IT Service Delivery and Support Week Five

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Network Topics

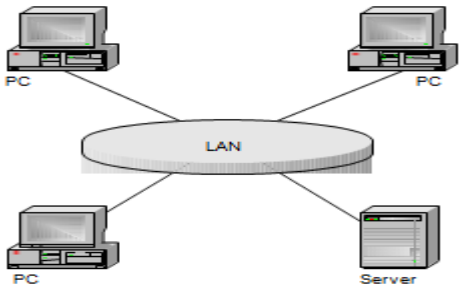
* Network Types
* Topology
* Network Devices 101
* Protocols
* Risks and Controls Associated with Network Environment
* Audit Network

Network Classification

* Local Area Network (LAN)
* Wide Area Network (WAN)
* Metropolitan Area Network (MAN)
* Storage Area Network (SAN)
* Personal Area Network (PAN)
* Wireless Network (sometimes WLAN)

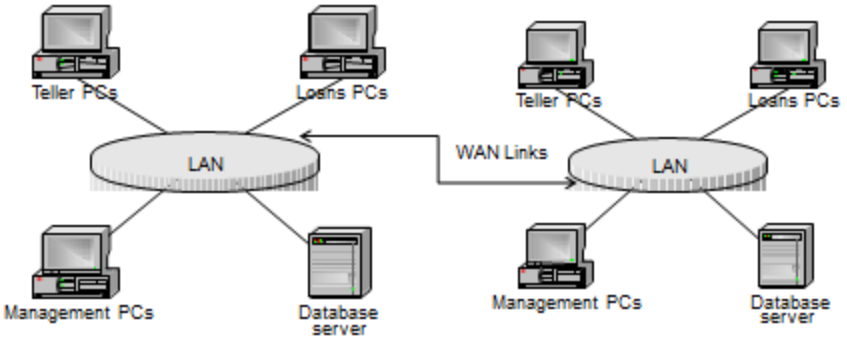
Local Area Network (LAN)

A local area network connects two or more computers or peripherals. Each computer and peripheral must be equipped with a network interface card (NIC) to connect to the wiring system. Software in the operating system (called drivers) operates the network interface cards.



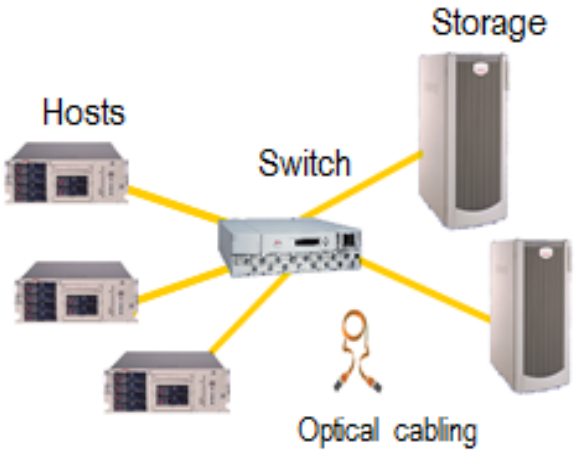
Wide Area Network (WAN)

A wide area network provides connectivity between local area networks. This is accomplished by using services such as dedicated leased phone lines, dial-up phone lines, satellite links and data packet carrier services. WANs can be as simple as two LANs connected or a very complex global corporate network connecting offices in many different countries.



SAN & PAN

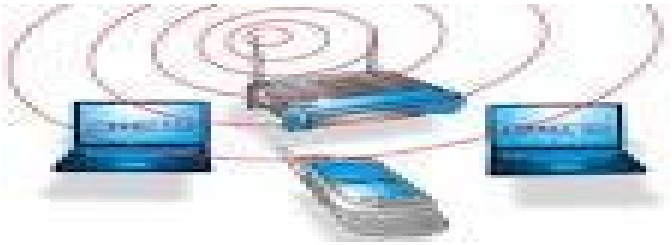
Storage Area Network (SAN)



Personal Area Network (PAN)

Wireless LANs

* No wiring – easy to install
* Security concerns:
  * Interception of wireless communication (war-drive)
  * Unauthorized wireless access points (back door)
  * Security of mobile, handheld devices (loss/misuse/distraction/health concerns)
  * Wi-Fi access point – broadcast outside of the org. ‘s perimeter



Cabling

A local area network can be implemented with several choices of connection technology. Characteristics of each technology are listed below:

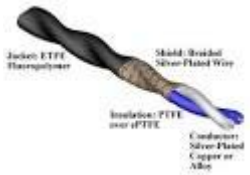
- Coaxial Cable
- Twisted Pair
- Fiber-Optic Cable
- Wireless LANs

Coaxial Cable

* Use cable similar to cable television cable
* Relatively immune to interference. The bulkiest and heaviest of the three types of cable
* Carry data for long distance (thousands of feet) without re-amplification
* An older technology and not typically used for new network installations (prior to 1992)

Twisted Pair

* Telephone-like wire. Modern LANs require a high quality cable designed specifically for data communication (CAT-5 & CAT-6 with RJ-45 Connector)
* Not immune to interference. Susceptible to wiretaps due to its simple construction
* Carry data only short distances (tens of hundreds of feet)
* Inexpensive
* The most common cabling for LAN installation



Fiber-Optic Cable

* Made from glass or plastic
* Most resistant to interface
* Sensitive to damage from extreme heat
* Very difficult to tap – NOT impossible
* Carry data the longest distances without re-amplification
* Extremely high transmission speeds (GHz) - FIOS

LAN Topology

Topology – How the network is wired

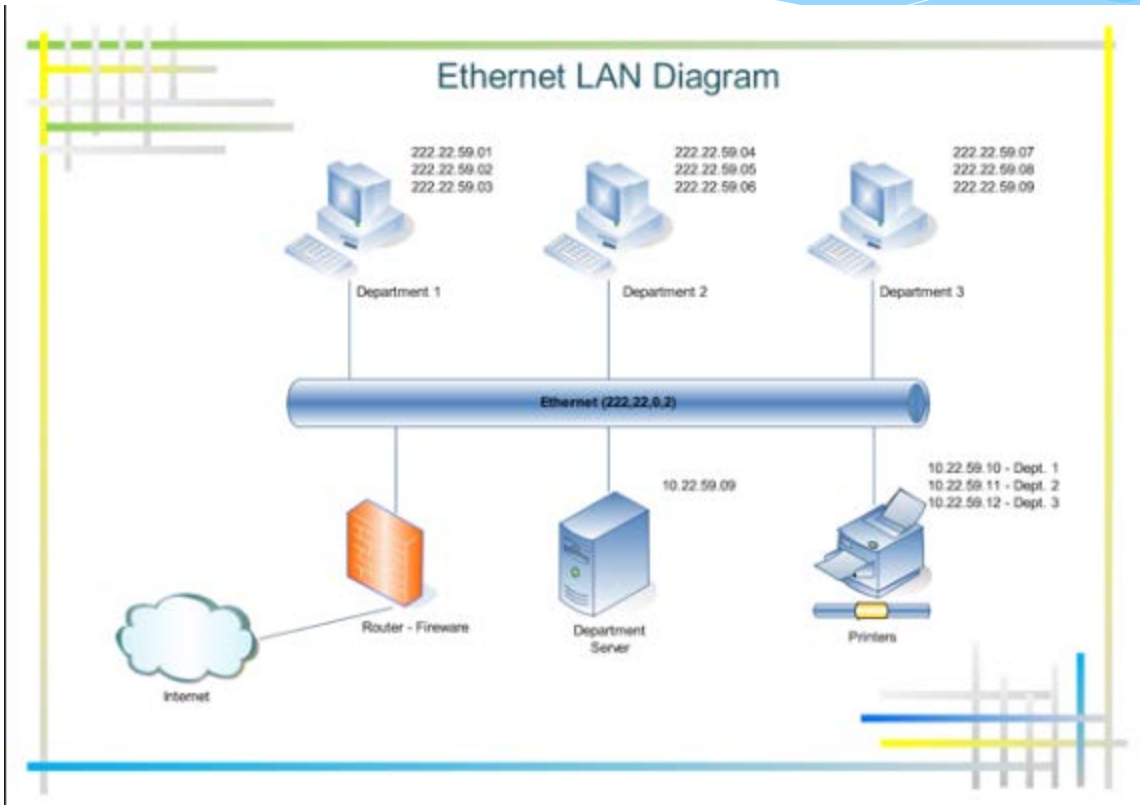
Common LAN Topology

* Ethernet
* Token Ring
* AppleTalk
* Fiber Distributed Data Interchange (FDDI)

Ethernet

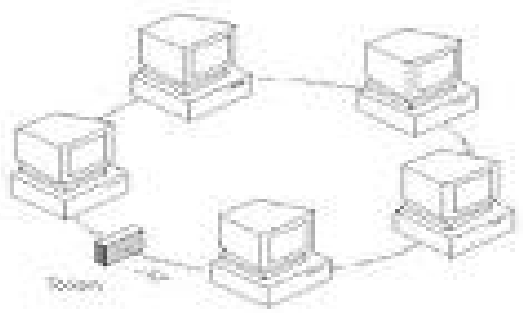
* Most widespread LAN topology
* Low cost
* Faster than token ring
* First come first serve protocol
* Good balance between speed, cost and ease of installation

Ethernet


Ethernet LAN Diagram
222.22.59.01
222.22.59.02
222.22.59.03
222.22.59.04
222.22.59.05
222.22.59.06
222.22.59.07
222.22.59.08
222.22.59.09
Department 1
Department 2
Department 3
Ethernet (222.22.0.2)
10.22.59.09
10.22.59.10 - Dept. 1
10.22.59.11 - Dept. 2
10.22.59.12 - Dept. 3
Router - Fireware
Department Server
Printers
Internet

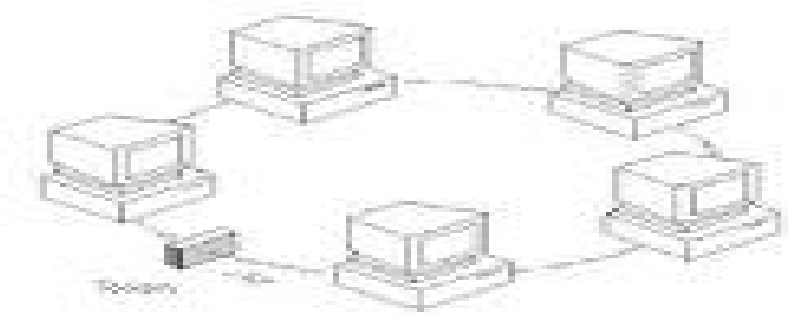
Token Ring

* Controlled protocol using tokens
* Passing token along the ring and viewed by each device
* More expensive
* Slower than Ethernet
* Small installed base



Fiber Distribute Data Interchange (FDDI)

* A Token Ring like protocol
* Reliable fiber optic systems
* Building wide and campus wide backbone network



Connectivity

Several types of devices provide LAN and WAN connectivity.

* Repeater
* Hub
* Bridge
* Switch
* Router
* Gateway

Connectivity

* Repeater A repeater is an electrical amplifier used to boost the signal on a LAN. Often a terminal is too far from the hub or switch to reliably send or receive data.
* Hub A hub is a concentration point for a LAN. The hub has four or more outlets (called ports). Each terminal, server, printer, etc. connects to one of the hub's outlet. The device pictured below has eight ports.

Bridge

* A bridge provides connection between two LANs. The bridge looks at every packet on both LANs and only pass the packets that need to travel from one LAN to the other LAN.
  * Both LAN segments must be the same type (either Token Ring or Ethernet).
  * Bridges use the NIC address (also called the media access control or MAC address) to decide which packets pass through the bridge. The MAC address identifies the machine that is sending the data, not the user associated with the machine or the type of data that is being sent. As a result bridges cannot be used as firewalls.
  * MAC address is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), e.g.01-23-45-67-89-ab

Switch

* A switch is similar in functionality to a bridge but has numerous switch ports versus two (2) ports for a bridge.
* Switches are widely used because they are fast and inexpensive. They are quickly replacing bridges due to the cost and speed factors.
* Switches can support both MAC Address and IP address, depending on the type of switch. Usually large networks use switches instead of hubs to connect computers within the same subnet.

Router

* A router is a more sophisticated bridge.
* Routers can be used to connect two or more LAN segments. One of the segments can be the Internet or a connection to another organization's network (extranet).
* A router can move messages between Token Ring and Ethernet LANs. (different protocols)
* Routers support different WAN technologies but switches do not.

Gateway

* A gateway moves messages between two networks that use different network protocols such as SNA/SDLC, TCP/IP, or IPX/SPX.
* A gateway often provides software translation and repackaging of messages as they move between the systems on each network.

Dial-Up

Dial-up circuits are analog or digital. Analog use standard voice circuits; connectivity is provided by a modem at each end. Digital dial-up circuits are available via a telephone company service called Integrated Services Digital Network (ISDN).

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) VPNs extend the corporate network out to employee homes, business partners and remote offices. VPNs look like a "private network" but are instead using service provider networks or the Internet to "tunnel" packets of information between two locations.

Firewalls

A firewall is hardware or software that is used to isolate one network from another such as between your organization and the Internet. Firewalls should also be used to isolate extranets. For sensitive areas, organizations can isolate divisions and departments within their own networks with firewalls.

The logic used by firewalls for blocking messages is based on configuration rules. Firewalls can isolate messages based on:

- Network (IP, IPX, Frame Relay) address
- Message type (port number)
- Message content

Firewall Types:

- Packet Filtering – inspect head of the packet
- Stateful Packet Inspection – head and content
- Application Layer Proxy – more stricter rules: they not only want to know who the guest is, but what he or she will be doing once they are inside the club

Characteristics of dial-up

Characteristics of dial-up are:

- Dynamic and on demand - can establish a connection almost anytime it is required.
- Easy to use - most programs are equipped with dialing software.
- Inexpensive back up solution.
- Usage costs - usually are based on a combination of time of day, distance between the two locations, and duration of the call.

Typical speeds - up to 52,000 bps between the sender and receiver.

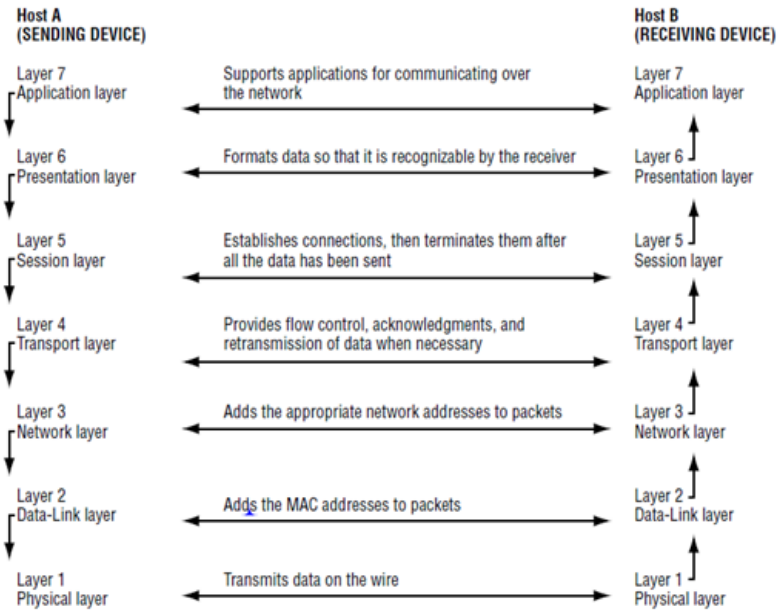
LAN Protocols

* Protocol – To ensure data uses consistent format and messaging rules between computers and application programs.
* Protocol example:
  * TCP/IP;
  * IPX/SPX;
  * Apple Talk

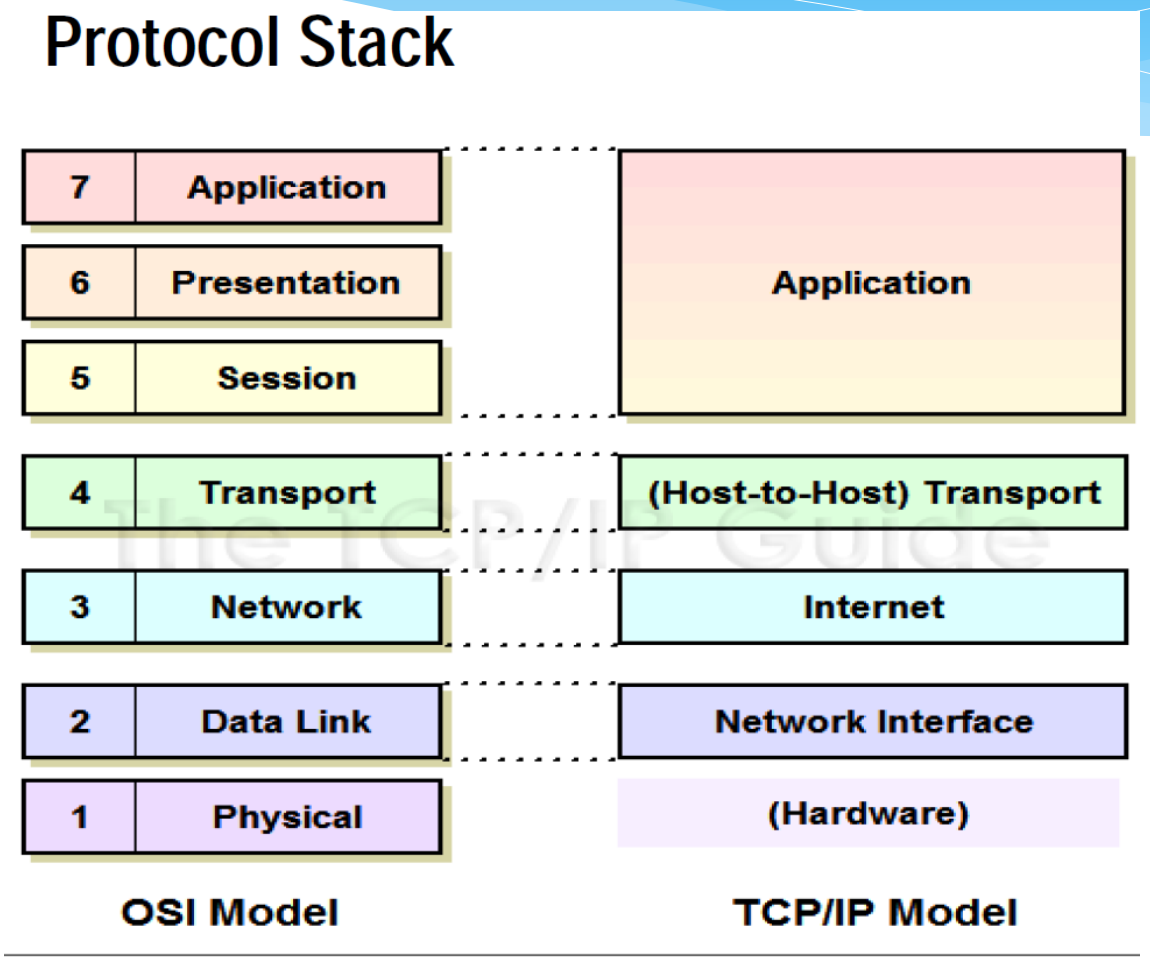
IP Address Classes

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

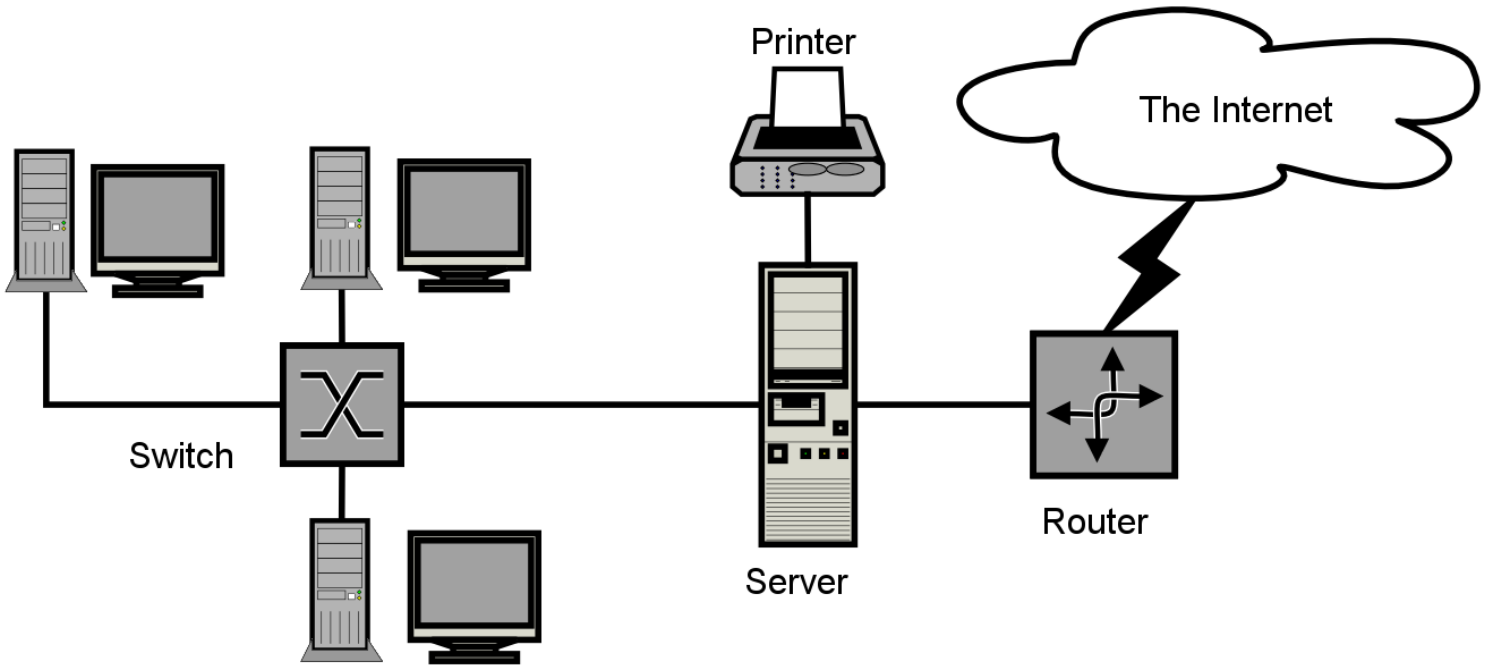
OSI Flow


Host A
(SENDING DEVICE)
Host B
(RECEIVING DEVICE)
Layer 7
Application layer
Supports applications for communicating over the network
Layer 7
Application layer
Layer 6
Presentation layer
Formats data so that it is recognizable by the receiver
Layer 6
Presentation layer
Layer 5
Session layer
Establishes connections, then terminates them after all the data has been sent
Layer 5
Session layer
Layer 4
Transport layer
Provides flow control, acknowledgments, and retransmission of data when necessary
Layer 4
Transport layer
Layer 3
Network layer
Adds the appropriate network addresses to packets
Layer 3
Network layer
Layer 2
Data-Link layer
Adds the MAC addresses to packets
Layer 2
Data-Link layer
Layer 1
Physical layer
Transmits data on the wire
Layer 1
Physical layer

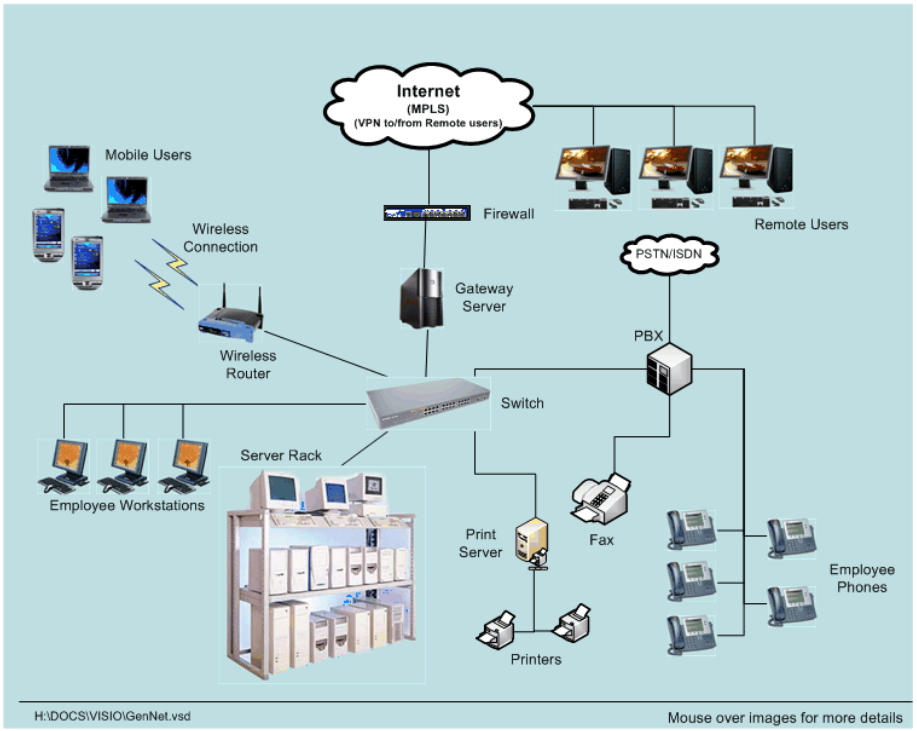
OSI and TCP/IP



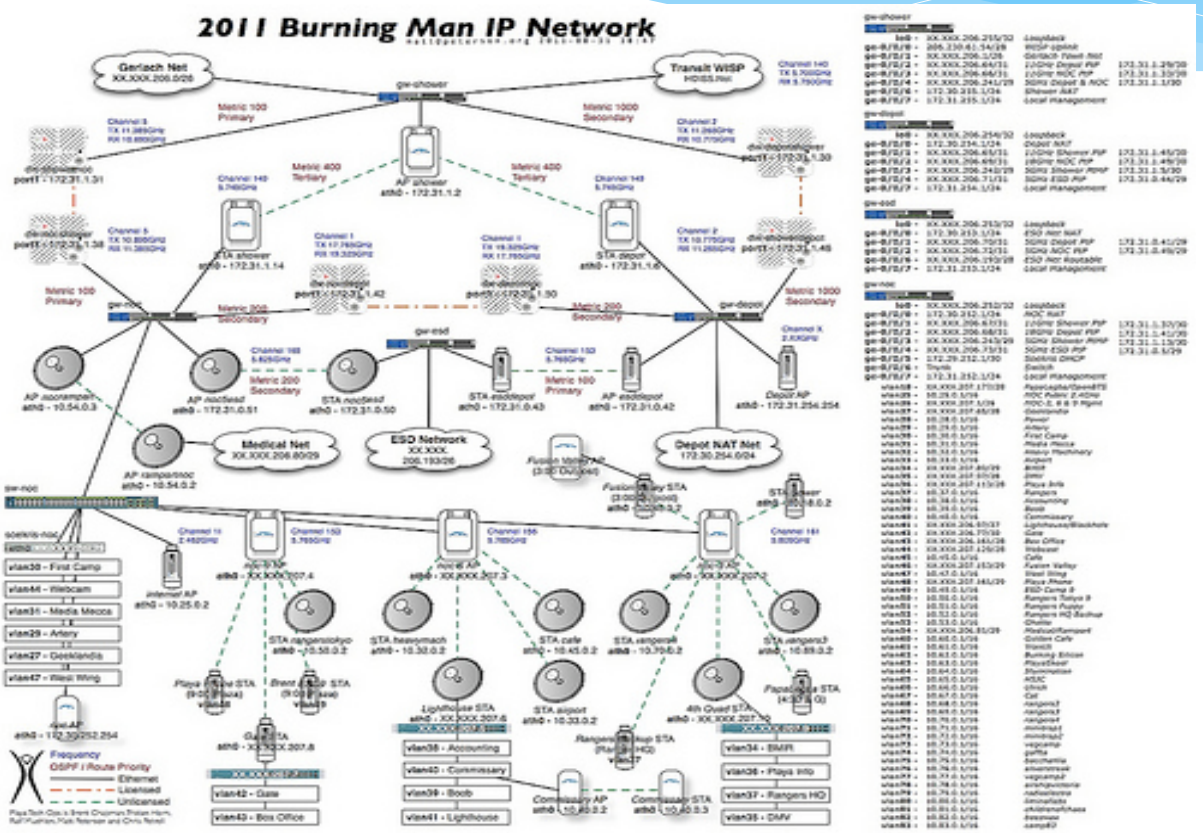
Network Diagram



Network Diagram



Network Diagram



Workgroup vs. Homegroup vs. Domain

In a workgroup:

* All computers are peers; no computer has control over another computer.
* Each computer has a set of user accounts. To log on to any computer in the workgroup, you must have an account on that computer.
* There are typically no more than twenty computers.
* A workgroup is not protected by a password.
* All computers must be on the same local network or subnet.

In a homegroup:

* Computers on a home network must belong to a workgroup, but they can also belong to a homegroup. A homegroup makes it easy to share pictures, music, videos, documents, and printers with other people on a home network.
* A homegroup is protected with a password, but you only need to type the password once, when adding your computer to the homegroup.

Source: http://windows.microsoft.com/en-us/windows7/what-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup

Workgroup vs. Homegroup vs. Domain

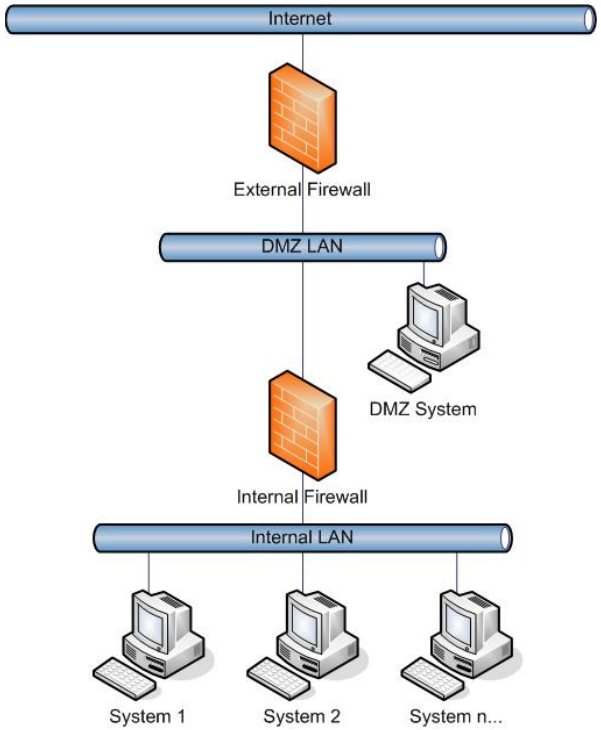
In a domain:

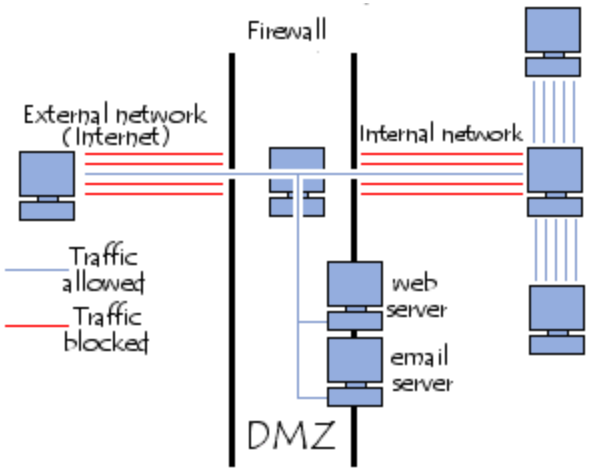
* One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers. Domain users must provide a password or other credentials each time they access the domain.
* If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer.
* You probably can make only limited changes to a computer's settings because network administrators often want to ensure consistency among computers.
* There can be thousands of computers in a domain.
* The computers can be on different local networks.

Source: http://windows.microsoft.com/en-us/windows7/what-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup

DMZ

DMZ


Internet
External Firewall
DMZ LAN
DMZ System
Internal Firewall
Internal LAN
System 1
System 2
System n...


Firewall
External network
(Internet)
Internal network
Traffic
allowed
Traffic
blocked
web
server
email
server
DMZ

LAN Environment Audit Concerns

An IT audit should review the following, at the minimum, in a LAN-based environment:

- Unauthorized use and access to the LAN
- Ability to diagnose and repair problems
- Reliability of the LAN
- Traffic capacity of the LAN, including room for growth
- Data backup procedures to ensure that important data will still be available should file servers encounter problems.

LAN Environment Audit Concerns

* Security Administration is especially important to review.
* LAN growth resulted in LAN administrators with centralized administration responsibilities regarding access, storage, and control over user programs and data files.
* Security administration is often combined with other administrative tasks, which may mean a relative lack of attention to security since the LAN administrators usually have a great deal of other work.

Networking Risks

* Organizations have built systems and applications that rely on networking almost all of the computers in the organization
* Companies have also increased the reliance on telecommunications and networking for daily business communications
* Extensive use of telecommunications and the Internet have introduced additional security and control risks

Auditing Networks

* Networks are a critical risk area for most companies and need to be frequently audited. It is important for auditors to first understand how networks function and then assess the overall risk to the organization.
* Network audits should be carefully planned with a focused scope to efficiently/effectively review the high risk factors. Networks can be implemented with many choices of hardware and software technology. The choices are a matter of organization goals, cost/benefit analysis, and availability.

Unauthorized Access to Applications and Data

Through various weaknesses in the network, networked computers, applications and user policies, our organizations are susceptible to:

* Trojan Horses - programs that do more than you think they do
* Viruses - programs that place nefarious code on your computer and are carried to other computers
* Macro - prewritten application program commands that get activated without your knowledge or consent when you start a program
* Attachments and downloads - programs that you intentionally download that misbehave. These programs might be Trojan horses or infected viruses
* Social engineering - convincing a human you are not who you really are convincing a human to perform a task for you on your behalf such as divulge a lost password.
* Uploading and unauthorized distribution - employees sharing data or programs with non-employees or other employees.

Denial Of Service Attacks

* Denial of service (DoS) attacks will flood a network or application with more transaction requests than the network or application can handle. The sheer volume of transaction requests will cause one or more of the following things to happen:
  * The server will crash or be so overloaded that legitimate transaction response time slows to a crawl.
  * The networking software (firewalls, routers) might crash because of the overload in traffic.

Denial of Service Attacks

* The result of a DoS attack is that legitimate users are unlikely to be able to receive service.
* DoS is a distributed denial of service attack. The difference between the two is that a DoS originates from a single network location, and a DoS originates from many network locations.
* To bring about a DoS, a hacker will attempt to place a zombie program on hundreds or thousands of machines. The zombie program is designed to awaken itself at a specific time (on all of the machines) and begin to generate the DoS attack on the target web site.

Control Objectives

- Protect your electronic domain.
- Do not allow a person on the Internet to learn about or have access to any resources on your machine.
- Protect access from outside your domain.
- Do not allow anyone to pass through, or learn about or access any resources on the network to which you are connected.
- Understand where all of the network access points are installed, and how they are controlled.

Control Objectives

- Ensure that adequate monitoring of network traffic is taking place - a surprising number of organizations are not doing so - or you won't know whether people are breaking in.
- Have a clearly stated banner at all gateways to your internal network and applications so trespassers can't claim they thought it was part of the web site. Ensure an adequate firewall is placed between your company's network and the Internet.
- Ensure an adequate firewall is placed between your organization's network and its extranets.
- Ensure employees have awareness and acknowledgement of network security policies and procedures.