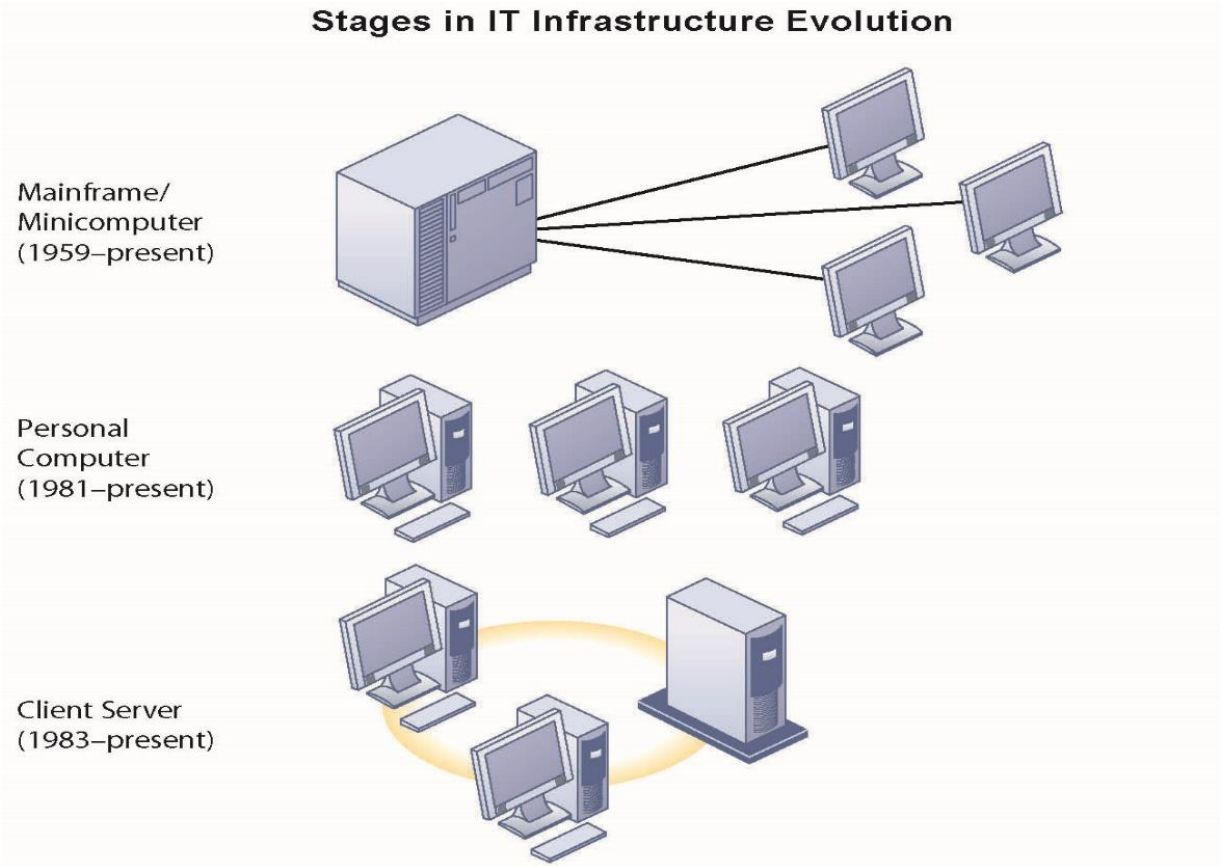
Infrastructure should support the firm's business and information systems strategy. New information technologies have a powerful impact on business and IT strategies, as well as the services that can be provided to customers.



IT Infrastructure

- Evolution of IT infrastructure
  - General-purpose mainframe and minicomputer era: 1959 to present
    - 1958 IBM first mainframes: support thousands of online remote terminals
    - 1965 less expensive DEC minicomputers: allowing decentralized computing
  - Personal computer era: 1981 to present
    - 1981 Introduction of IBM PC These PCs were stand-alone systems until PC operating system software in the 1990s made it possible to link them into networks.
    - Proliferation in 80s, 90s resulted in growth of personal software
  - Client/server era: 1983 to present
    - Desktop clients networked to servers, with processing work split between clients and servers Desktop/laptop computers called clients are networked to powerful server computers that provide the client computers with a variety of services and capabilities.
    - Network may be two-tiered or multi-tiered (N-tiered)
    - Various types of servers (network, application, Web)

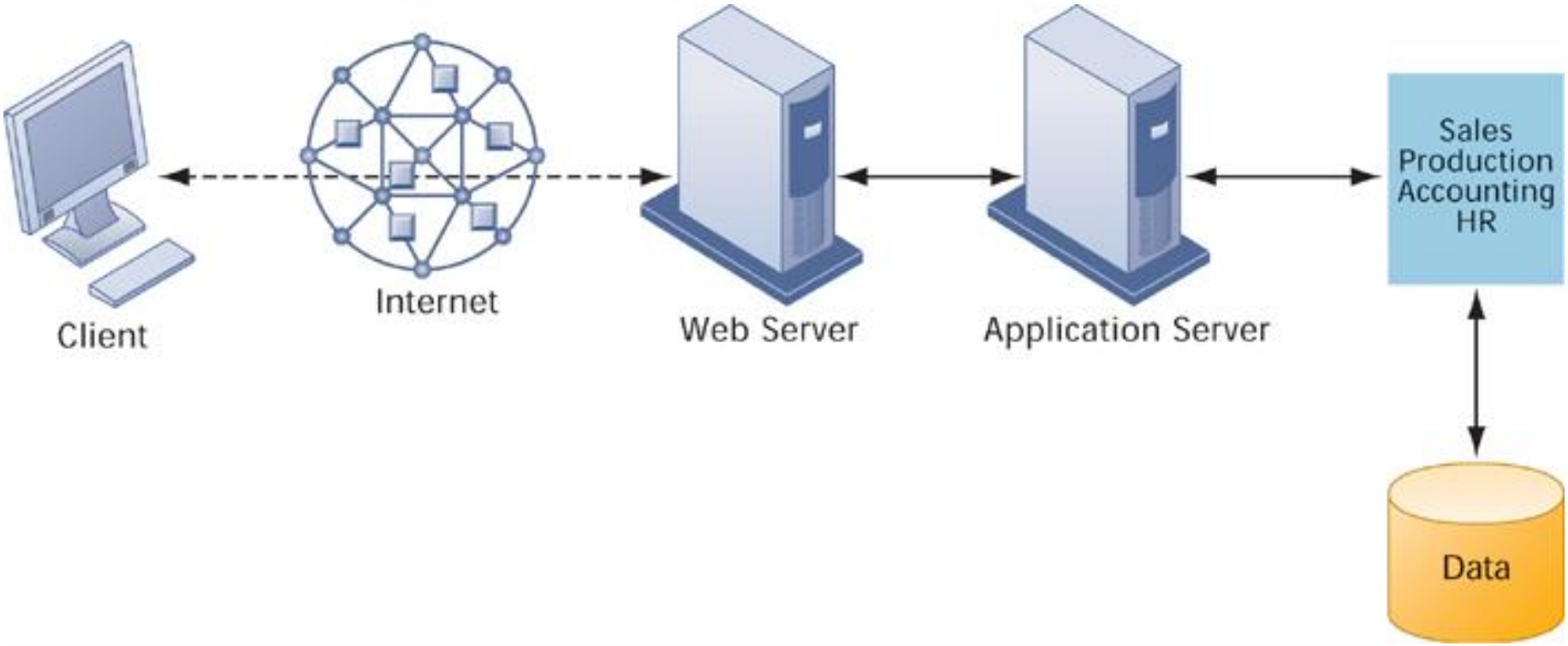
IT Infrastructure



Illustrated here are the typical computing configurations characterizing each of the five eras of IT infrastructure evolution.

IT Infrastructure

A Multitiered Client/Server Network (N-Tier)



In a multi-tiered client/server network, client requests for service are handled by different levels of servers.

IT Infrastructure

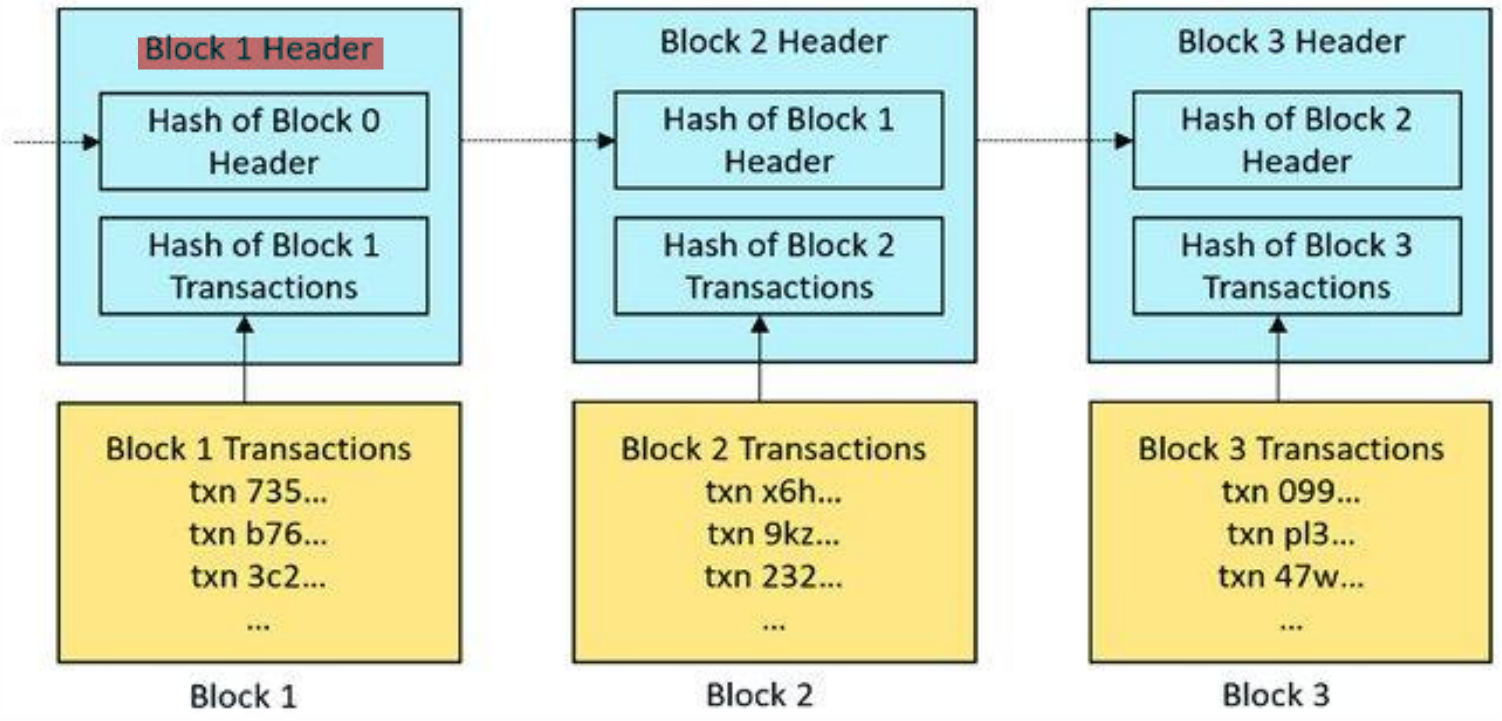
- Evolution of IT infrastructure (cont.)
  - Enterprise Internet computing era: 1992 to present
    - Move toward integrating disparate networks, applications using Internet standards and enterprise applications
  - Cloud Computing: 2000 to present Cloud computing (Google Collaborator)
    - Refers to a model of computing where firms and individuals obtain computing power and software applications over the Internet
    - Fastest growing form of computing

IT Infrastructure

The use of digital signatures based on blockchain data, which allows access only with the permission of several people and full compliance with keys, will allow to regulate the availability and maintain the confidentiality of medical records.

- Evolution of IT infrastructure (cont.)
  - Blockchain: 2008 to present
    - In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB.
    - a growing list of records, called blocks, that are linked using cryptography.
    - Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

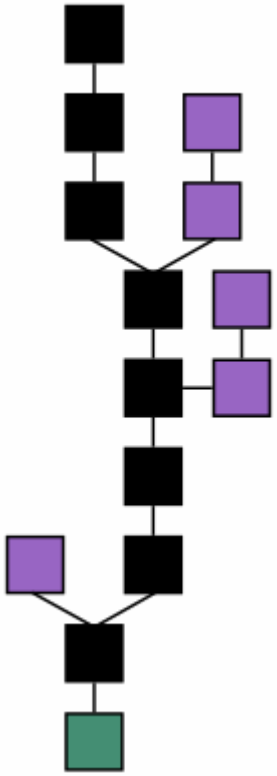
IT Infrastructure



https://www.researchgate.net/publication/332215097_Blockchain_Technology_in_Healthcare_A_Systematic_Review/figures?lo=1

IT Infrastructure

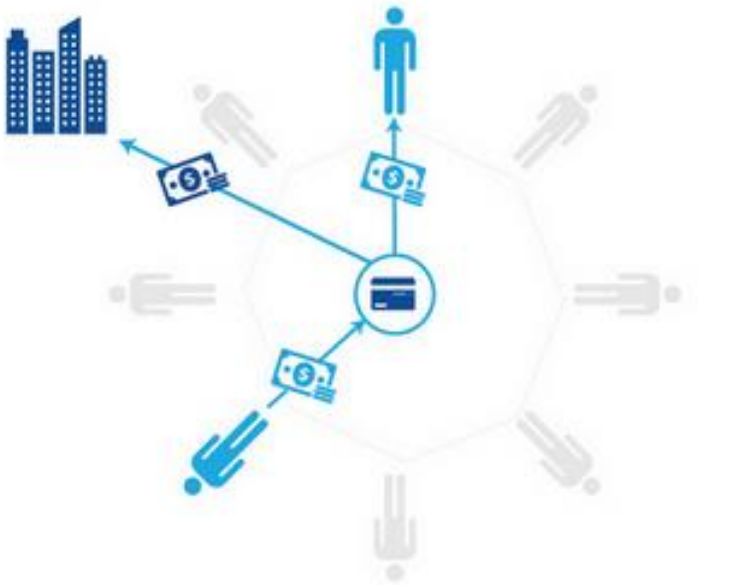
blockchain



Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

IT Infrastructure

blockchain



Current payment systems require third-party intermediaries that often charge high processing fees ...

... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

A blockchain infrastructure platform-as-a-service (PaaS) provider coordinates and maintains access to those amenities while also developing the code to build on them, the platform to access them, development tools, metrics and analytics, container services, and community support.

https://techsauce.co/tech-and-biz/understand-blockchain-in-5-minutes

IT Infrastructure

- Technology drivers of infrastructure evolution
  - Standards and network effects
    - Technology standards:
      - Specifications that establish the compatibility of products and the ability to communicate in a network
      - Unleash powerful economies of scale and result in price declines as manufacturers focus on the products built to a single standard

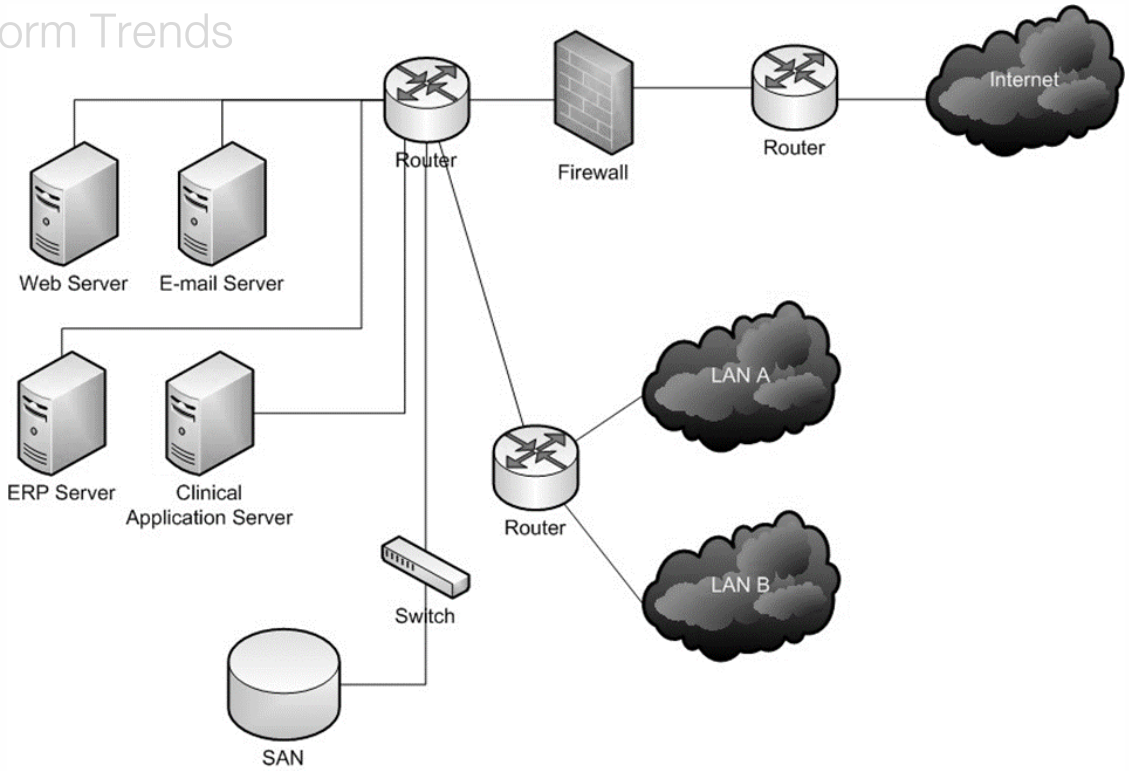
we have to communicate with other servers from other companies to drive infrastructure evolution

IT Infrastructure

What might today's enterprise infrastructure and Internet have been like without widespread and universal standards, such as Windows, Microsoft Office, Unix, and Ethernet?

Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Software Platform Trends
- Security Management
- Example of Hospital IT infra.



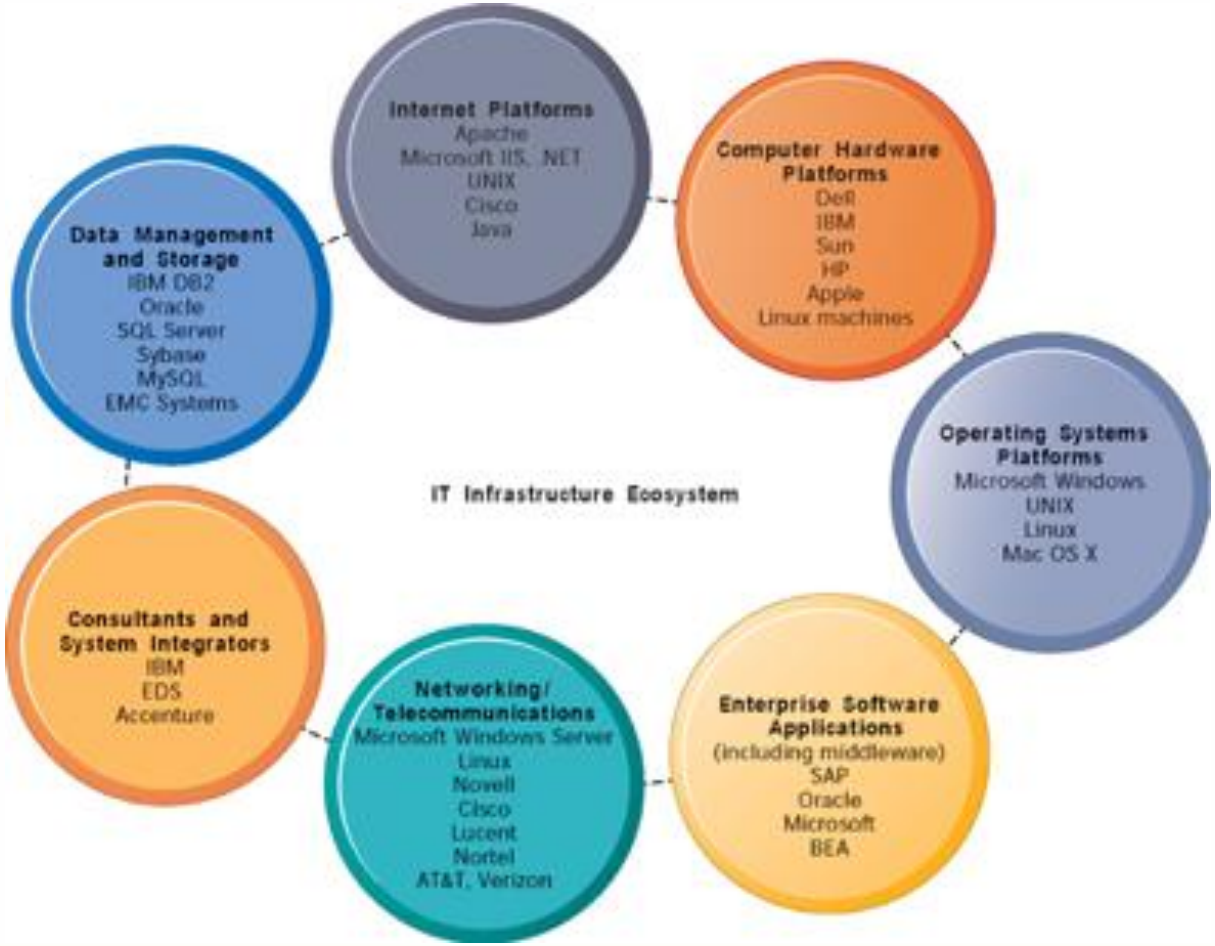
Infrastructure Components

IT Infrastructure has 7 main components

1. Computer hardware platforms
2. Operating system platforms
3. Enterprise software applications
4. Data management and storage
5. Networking/telecommunications platforms
6. Internet platforms
7. Consulting system integration services

Infrastructure Components

There are seven major components that must be coordinated to provide the firm with a coherent IT infrastructure. Listed here are major technologies and suppliers for each component.



Infrastructure Components

1. Computer hardware platforms
   - Client machines client: desktop PCs, mobile devices
     - Desktop PCs, mobile computing devices – PDAs, laptops
   - Servers
     - Blade servers: ultrathin computers stored in racks
   - Mainframes:
     - IBM mainframe equivalent to thousands of blade servers
   - Top chip producers: AMD, Intel, IBM
   - Top firms: IBM, HP, Dell, Sun Microsystems

Infrastructure Components: 1. Computer hardware

Types of Computers

- Computers come in different sizes with varying capabilities for processing information. a measure of computer performance, useful in fields of scientific computations that require floating-point calculations.
  - FLOPS (Floating point operations per second)
- Smartphones, netbooks, e-book readers
  - Today's smartphones are far more powerful than the early PCs of the 1980s
- PCs
- Workstations can run simulations 24/7 without interruptions and can manage the heat of the hardware
  - More powerful mathematical and graphics-processing capabilities than a PC
  - Used primarily for advanced design or engineering work requiring powerful graphics or computational capabilities.

Infrastructure Components: 1. Computer hardware

Types of Computers

- **Servers:**
  - Type of midrange computer.
  - Support computer network, sharing files and resources.
  - Provide hardware platform for e-commerce.
- **Mainframes:** a computer used primarily by large organizations for critical applications like bulk data processing for tasks such as censuses, industry and consumer statistics, enterprise resource planning, and large-scale transaction processing
  - Large-capacity, high-performance computer that can process large amounts of data very rapidly
  - E.g., used by airlines for thousands of reservations per second
  - Mainframes are still a major revenue and profit source for IBM. They are used often as huge Web servers where they are more efficient than tens of thousands of PCs in processing large volumes of records

Infrastructure Components: 1. Computer hardware

Types of Computers

Supercomputers are used for large and complex mathematical computations. While Mainframe computers are used as a storage for large databases and serve as a maximum number of users simultaneously.

- Supercomputer:
  - More sophisticated computer used for tasks requiring extremely rapid and complex calculations with thousands of variables, millions of measurements
  - Used in engineering, scientific simulations, military/weapons research, weather forecasting

- Grid computing:
  - Power of geographically remote computers connected into single network to act as “virtual supercomputer”

Infrastructure Components: 1. Computer hardware

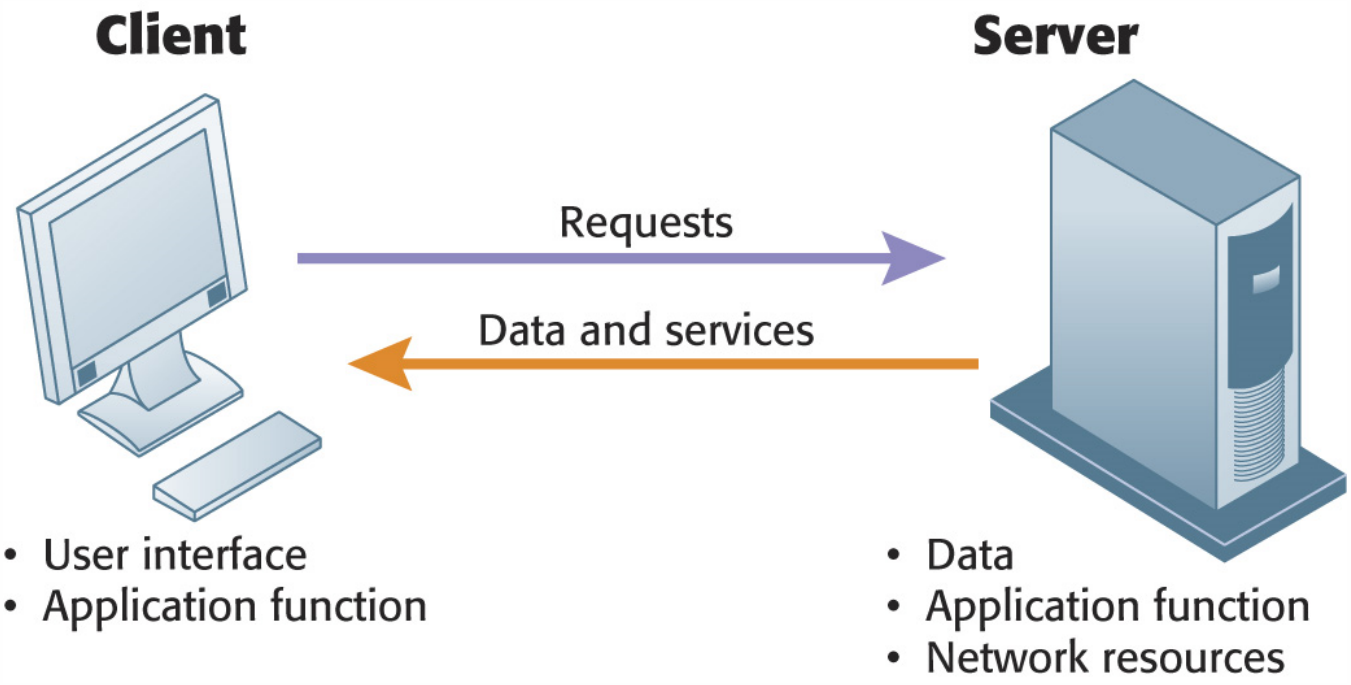
Types of Computers

- **Client/server computing:**
  - Form of distributed computing
  - Splits processing between "clients" and "servers"
  - **Clients:** user point of entry
    - The user generally interacts directly only with the client portion of the application, often to input data or retrieve data for further analysis.
  - **Servers:** store and process shared data and perform network management activities

Infrastructure Components: 1. Computer hardware

Client/Server Computing

In client/server computing, computer processing is split between client machines and server machines linked by a network. Users interface with the client machines.



Infrastructure Components: 1. Computer hardware

Storage, Input, and Output Technology

- Primary secondary storage technologies
  - Magnetic disk:
    - Hard drives, USB flash drives Redundant Array of Independent Disks
    - RAID: can package hundreds of drives for massive storage requirements
  - Optical disks
    - CD-ROM, CD-RW, DVD
  - Magnetic tape
  - Storage networking: SANs
    - Connect multiple storage devices on a separate high-speed network dedicated to storage

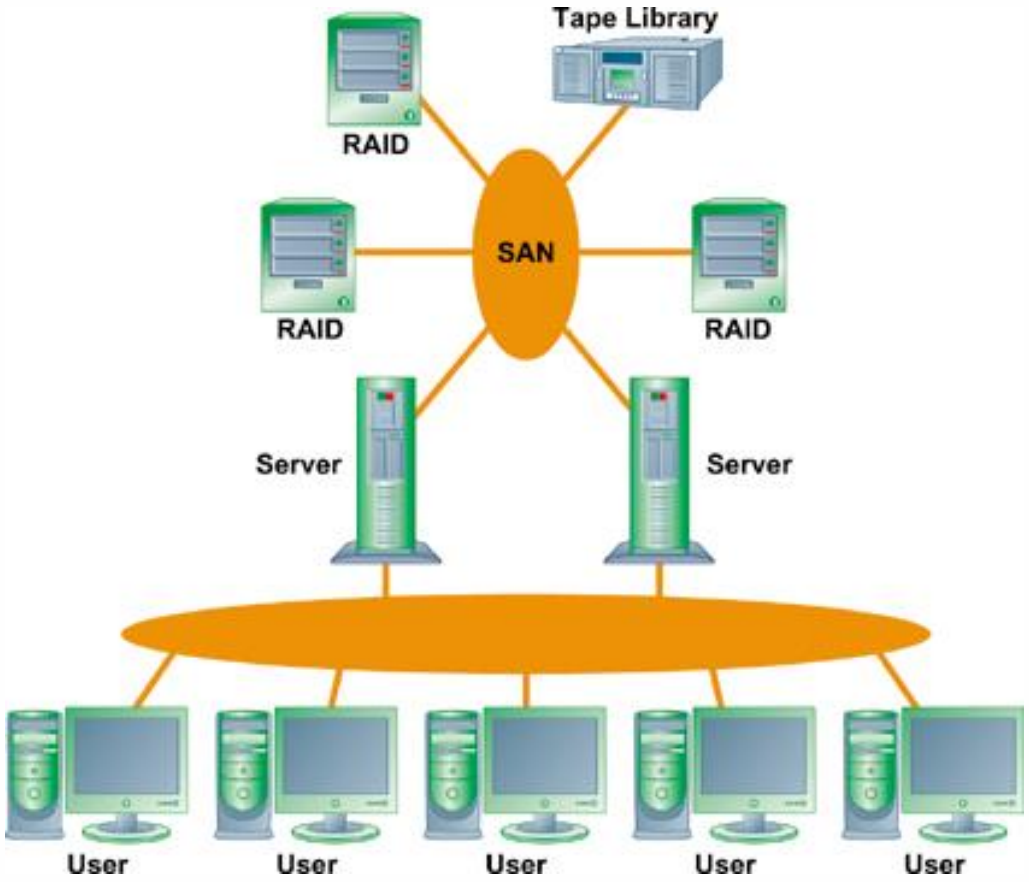
A CD-RW can be written to but a CD ROM can only be read from. A CD-ROM holds more information than a CD-RW.

Infrastructure Components: 1. Computer hardware

A Storage Area Network (SAN)

A typical SAN consists of a server, storage devices, and networking devices, and is used strictly for storage. The SAN stores data on many different types of storage devices, providing data to the enterprise. The SAN supports communication between any server and the storage unit as well as between different storage devices in the network.

Extraordinary efforts are taken to make redundant copies of digital information, and placing it on separate secure servers, even remote servers in separate facilities.



Infrastructure Components: 1. Computer hardware

Storage, Input, and Output Technology

- **Input devices:**
  - Gather data and convert them into electronic form.
    - Keyboard
    - Computer mouse
    - Touch screen
    - Optical character recognition
    - Magnetic ink character recognition
    - Pen-based input
    - Digital scanner
    - Audio input
    - Sensors

Infrastructure Components: 1. Computer hardware

Storage, Input, and Output Technology

- **Output devices:**
  - Display data after they have been processed.
    - Monitor
    - Printer
    - Audio output
- **Information systems collect and process information in one of two ways.**
  - **Batch processing:** transactions stored for predefined amount of time, then processed as group
  - **Online processing:** transactions processed immediately

Infrastructure Components: 1. Computer hardware

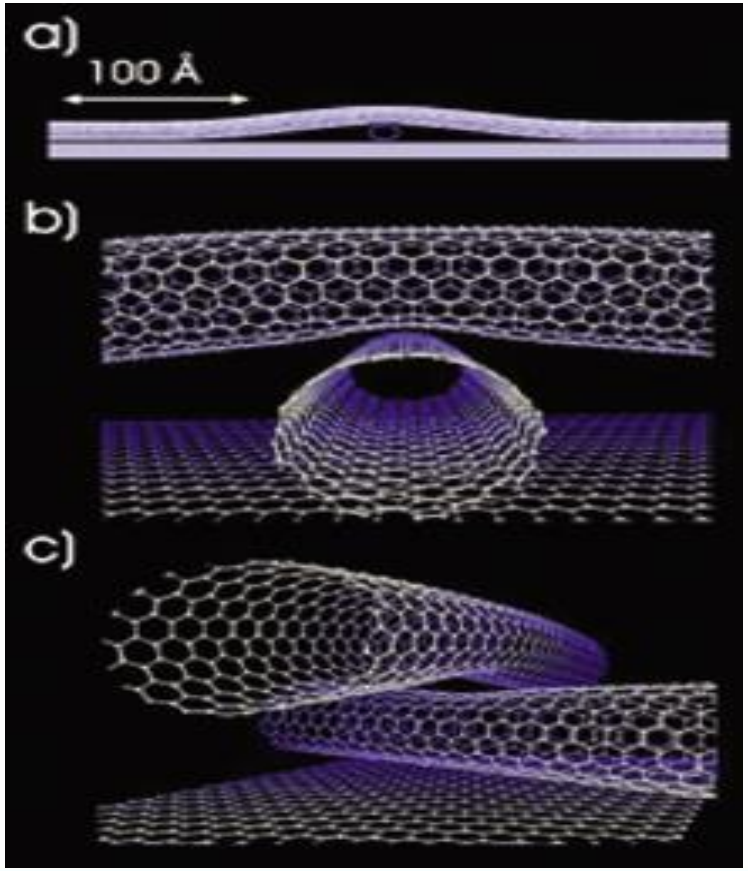
Contemporary Hardware Trends

- The emerging mobile digital platform
  - Based on new handheld hardware like cell phones, netbooks, and tablet computers. A new "platform."
  - Wireless communications through 3G cell networks and Wi-Fi.
  - New software apps.
- Nanotechnology:
  - Uses individual atoms and molecules to create computer chips and other devices that are thousands of times smaller than current technologies permit.
  - Nanotechnology shrinks the size of transistors down to the width of several atoms.

Infrastructure Components: 1. Computer hardware

Examples of Nanotubes

Nanotubes are tiny tubes about 10,000 times thinner than a human hair. They consist of rolled up sheets of carbon hexagons, have potential uses as minuscule wires or in ultrasmall electronic devices, and are very powerful conductors of electrical current.



Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

- Cloud Computing: Google Collaborator, Dropbox (SaaS), Amazon Web Services (IaaS), Microsoft Azure (IaaS)
  - A model of computing in which firms and individuals obtain computing resources over the Internet
    - Cloud infrastructure as a service
      - customers use processing, storage, networking, and other computing resources from cloud service providers to run their information systems.
    - Cloud platform as a service
      - customers use infrastructure and programming tools hosted by the service provider to develop their own applications.
    - Cloud software as a service
      - customers use software hosted by the vendor.

Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

Cloud Advantages

- Eliminates need for large up-front capital investments in systems
- Eliminates lengthy implementations on corporate computers
- Low cost subscriptions; no expensive licensing and maintenance fees
- No hardware for subscribers to purchase, scale, and maintain
- No operating systems, database servers or applications servers to install
- No consultants and staff
- Accessible via standard Web browser with behind-the-scene software updates
- Better scalability, eliminate cost and complexity of managing multiple layers of hardware and software

Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

Cloud Disadvantages data leakage and privacy concerns

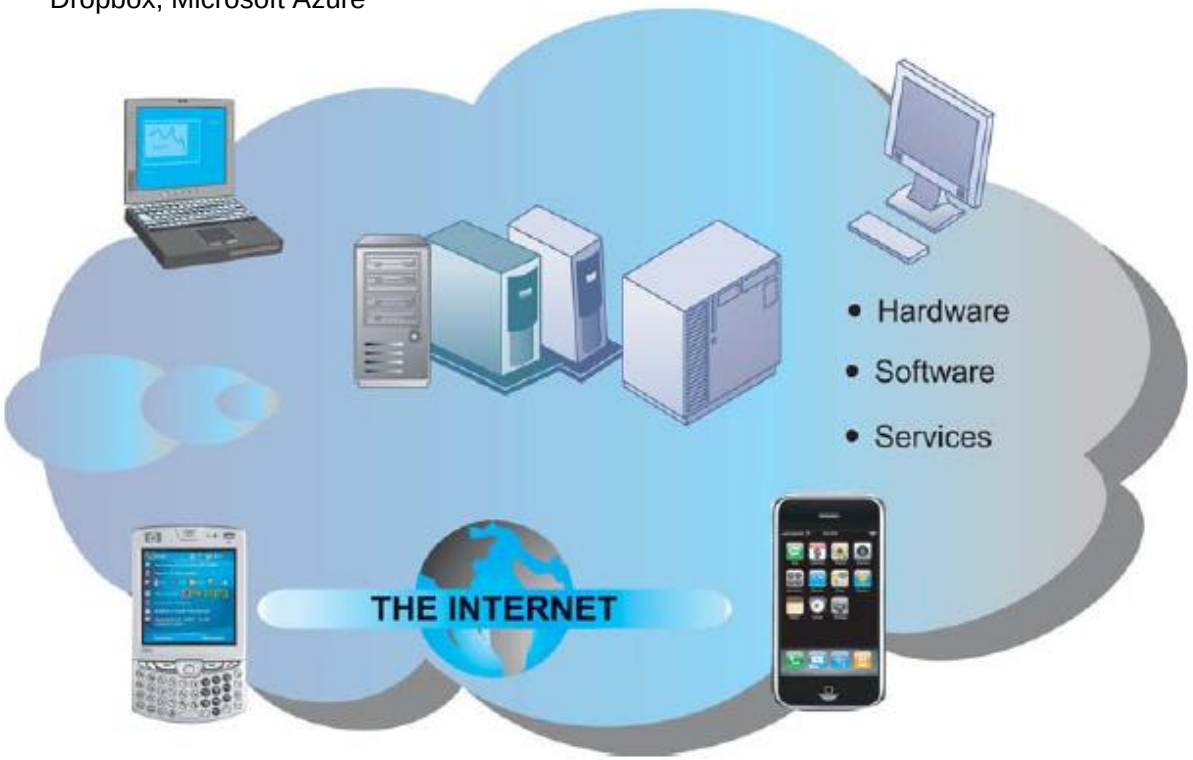
- May not be attractive to larger companies for their application needs
- Responsibility of data storage and control is in the hands of the provider
- Security risks may increase and open vulnerabilities to data maintenance
- System reliability issues
- Users dependency on the cloud computing provider

DoS attacks meant to shut down a machine or network

Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

Dropbox, Microsoft Azure



Cloud Computing Platform

In cloud computing, hardware and software capabilities are provided as services over the Internet. Businesses and employees have access to applications and IT infrastructure anywhere at any time using an Internet-connected device.

Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

- **Virtualization:**
  - Process of presenting a set of computing resources so they can be accessed in ways that are unrestricted by physical configuration or geographic location
  - IBM's mainframes run tens of thousands of separate instances of Windows or Linux on a single large mainframe computer, giving users the impression they have their own dedicated computer
  - **Server virtualization:** running more than one operating system at the same time on single machine.
  - Virtual memory is memory which fools the processor into thinking it is hardware memory but in fact is memory located on a hard drive.

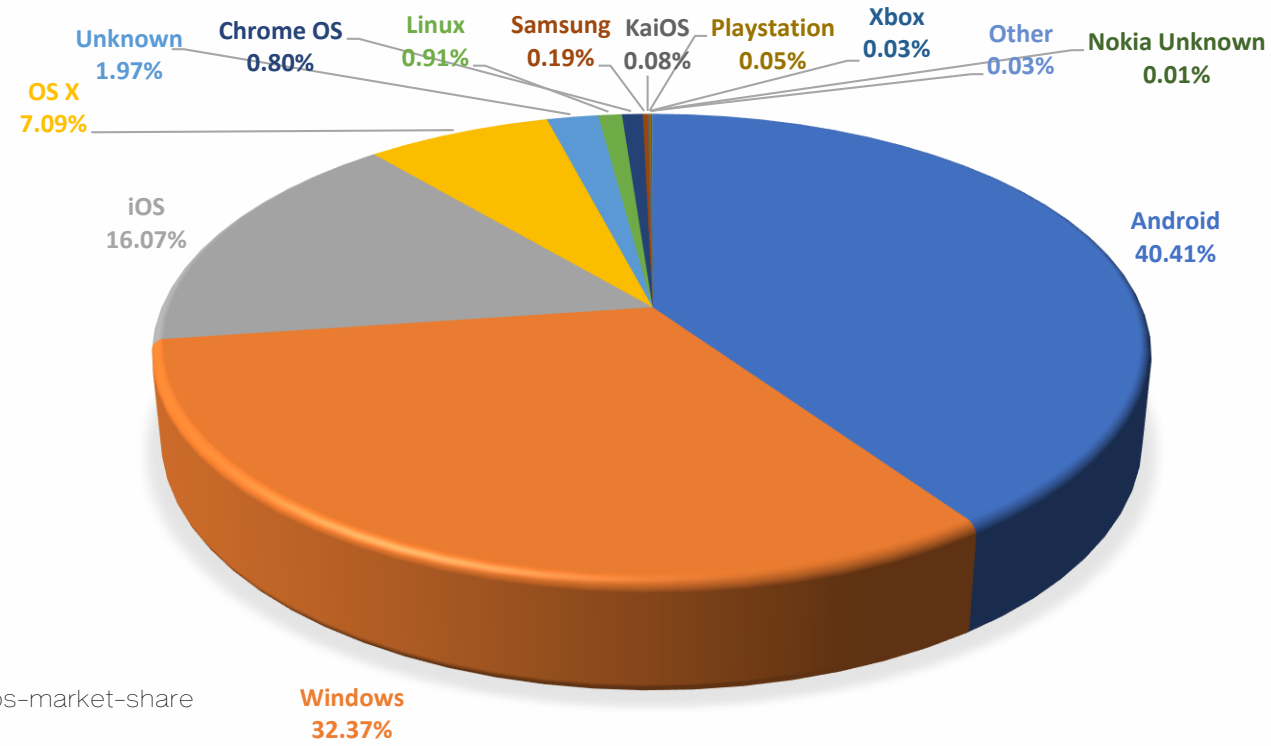
Infrastructure Components: 1. Computer hardware

Contemporary Hardware Trends

- **Multicore processors:**
  - Integrated circuit with two or more processors
  - Enhanced performance, reduced power consumption, and more efficient simultaneous processing of multiple tasks

Infrastructure Components: 2. Operating system platforms

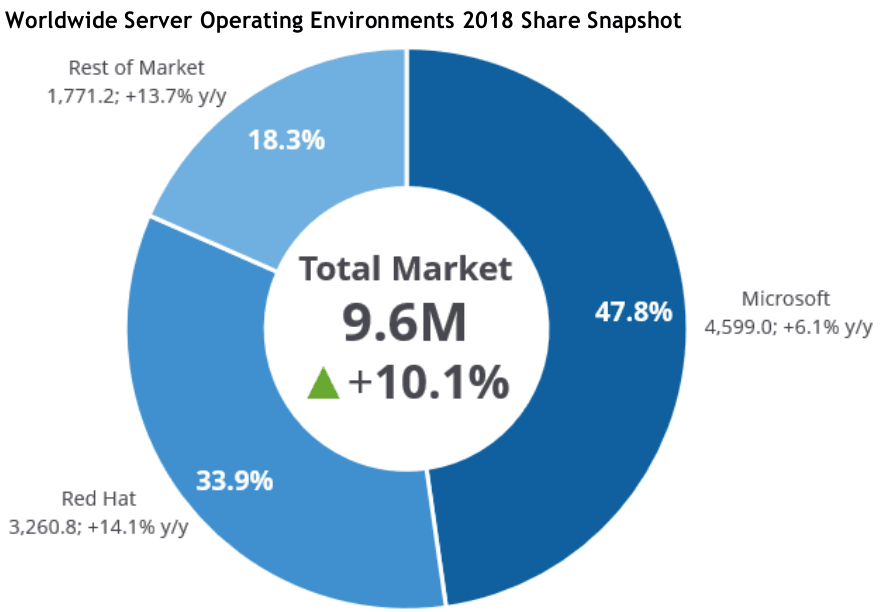
- Operating system platforms
  - Client Operating systems (Sep 2020 – Sep 2021)



https://gs.statcounter.com/os-market-share

Infrastructure Components: 2. Operating system platforms

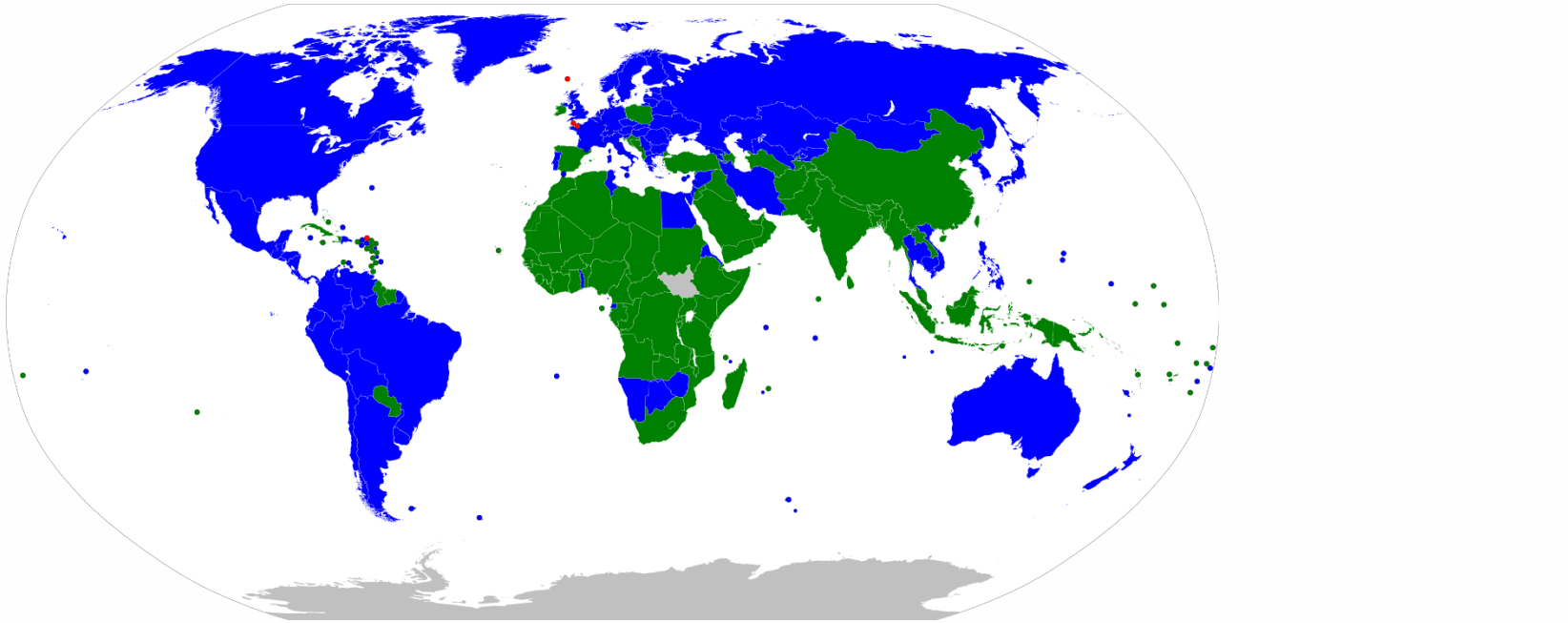
- Operating system platforms
  - Server Operating systems (2018)



https://gs.statcounter.com/os-market-share

Infrastructure Components: 2. Operating system platforms

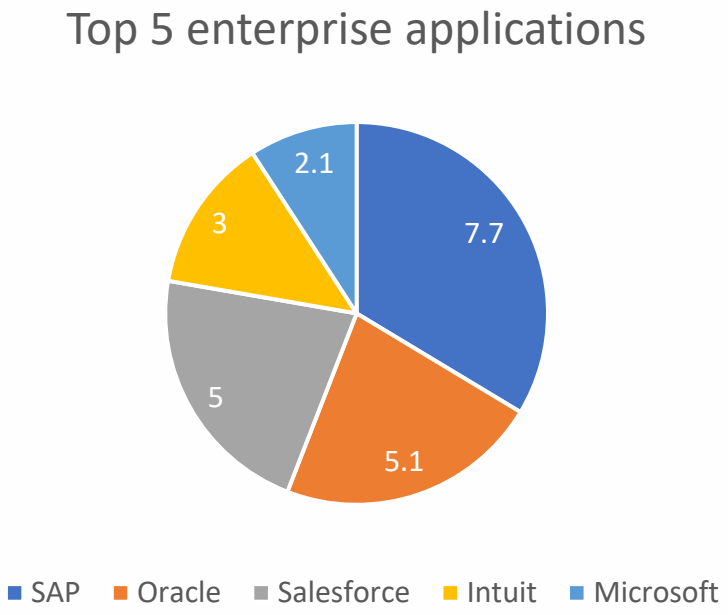
- Operating system platforms
  - Operating systems (2019-2020)



By Windfarmer1799 – Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=83045903

Infrastructure Components: 3. software applications

- Enterprise software applications
  - Enterprise software applications (2019)



https://www.idc.com/getdoc.jsp?containerId=prUS46724220

Infrastructure Components: 3. software applications

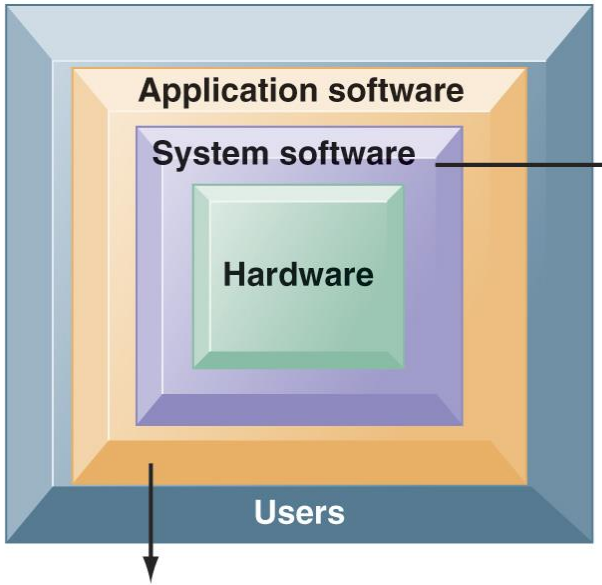
Operating System Software

- The software that manages and controls the computer's activities
- PC operating systems and graphical user interfaces
  - GUIs
  - Windows Server
  - UNIX
  - Linux
    - Open-source software

Infrastructure Components: 3. software applications

The Major Types of Software

The relationship among the system software, application software, and users can be illustrated by a series of nested boxes. System software—consisting of operating systems, language translators, and utility programs—controls access to the hardware. Application software, including programming languages and "fourth-generation" languages, must work through the system software to operate. The user interacts primarily with the application software.



SYSTEM SOFTWARE

Operating system

Language translators

Utility programs

APPLICATION SOFTWARE

Programming languages
Fourth-generation languages
Software packages and desktop productivity tools

Infrastructure Components: 3. software applications

Software for the Web: Java, AJAX, and HTML

- Java:
  - Operating system–independent, processor-independent, object-oriented programming language
- AJAX:
  - Allows a client and server to exchange data behind the scenes to avoid reloading a Web page after each change
- Hypertext markup language (HTML):
  - Page description language for specifying how elements are placed on a Web page and for creating links to other pages and objects

Infrastructure Components: 3. software applications

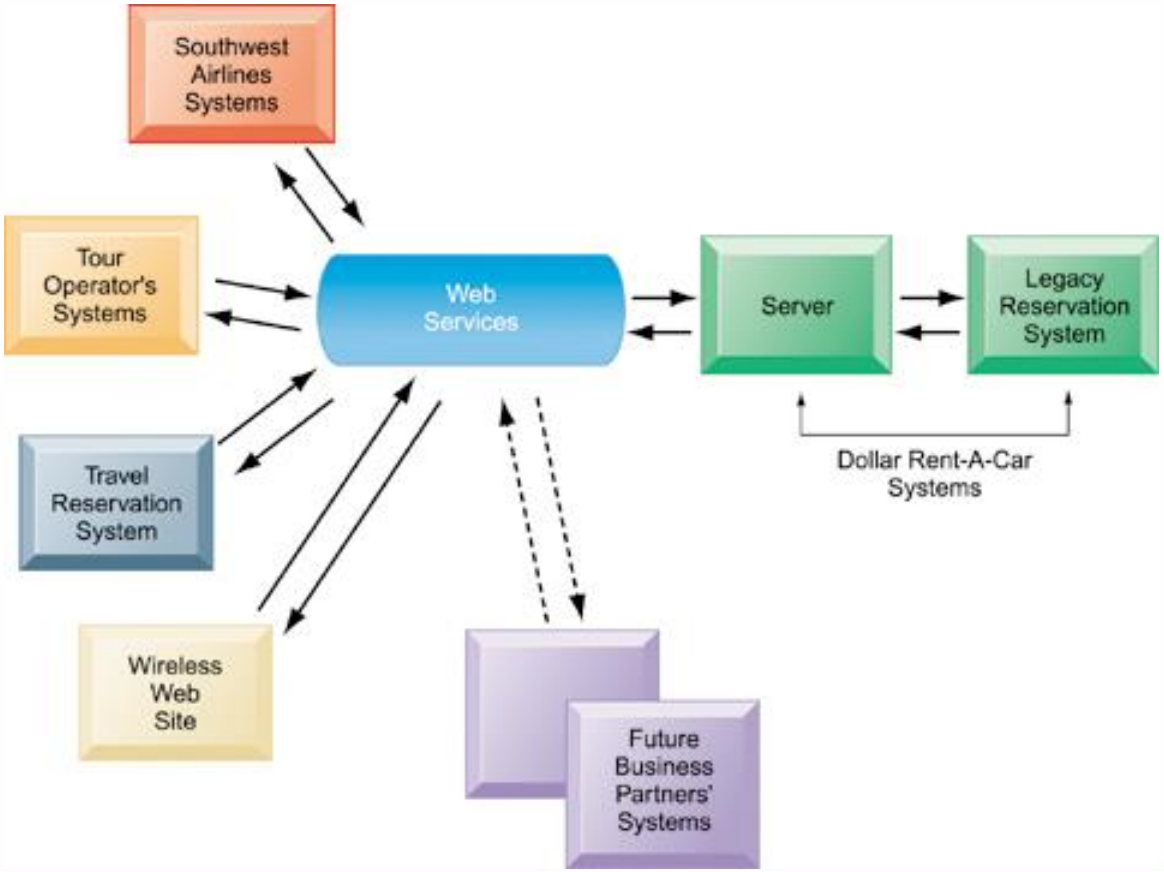
Web 2.0

- **Web services:**
  - Software components that exchange information with one another using universal Web communication standards and languages
  - It's a "messaging system" which allows diverse computing applications in a firm to communicate data with one another without integration of the constituent apps.
  - **XML (extensible markup language)**
    - **SOAP** (simple object access protocol)
    - **WSDL** (Web services description language)
    - **UDDI** (universal description, discovery, and integration)
  - **Service oriented architecture (SOA)**
    - In a service-oriented architecture, various applications provide "services" (data) on request to other applications needing data (large scale enterprise systems)

Infrastructure Components: 3. software applications

How Dollar Rent-A-Car Uses Web Services

Dollar Rent-A-Car uses Web services to provide a standard intermediate layer of software to "talk" to other companies' information systems. Dollar Rent-A-Car can use this set of Web services to link to other companies' information systems without having to build a separate link to each firm's systems.



Web server + Application: connected, the web server is connected to the database

Authentication server, no need to regenerate the connection

Infrastructure Components: 3. software applications

Software Trends

- **Open Source Software** Linux, Apache
- **Cloud Computing** Google Apps, Office Web Apps
- **Mashups** are Web applications that combine content or data from multiple online sources into new Web applications
  - ✓ Contents are continually updated
  - ✓ Content for mashups often comes from Web feeds and Web services
  - ✓ Amazon uses mashup technologies to aggregate product descriptions with partner sites and user profiles, commentaries, and images.
  - ✓ Travel sites, such as Travelocity, Kayak, Matador, and Travature, integrate standard content (such as airfare search engines, travel guides, maps, and hotel reviews) with comments, ratings, and images from users

Infrastructure Components: 3. software applications

Managing Hardware and Software Technology

- **Capacity planning** how to plan the scalability issues in an organization
  - Process of predicting when hardware system becomes saturated
  - Ensuring firm has enough computing power for current and future needs
  - Factors include:
    - Maximum number of users
    - Impact of current, future software
    - Performance measures
      - minimum response time for processing business transactions.
      - Throughput

Infrastructure Components: 3. software applications

Managing Hardware and Software Technology

- **Scalability:**

  ability of system to expand to serve large number of users without breaking down

  - Organizations must ensure they have sufficient computer processing, storage, and network resources to handle surging volumes of digital transactions and to make such data immediately available online.

Infrastructure Components: 3. software applications

Managing Hardware and Software Technology

- **Total Cost of Ownership (TCO) model**
  - Used to analyze direct and indirect costs to help determine the actual cost of owning a specific technology
    - **Direct costs: hardware, software purchase costs**
    - **Indirect costs: ongoing administration costs, upgrades, maintenance, technical support, training, utility, and real estate costs**
    - **Hidden costs: support staff, downtime, additional network management**
  - Five year TCO for computing equipment can be 3 – 10 times the original purchase price
  - TCO can be reduced through increased centralization, standardization of hardware and software resources.

Infrastructure Components: 3. software applications

Components of TCO for a IT System

Hardware acquisition	Purchase price of hardware including computers, terminals, storage and printers
Software acquisition	Purchase or license of software for each user
Installation	Cost to install hardware and software
Training	Cost to train IT staff and end-users
Support	Cost to provide ongoing technical support; help desks, documentation etc.
Infrastructure	Cost to acquire, maintain and support related infrastructure such as networks and specialized equipment (including storage and backup units)
Downtime	Lost productivity if hardware or software failures cause the system to unavailable for processing user tasks
Space and energy	Real estate and utility costs for hosing and providing power for the technology

Infrastructure Components: 3. software applications

Strategies for Creating and Deploying Software

- **Commercial off-the-shelf** software solutions are ready-made and available for licensing or sale to the general public
  - Off-the-shelf software systems that cannot be modified to meet the specific needs of a particular organization are sometimes called turn-key systems or software

- **Custom software development** describes how an organization develops and builds software tailored specifically to its needs.

Infrastructure Components: 3. software applications

Strategies for Creating and Deploying Software

- **Using technology service providers**
  - **Outsourcing**
    - Using external provider to:
      - Run networks.
      - Host, manage Web site(s).
      - Develop software (**offshore software outsourcing**).
      - Manage IT infrastructures.
    - Requires **Service Level Agreements (SLAs)**
      - a formal contracts between customers and service providers that define the specific responsibilities of the service provider and the level of service expected by the customer.

Infrastructure Components: 3. software applications

Advantages of Outsourcing

- Allows a business to concentrate on its core competencies rather than focusing on technology issues.
- Instead of purchasing all the necessary hardware and software for hosting a Web site, a business can use a Web hosting service that maintains a large Web server
- Outsourcing custom software development or maintenance to outside firms benefits a company because it won't have to hire programmers, analysts, and managers with the necessary skills.
- An outsourcer often has the technical and management skills to do the job better, faster, and more efficiently.
- Even though it's often cheaper to outsource the maintenance of an IT infrastructure and the development of new systems to external vendors, a business must weight the pros and cons carefully.

Infrastructure Components: 3. software applications

Managing Hardware and Software Technology

- Using cloud services
  - Small businesses “rent” infrastructure from another firm to avoid expenses of maintaining hardware and software on their own.
    - Off-loading peak demand to remote data centers
  - Amazon Markets http://www.amazonservices.com/ provides cloud services to major business firms, and also to thousands of small merchants who want to use Amazon software to sell their goods and services.
- Managing mobile platforms
  - Balancing gains in productivity from using mobile devices with expenses of equipping employees with these devices
    - TCO for wireless devices ranges from $1,000 to $3,000

Infrastructure Components: 3. software applications

Managing Hardware and Software Technology

- Managing software localization for global business
  - Local language interfaces
    - English not typically standard at middle, lower levels
    - Interfaces are complex: menu bars, error messages, online forms, search results, and so on
  - Differences in local cultures
  - Differences in monetary structure
  - Differences in business processes
- All of these factors add to TCO of using technology service providers

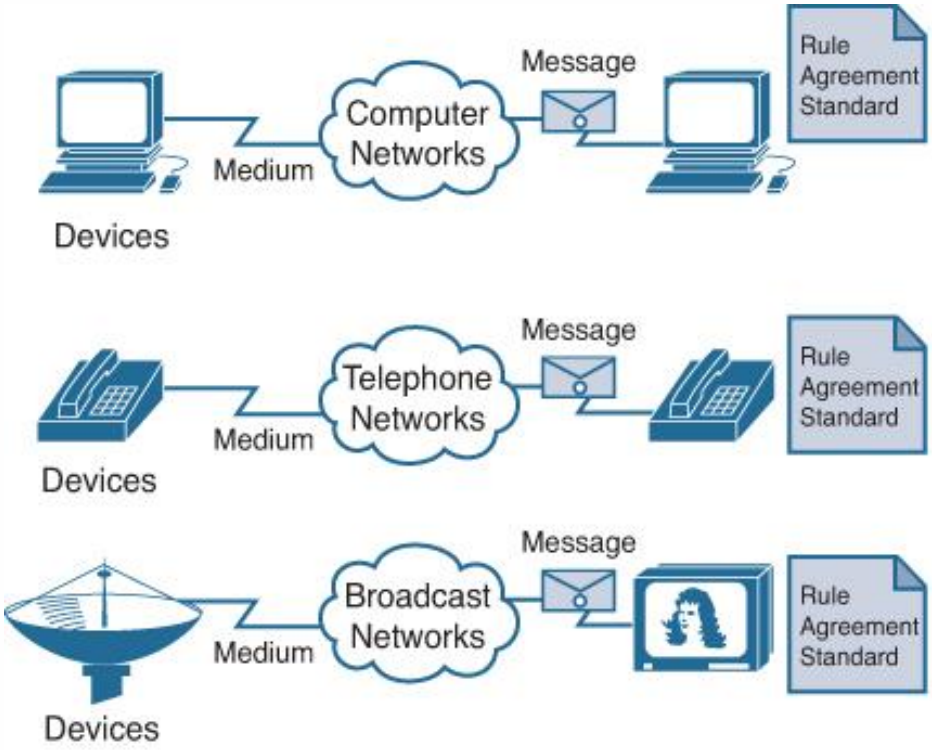
Infrastructure Components: 4. Data management and storage

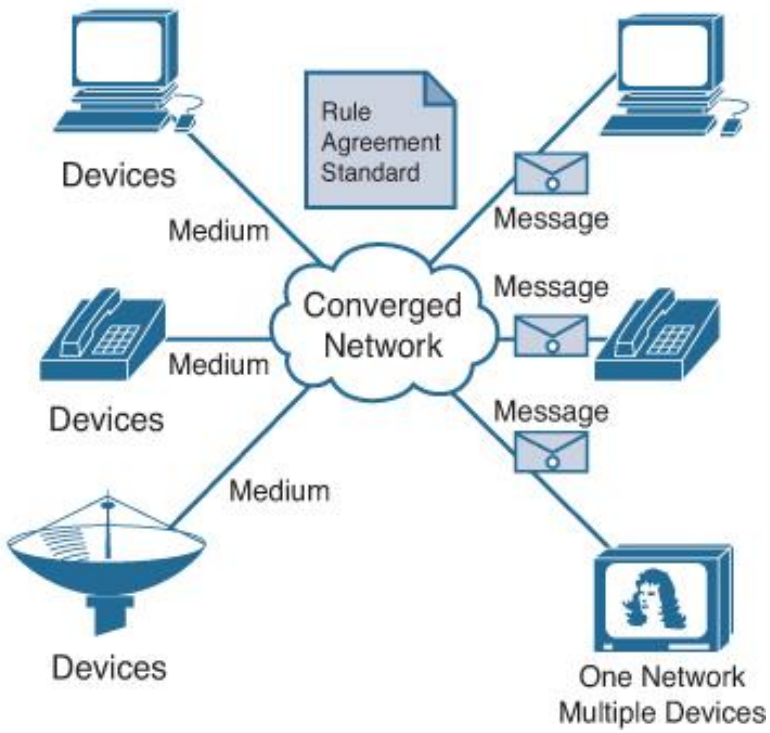
- Data management and storage
  - Database software: IBM (DB2), Oracle, Microsoft (SQL Server), Sybase (Adaptive Server Enterprise), MySQL
  - Physical data storage: EMC Corp (large-scale systems), Seagate, Maxtor, Western Digital
  - Storage area networks: connect multiple storage devices on dedicated network

Infrastructure Components: 5. Networking platforms

- **Networking/telecommunications platforms**
  - Telecommunication services
    - Telecommunications, cable, telephone company charges for voice lines and Internet access
  - Network operating systems:
    - Windows Server, Novell, Linux, Unix
  - Network hardware providers: Cisco, Lucent, Nortel, Juniper Networks

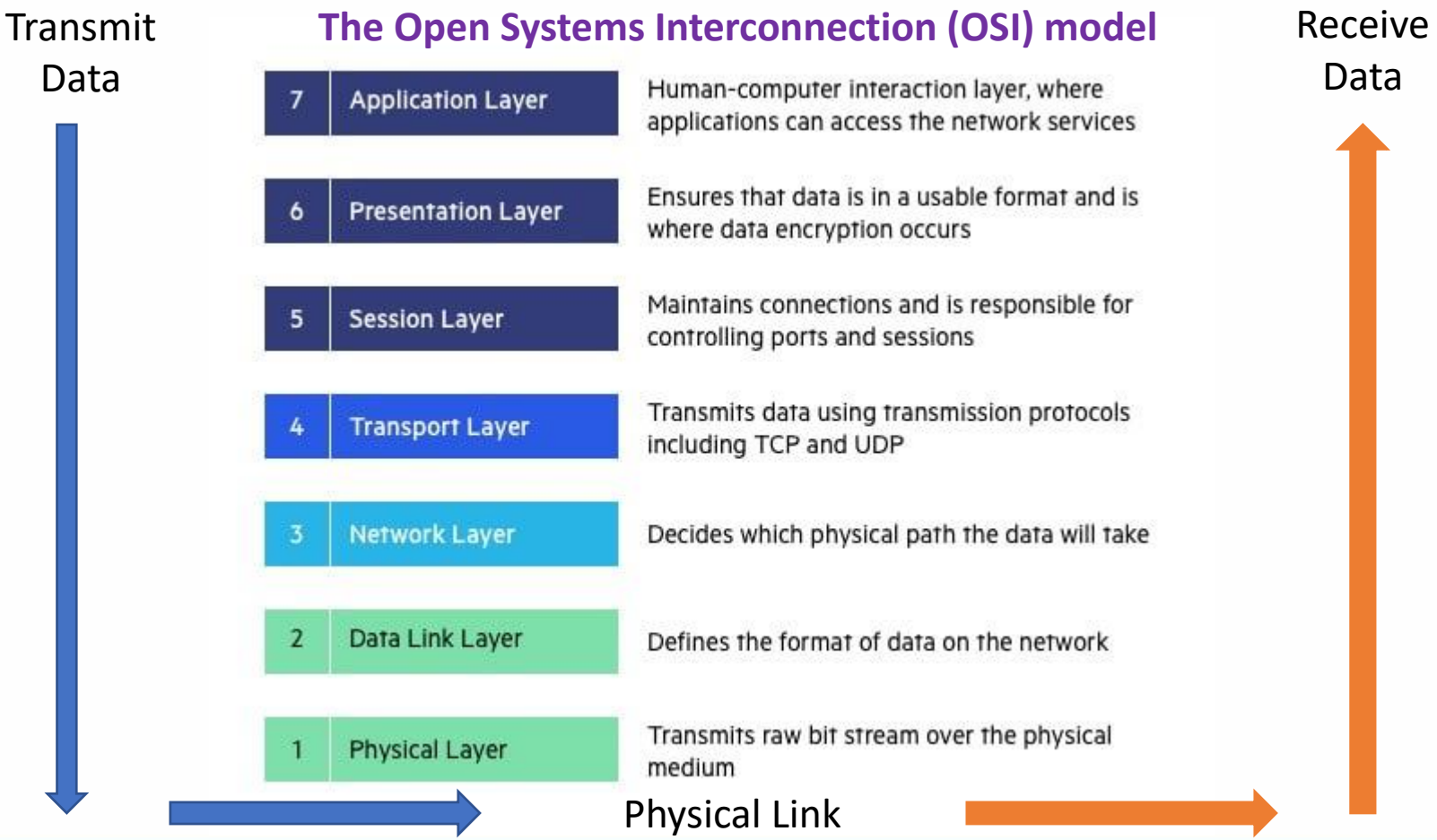
Infrastructure Components: 5. Networking platforms





https://www.ciscopress.com/articles/article.asp?p=2158215&seqNum=5

Infrastructure Components: 5. Networking platforms

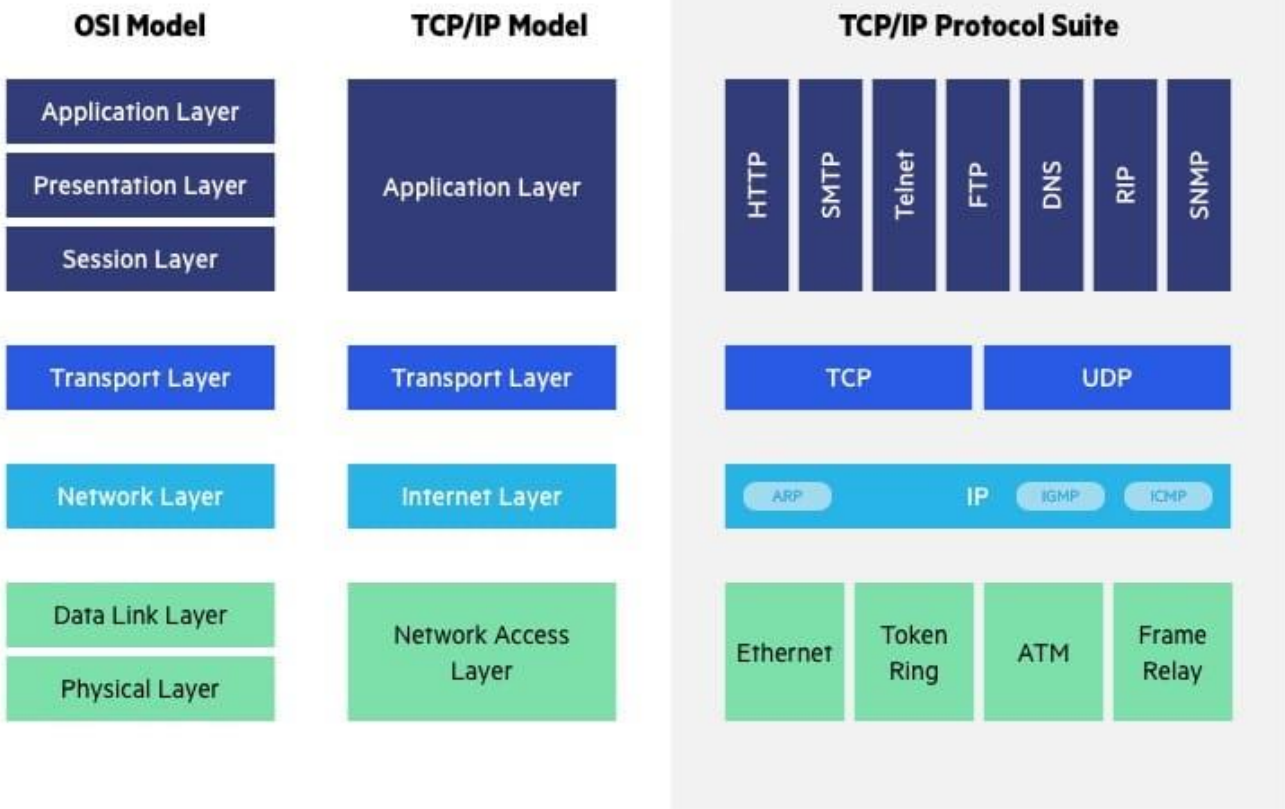


Infrastructure Components: 6. Internet platforms

- Internet platforms
  - Hardware, software, management services to support company Web sites, (including Web hosting services) intranets, extranets
  - Internet hardware server market: Dell, HP/Compaq, IBM
  - Web development tools/suites: Microsoft (FrontPage, .NET) IBM (WebSphere) Sun (Java), independent software developers: Macromedia/Adobe, RealMedia

Infrastructure Components: 6. Internet platforms

OSI vs. TCP/IP Model

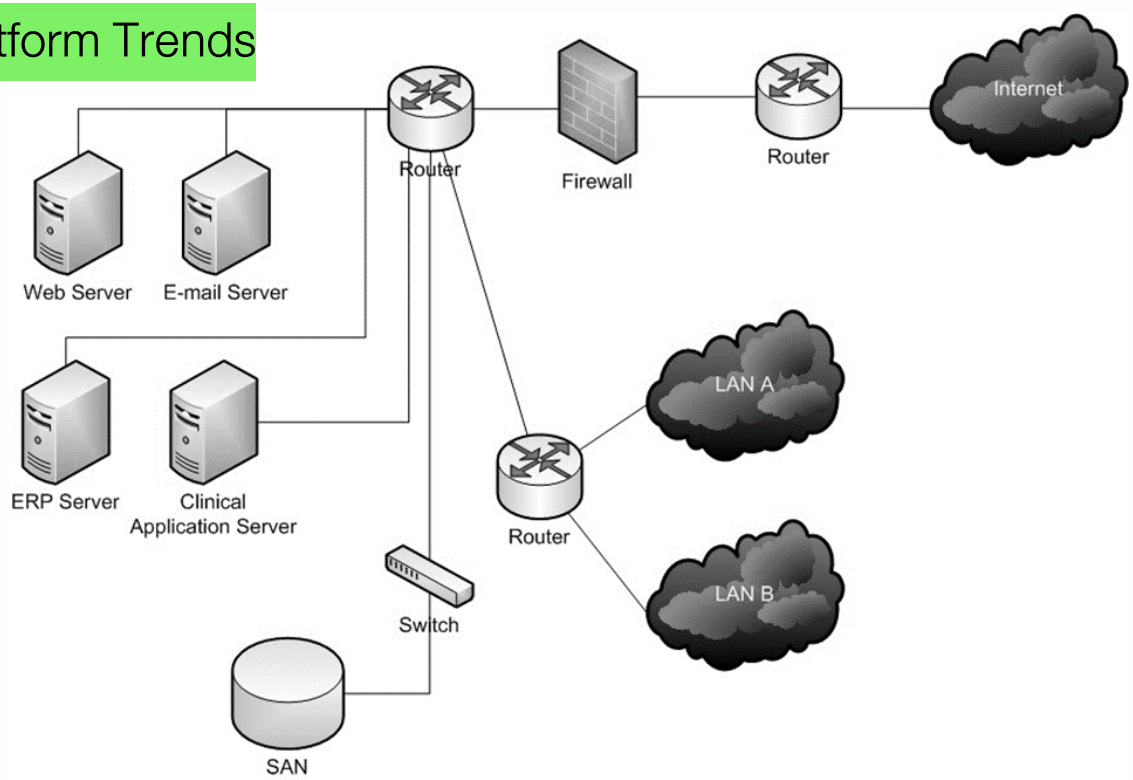


Infrastructure Components: 7. Consulting and system integration services

- Consulting and system integration services
  - Even large firms do not have resources for full range of support for new, complex infrastructure
  - Software integration: ensuring new infrastructure works with legacy systems
  - Legacy systems: older TPS created for mainframes that would be too costly to replace or redesign
  - Accenture, IBM Global Services, EDS, Infosys, Wipro

Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Hardware Platform Trends
- Security Management
- Example of Hospital IT infra.



Contemporary Hardware Platform Trends

- While cost of computing is lower, infrastructure costs have expanded
  - More computing, more sophisticated computing, increased consumer expectations, need for security
- The emerging mobile digital platform
  - Cell phones, smartphones (Samsung, iPhone) have assumed data transmission, Web surfing, e-mail and IM duties
  - Netbooks: small, low-cost lightweight notebooks optimized for wireless communication and core computing tasks

Contemporary Hardware Platform Trends

- **Grid computing**
  - Connects geographically remote computers into a single network to combine processing power and create virtual supercomputer
  - Provides cost savings, speed, agility
- **Cloud computing (utility computing)**
  - Data permanently stored in remote servers, accessed and updated over the Internet by users
  - Organizations using cloud computing need only pay for the computing power they actually use (on-demand or utility computing)

Contemporary Hardware Platform Trends

Software Platform Trends and Emerging Technologies

- Web Services
  - Software components that exchange information using Web standards & languages
  - **XML**: Extensible Markup Language
    - More powerful and flexible than HTML
    - Tagging allows computers to process data automatically
  - **SOAP**: Simple Object Access Protocol
    - Rules for structuring messages enabling applications to pass data & instructions
  - **WSDL**: Web Services Description Language
    - Framework for describing Web service and capabilities
  - **UDDI**: Universal Description, Discovery, and Integration
    - Directory for locating Web services

Contemporary Hardware Platform Trends

- **Mashups and widgets**
  - Mashups: Combinations of two or more online applications, such as combining mapping software (Google Maps) with local content
  - Widgets: small programs that can be added to Web pages or placed on the desktop to add additional functionality
- **Software outsourcing**
  - Three sources: external commercial vendor, online service providers, offshore firms
  - Software packages: prewitten set of software available commercially
  - Software as a service (SaaS): software delivered over the Internet
  - Offshore outsourcing: usually governed by service level agreement

Contemporary Hardware Platform Trends

- Management and governance
  - Who controls IT infrastructure
  - Centralized/decentralized
  - How are costs allocated between divisions, departments?

Contemporary Hardware Platform Trends

Storage Mgt, Backup & Recovery

- **Storage management and allocation**: this activity manages all aspects of the management, allocation and housekeeping of media and information storage

- **System backup and recovery:** backup and recovery are complementary in the sense that backup is almost always scheduled in advance and recovery is usually reactive and unscheduled.

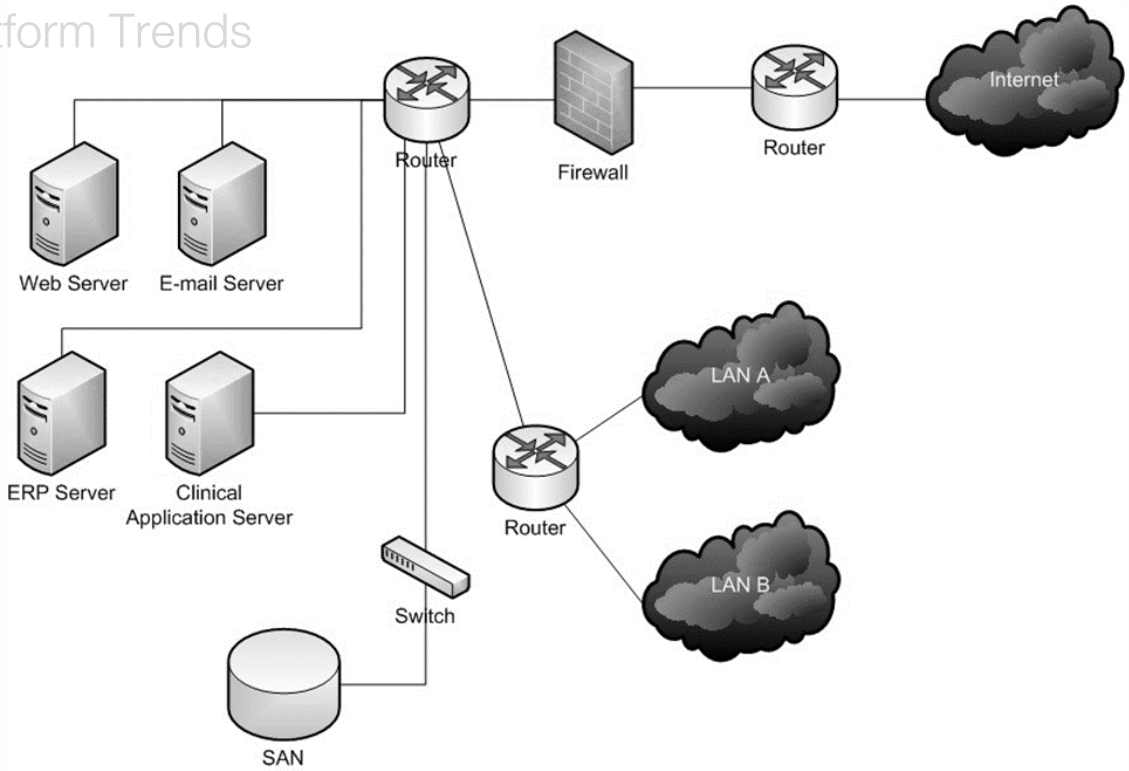
Contemporary Hardware Platform Trends

Storage Mgt, Backup & Recovery

- **Information management:** would include the use of document and hierarchical information management systems. This process should ensure that the right information is stored in the appropriate media, with the right level of access and speed of retrieval.
- **Database management and administration:** is responsible for the regular management and administrative tasks necessary for support and maintenance of all operational databases.

Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Hardware Platform Trends
- Security Management
- Example of Hospital IT infra.



Security Management

- Security monitoring:
- Security control:

https://images.app.goo.gl/Xp986gyHE28uVBa19

Security Management

- Security monitoring:

  monitors, verifies and tracks

  - detection and containment of all intrusion attempts and attempts at unauthorised access
  - logging, management and reporting.

Security Management

- **Security control:**
  - physical security: the element of Security Management that prevents unauthorised, unwanted and unnecessary physical access
  - logical security: the component of Security Management that prevents unauthorised, unwanted and unnecessary logical access to ICT information and systems by using measures on classification, authentication and access controls.

Network Security

- What is security?
- Why do we need security?
- Who is vulnerable?
- Common security attacks and countermeasures
  - Firewalls & Intrusion Detection Systems
  - Denial of Service Attacks
  - Transmission Control Protocol (TCP) Attacks
  - Packet Sniffing
  - Social Problems

What is "Security"

- Freedom from risk or danger; safety.
- Something that gives or assures safety, as:
  - A group or department of private guards: Call building security if a visitor acts suspicious.
  - Measures adopted by a government to prevent espionage, sabotage, or attack.
  - Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.
- …etc.

From dictionary.com

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: The Andrew File System (AFS)
- Guarantee availability of resources
  - Ex: 99.99 % Reliability

The theoretical availability is computed as 100% minus the product of the component failure rates

Who is vulnerable?

- Anyone on the network
- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

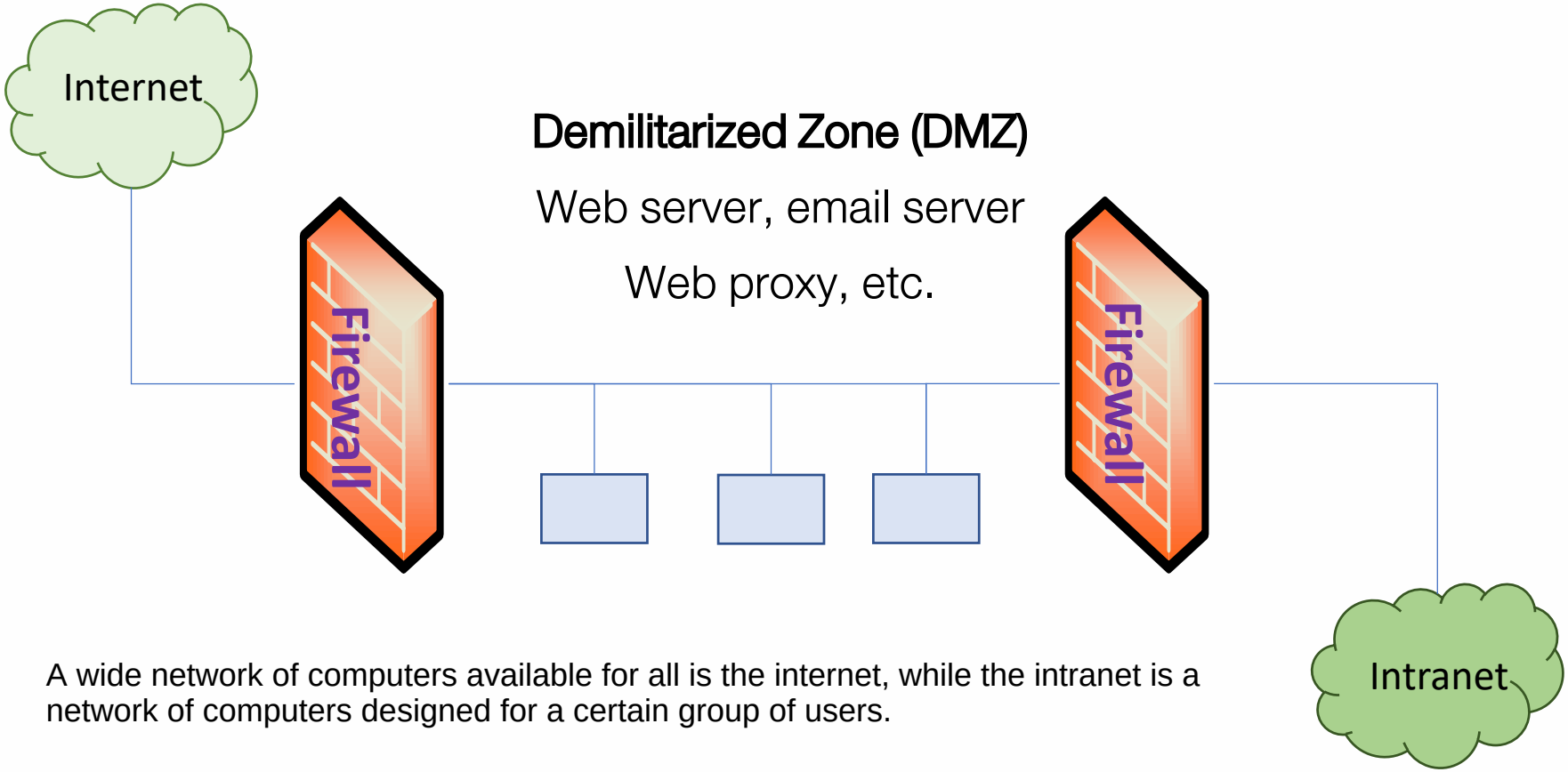
Firewalls

- Basic problem – many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators

Firewalls

- A firewall is like a castle with a drawbridge
  - Only one point of access into the network
  - This can be good or bad
- Can be hardware or software
  - Ex. Some routers come with firewall functionality
  - Windows XP and Mac OS X have built in firewalls

Firewalls



A wide network of computers available for all is the internet, while the intranet is a network of computers designed for a certain group of users.

Intrusion Detection

- Used to monitor for "suspicious activity" on a network
  - Can protect against known software exploits, like buffer overflows

- Open Source IDS: Snort, www.snort.org

Intrusion Detection

- Uses “intrusion signatures”
  - Well known patterns of behavior
  - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
- Example
  - IRIX vulnerability in webdist.cgi
- However, IDS is only useful if contingency plans are in place to curb attacks as they are occurring

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, “3c9i28@$e” is a good password

Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks

Denial of Service : SYN flooding attack

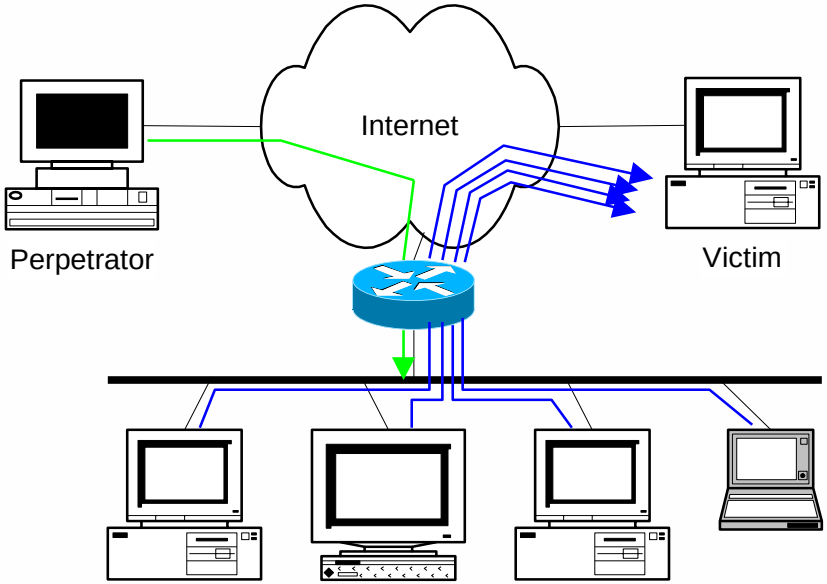
- Send SYN packets with bogus source address
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state
- Solution: use "SYN cookies"
  - In response to a SYN, create a special "cookie" for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

Denial of Service : SMURF

- Source IP address of a broadcast ping is forged
- Large number of machines respond back to victim, overloading it

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply



Denial of Service : Distributed Denial of Service

- Same techniques as regular DoS, but on a much larger scale
- Example: Sub7Server Trojan and IRC bots
  - Infect a large number of machines with a “zombie” program
  - Zombie program logs into an IRC channel and awaits commands

TCP Attacks

- Recall how IP works…
  - End hosts create IP packets and routers process them purely based on destination address alone
- Problem: End hosts may lie about other fields which do not affect delivery
  - Source address – host may trick destination into believing that the packet is from a trusted source
    - Especially applications which use IP addresses as a simple authentication method
    - Solution – use better authentication methods

TCP Attacks

- TCP connections have associated state
  - Starting sequence numbers, port numbers
- Problem – what if an attacker learns these values?
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be hijacked!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

TCP Attacks

- Say hello to Jane, Loki and Thor

TCP Attacks

- Jane and Thor have an established TCP connection

TCP Attacks

- Loki lies on the path between Jane and Thor on the network
- He can intercept all of their packets

TCP Attacks

- First, Loki must drop all of Jane's packets since they must not be delivered to Thor

TCP Attacks

- Then, Loki sends his malicious packet with the next ISN (sniffed from the network)

ISN, SRC = Jane

TCP Attacks

- What if Loki is unable to sniff the packets between Jane and Thor?
  - Can just DoS Jane instead of dropping her packets
  - Can just send guesses of what the ISN is until it is accepted

TCP Attacks

- Why are these types of TCP attacks so dangerous?

Web Server

Malicious User

Trusting Web Client

TCP Attacks

- How do we prevent this?
- IPSec
  - Provides source authentication, so Loki cannot pretend to be Jane
  - Encrypts data before transport, so Loki cannot talk to Thor without knowing what the session key is

Two Factor Authentication, or 2FA, is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.

Packet Sniffing

- Recall how Ethernet works …
- When someone wants to send a packet to some else …
- They put the bits on the wire with the destination MAC address …
- And remember that other hosts are listening on the wire to detect for collisions …
- It couldn't get any easier to figure out what data is being transmitted over the network!

Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium

Packet Sniffing

- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
  - Passwords are the most popular

Packet Sniffing

- How can we protect ourselves?
- HTTPS
  - Especially when making purchases with credit cards!
- IPSec
  - Provides network-layer confidentiality

Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the “harmed” stage, unless they have been specially trained
    - Think government here…

Social Problems

- Fun Example 1:
- Someone calls you in the middle of the night
  - "Have you been calling Egypt for the last six hours?"
  - "No"
  - "Well, we have a call that's actually active right now, it's on your calling card and it's to Egypt and as a matter of fact, you've got about $2000 worth of charges on your card and … read off your AT&T card number and PIN and then I'll get rid of the charge for you"

Social Problems

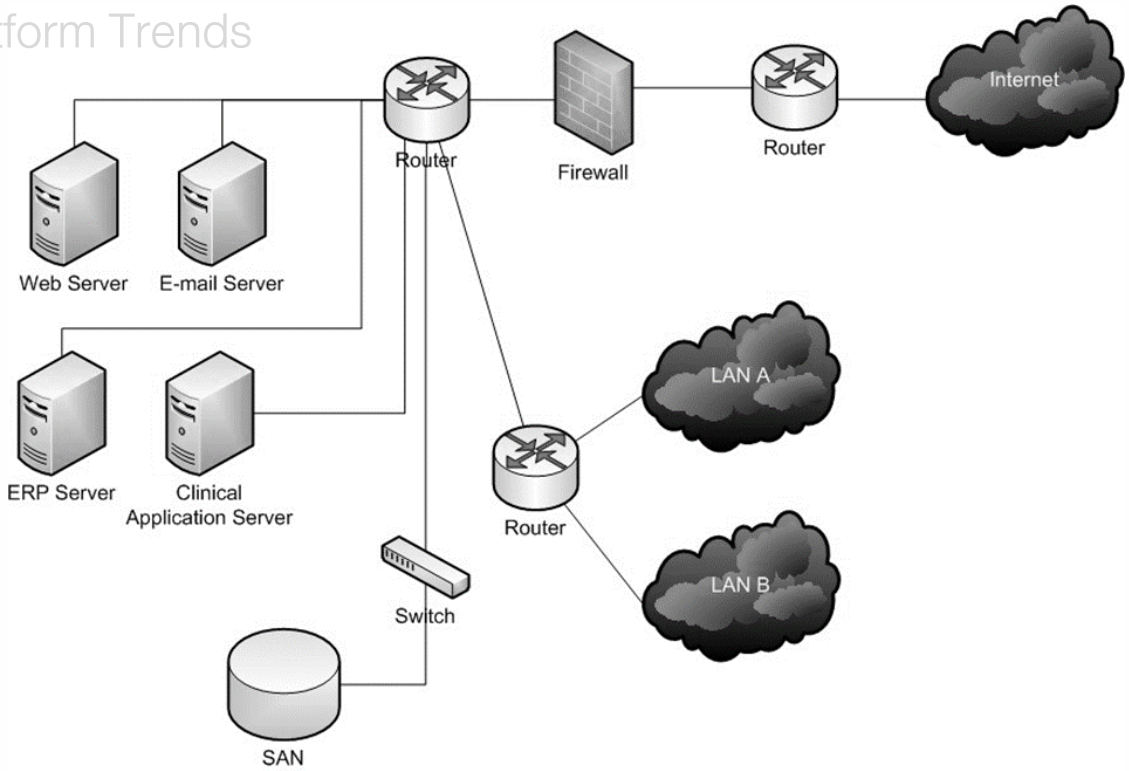
- Fun Example 2:
- Who saw Office Space?
- In the movie, the three disgruntled employees installed a money-stealing worm onto the companies systems
- They did this from inside the company, where they had full access to the companies systems
  - What security techniques can we use to prevent this type of access?

Social Problems

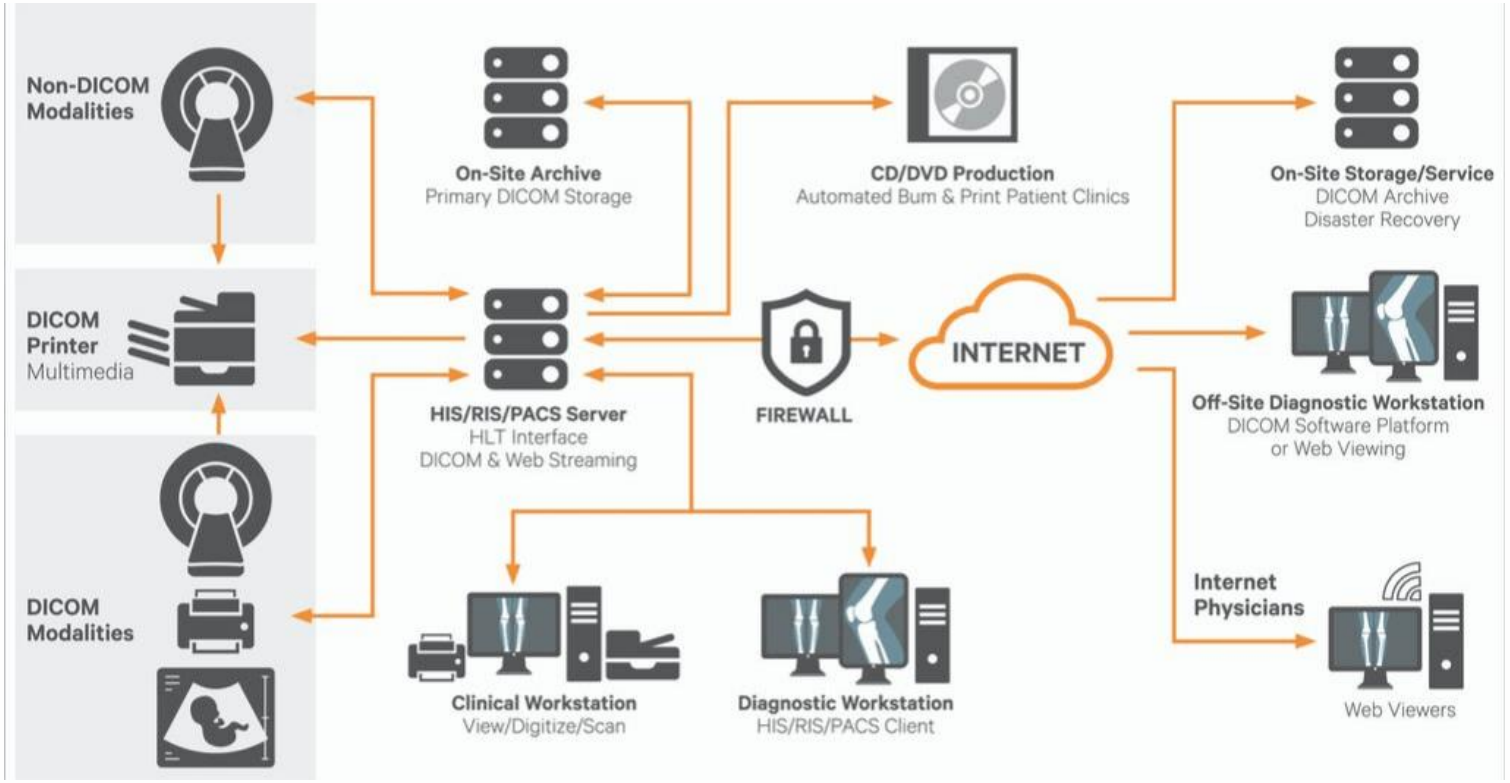
- There aren't always solutions to all of these problems
  - Humans will continue to be tricked into giving out information they shouldn't
  - Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
- So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information
  - But, this solution is still not perfect

Outline

- Defining IT infrastructure
- Infrastructure Components
- Contemporary Hardware Platform Trends
- Security Management
- Example of Hospital IT infra.

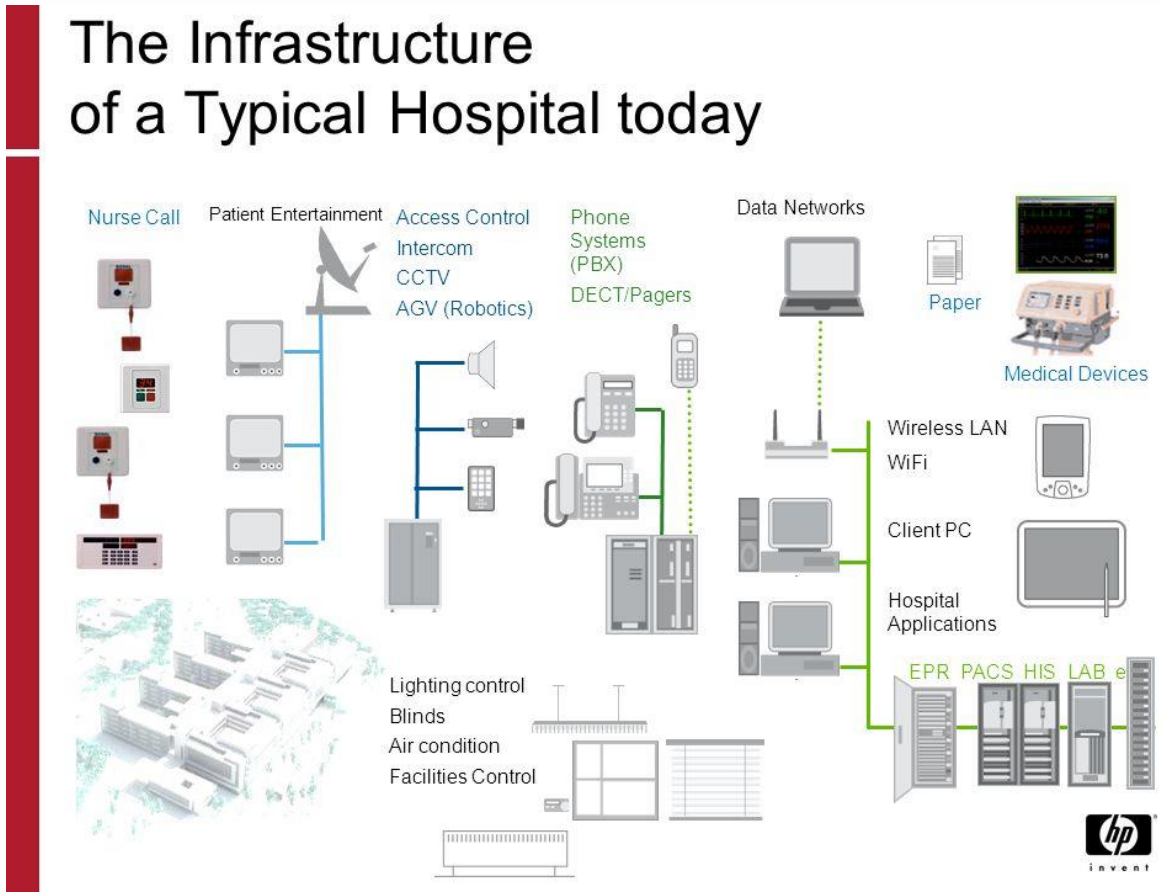


Example of Healthcare IT Infrastructure



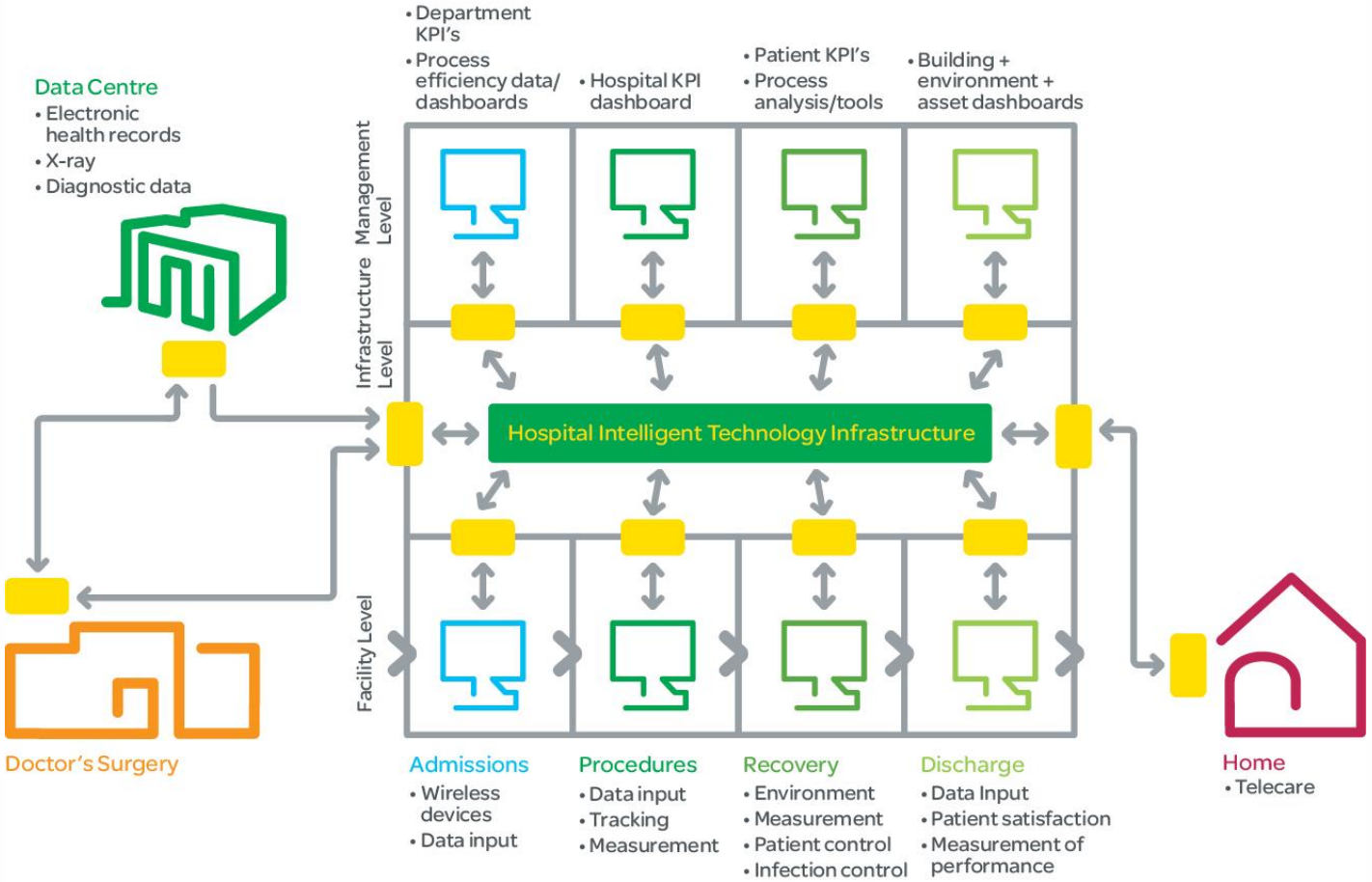
https://www.healthtechdigital.com/vertiv-identifies-solutions-to-gaps-in-hospital-it-infrastructure/

Example of Healthcare IT Infrastructure



https://slideplayer.com/slide/1594486/

Example of Healthcare IT Infrastructure



https://blog.se.com/uncategorized/2013/05/10/intelligent-infrastructure-the-future-of-high-performing-healthcare-organizations/