Computer Networking Course - Network Engineering (CompTIA Network+) Part 9

Introduction to wireless standards

CSMA/CA

- all wireless Ethernet standards employ an algo called CSMA/CA
- a CSMA/CA nw involves a method of transmission that avoids packet collisions. It differs from a CSMA/CD type of nw which is about how to transmit after a collision has occurred.

Frequency modulation

- is the process used to encode data into a carrier wave
- 802.11 uses two main frequency modulation methods

Orthogonal frequency-division multiplexing (OFDM)

- is a frequency division multiplexing scheme that uses multiple sub-carrier channels to carry data
- is used to mitigate against attenuation (loss of signal strength over distances) and multipath issues that exist in nwing

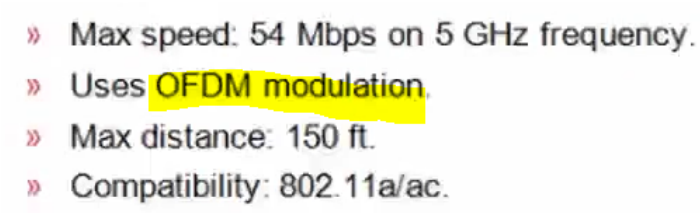
Direct-sequence spread spectrum (DSSS)

- is a modulation technique that uses spread spectrum technology to affect data transfer
- is used to mitigate the problem of multiple users on a channel and for effective timing between the transmitter and receiver

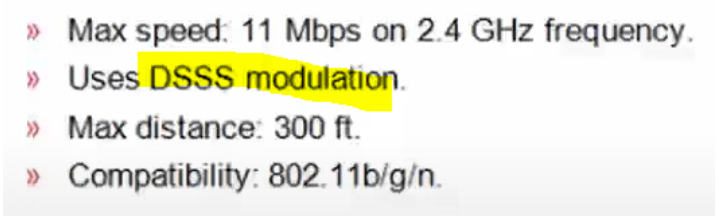
Wireless standards

- Wireless nwing standards are established by the 802.11 committee of the IEEE.
- the term Wi-Fi is actually a reference to the Wi-Fi Alliance, which is responsible for certifying that wireless nwing equipement actually meets the 802.11 standards. It has become synonymous with the WLAN in the English language.

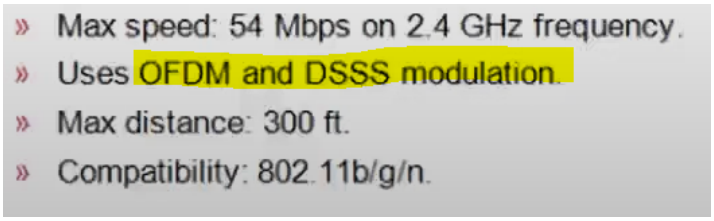
802.11a



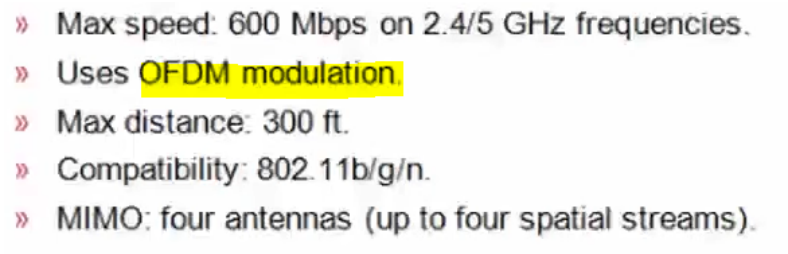
802.11b



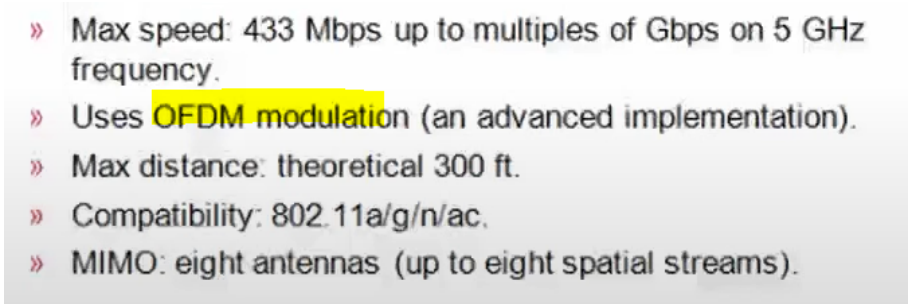
802.11g



802.11n



802.11ac



Note:

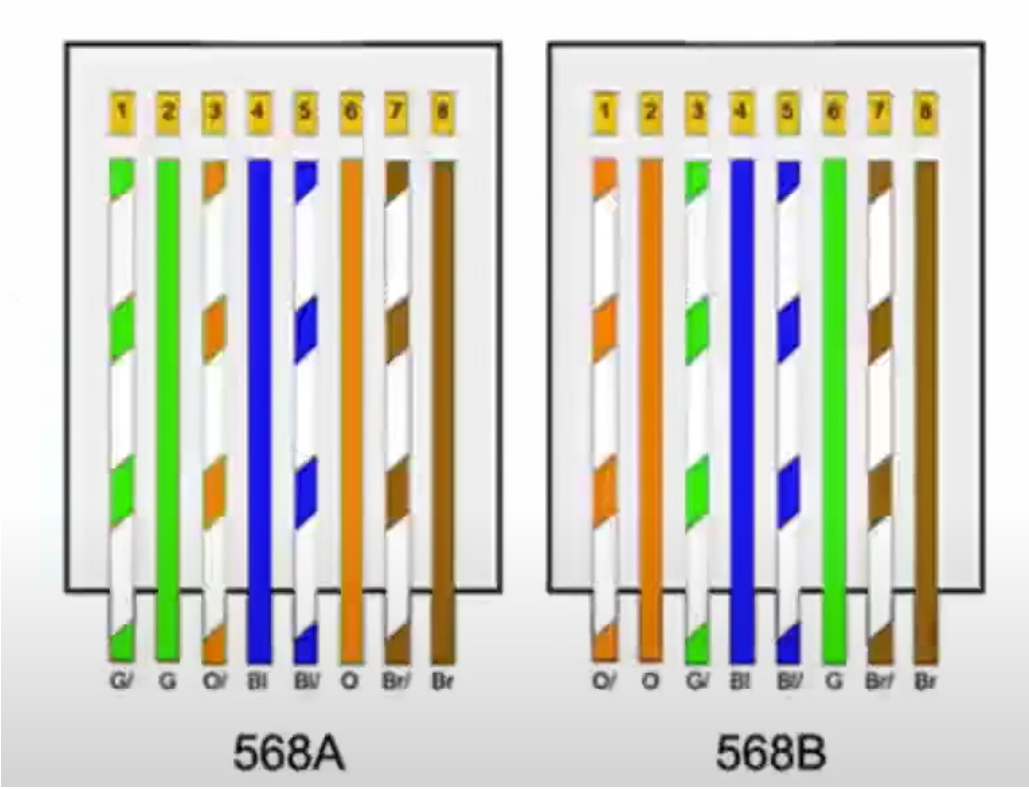
- Each standard has a theoretical max throughput.
- MIMO is used to increase throughput and to reduce weak spots or dead zones in a wireless nw.

Introduction to wired network standards

TIA/EIA 568A and TIA/EIA 568B

Twisted pair wire standards

- there are 2 twisted pair cable pinout standards that are regulated by TIA/EIA (telecommunications industry association/electronic industries alliance). The pinout standards specify the ordering of the wires to ensure that proper nwing communications can take place
    - TIA/EIA 568A (T568A)
    - TIA/EIA 568B (T568B)

- 

- all modern Ethernet nws that utilize unshielded twisted pair (UTP) or shielded twisted pair (STP) use the TIA/EIA standards.

Common tools used with twisted pair cable

Wire strippers

- used to remove the insulating jacket from the cable

Crimping tools

- used to secure wires into modular connectors

Punchdown tools

- used to secure wires into a punchdown block

Cable testers

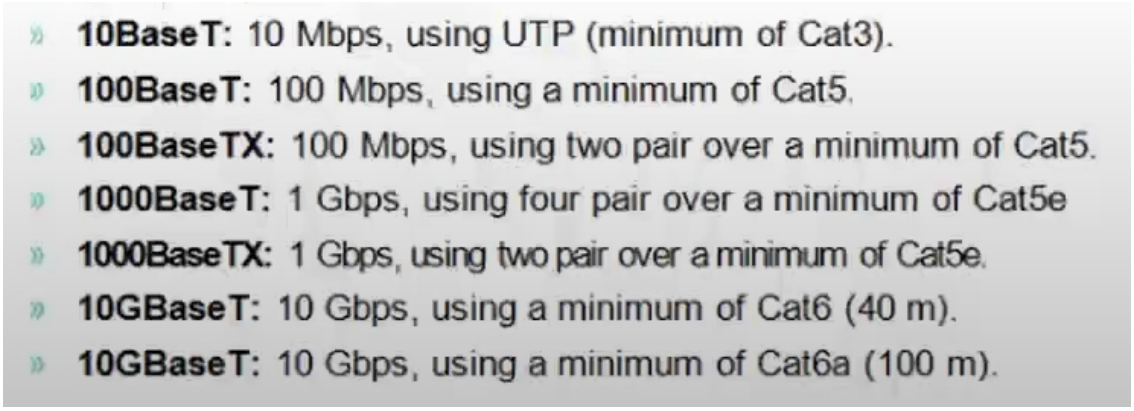
- used to test the integrity of a nw cable

Ethernet Standards

Distance limitations

- twisted pair is limited to 100 m without a repeater, unless otherwise stated
- coaxial LAN is limited to either 185 or 500 m, depending on the coaxial cable that is used
  - 10Base2: 10Mbps, using RG-58, limited to 185m
  - 10Base5: 10Mbps, using RG-8, limited to 500m
- Fiber optic LAN transmission is limited by the cable used, current max is over 40km over **single-mode optical fiber (SMF)**

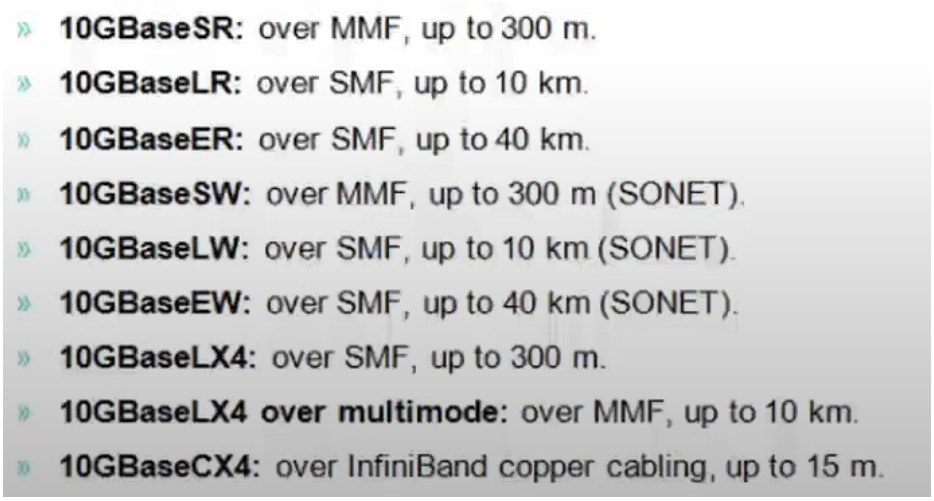
Twisted pair cable

- 

Multi-cable standard

- 1000BaseX
  - 1000BaseSX: 1 Gbps over short distance **multimode fiber optic (MMF)** (less than 2 km)
  - 1000BaseLX: 1 Gbps over long distance SMF (greater than 2 km)
  - 1000CX: 1 Gbps over coaxial cable up to 25 m

10 gigabit networking



Other standards

DOCSIS (Data over cable service interface specification)

- to provide the interface requirements for data transmissions over a broadband cable nw
  - to achieve the best performance when using broadband cable, the cable modem should meet the highest DOCSIS standard used by the cable provider
- the most current standard is DOCSIS 3.1, which allows for up to a theoretical maximum download speed of 10 Gbps with a theoretical upload speed of 1 Gbps

IEEE 1905.1-2013

- defines a nw enable (or device) that is used to create a convergent home nwing env that includes different types of wired and wireless nws
  - the standard also includes Ethernet over power line, which is using the existing electrical wiring in a structure as the media to transport data
  - also includes Ethernet over HDMI, which is using an HDMI interface and cable to transport nw traffic

Security policies and other documents

Security policies

- Policies: a set of guidelines, established by management, that are used to set the expected behavior in the workplace
- Procedures: the set of steps required to be taken in a given situation

Consent to monitoring

- A policy that established the employer's right to monitor the employee's actions and communications, which include:
    - monitoring emails
    - monitoring or recording of phone conversations
    - monitoring activities on computers, drives and phones
    - in highly secure work env, it may also include the video monitoring and recording of normal work activities

Clean desk policy

- a policy that is concerned about the handling of sensitive data
    - should not left unattended in a workplace and should be put away when not in use
    - includes the computer desktop; sensitive data should not be left easily accessible on the PC

Recording policy

- restricts the use of cameras, tape recorders, portable storage devices, or any other device that may be used to record or copy sensitive workplace info

Equipment access policy

- a security policy that establishes who has access to which equipment and when. could include access to:
    - server rooms
    - wiring closets
    - nw racks

Handling of user or customer information

- how to secure sensitive employee and customer info
    - user and customer info is a major target of hackers when they breach computing systems. The loss of control of this data can severely damage a company.

Note

- any policy that is used to help secure the workplace or company data is, by default, a security policy

Other documents

AUP (Acceptable use policy)

- a set of rules and guidelines established by the creator, owner, or administrator of info sys that detail what users may or may not do with that info sys.
    - is considered to be a part of the security policy
    - should be fairly detailed in what is allowed or not allowed to occur
    - all users should be required to sign the policy and these records should be kept on file

Network policies

- a broad range of policies that establish the guidelines for the nw, include policies that control the use and operation of the nw, as well as how to implement changes to it
    - many security policies may fall under the general nw policies category

Standard business documents

Memorandum of understanding (MOU)

- an agreement between two or more organizations that details how those organizations are to undertake some common course of action
    - often used before a legally binding agreement has been created
    - sometimes it is called **a letter of intent (LOI)**

Statement of work (SOW)

- a detailed document that specifies what work is to be performed, the expected outcome or deliverables, and the timelines to perform the work
    - plays an important role in project management documentation

Master license agreement (MLA)

- a legal agreement between 2 entities in which one agrees to pay the other for the use of a specific piece of software (or software package) fir a specified period of time

Service level agreement (SLA)

- an agreement that details the allowable amount of response time the vendor has to resolve an issue or problem
    - most commonly is associated with a service contract

Introduction to safety practices

Electrical safety

Electrical grounding

- is used to protect technicians in the case of electrical insulation failure
    - provides an alternate path for the electricity; is often referred to as a return to earth
- all electrical sys should be connected to properly grounded circuits

ESD (electrostatic discharge)

- is caused when 2 electrically charged objects that have different amounts of electrical charge come into contact, creating a flow of energy between the objects as they normalize the levels
    - can damage sensitive components, particularly the CPU and/or RAM
- using an ESD mat helps to reduce the chances of ESD
- using an ESD strap will also reduce the chances for ESD
    - the strap goes around the wrist and then is clipped to a ground source (usually to an exposed metal surface inside of the case)

Practice self grounding

- is a normalization tech used to equalize the amount of electrical charge between the worker and the equipment being worked on
    - after the case has been opened and the ESD strap is attached to a ground source, touch an exposed metal surface inside the case (before actually touching any of the components)

Additional equipment grounding

- in some cases, actually attaching a ground strap from the piece of equipment to a ground source is advised

Electrical fire safety

- in case of fire:
    - unplug the power source or turn off the circuit breaker
    - use a class C or multiclass fire extinguisher
    - never use water

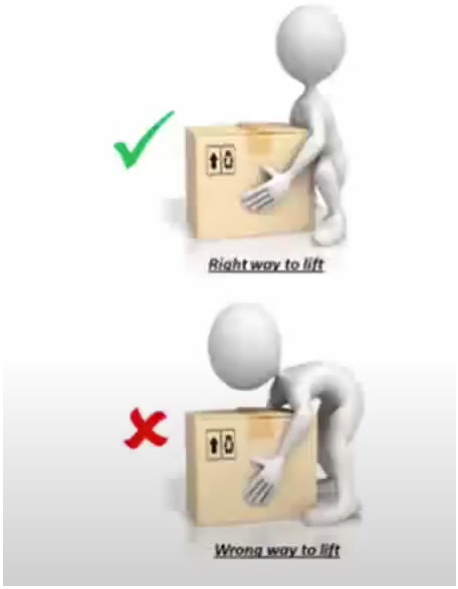
Fire suppression systems

- building codes often call for the installation of fire suppression systems. There are several different types of common systems:
    - **Wet pipe**
        - the pipes are pressurized and contain water
    - **Dry pipe**
        - are not pressurized; water is contained in a holding tank
    - **Pre-action**
        - similar to a dry pipe sys, but the sprinkler head contains a thermal-fusible link that must melt before the water is released
    - **Deluge**
        - designed to release a large amount of water in a short amount of time into a predefined space
        - least desirable option for electrical components

- **Halon(卤化烷)**
  - a non-conducting volatile gaseous chemical
  - works by chemically disrupting combustion
  - not leave a residue upon evaporation; unlike water, halon will not ruin electrical components
  - safe for exposure to humans in limited amounts for a limited amount of time
  - environmentally safe, also known as a **clean agent**

Installation safety

User proper lifting techniques

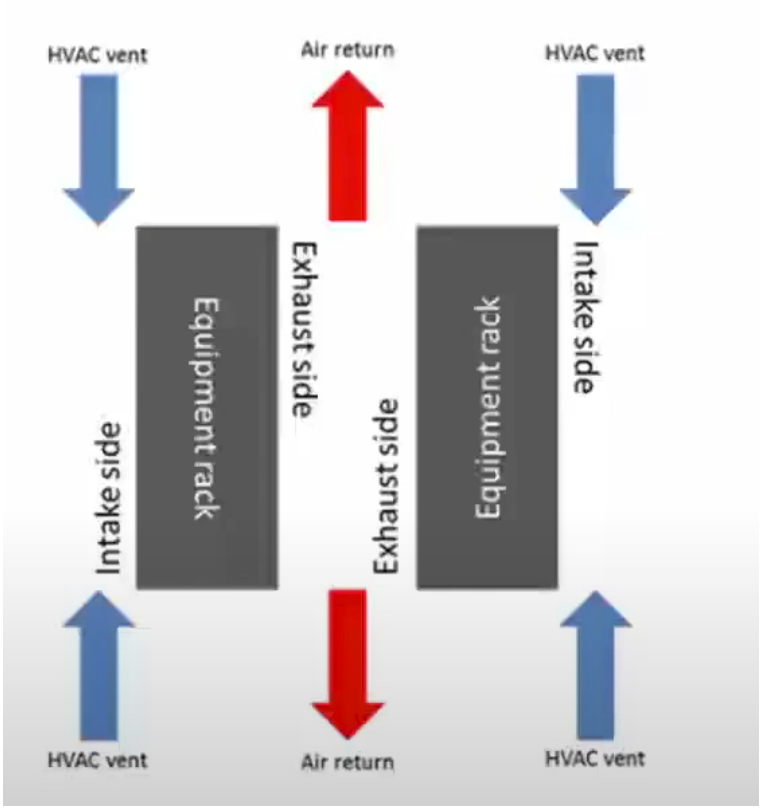
- » Bend at the knees, not the waist.
- » Keep the head up.
- » Avoid twisting when carrying items.
- » If the item is heavy or awkward, request help in lifting it.
  - Most companies establish weight limitations.
- 

Rack installations

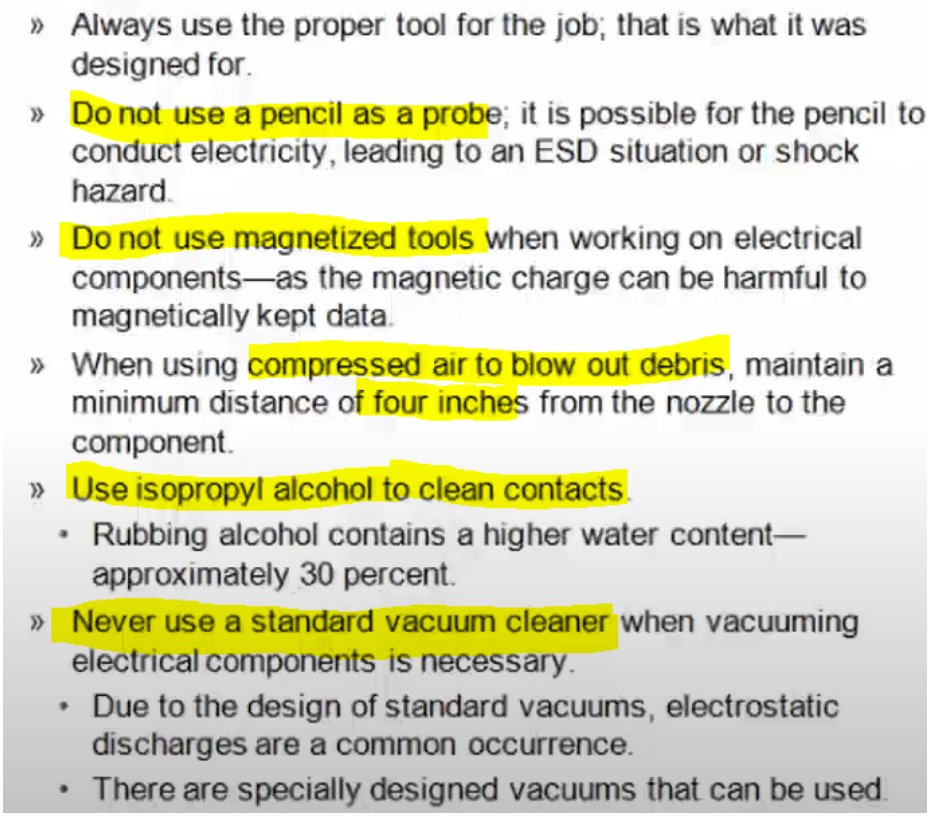
- » Racks are used to help create a clean organized environment.
  - Especially when used with proper cable management techniques.
- » Racks are designed to provide sufficient airflow for the electrical components that are placed in them.
- » When assembling and installing racks, always follow the manufacturer's instructions.
  - Always use the proper tools to prevent damaging the racks or the fasteners that hold them together.
- » Many servers and networking components come rack ready—specifically designed to be placed in a rack.

Rack placement

- » When designing a room that is going to hold multiple racks of computing systems (e.g., servers and networking gear) some thought needs to go into the placement of those racks.
- » HVAC and rack placement should be done concurrently.
  - HVAC systems should be designed to control both heat and humidity levels.
- » Creating a hot aisle/cold aisle design is recommended.
- » The hot aisle is the side or aisle that receives the exhaust airflow from the computing equipment.
  - The aisle should face an HVAC air intake.
- » The cold aisle is the side or aisle that the air intakes of the computing equipment face.
  - The aisle should face an HVAC air vent.
- » Whenever possible, a server room should be designed with a raised floor to help protect against water damage.
  - The raised floor, like a drop ceiling, can also be utilized as part of the cable management system.



Tool Safety

- 
  - » Always use the proper tool for the job; that is what it was designed for.
  - » Do not use a pencil as a probe; it is possible for the pencil to conduct electricity, leading to an ESD situation or shock hazard.
  - » Do not use magnetized tools when working on electrical components—as the magnetic charge can be harmful to magnetically kept data.
  - » When using compressed air to blow out debris, maintain a minimum distance of four inches from the nozzle to the component.
  - » Use isopropyl alcohol to clean contacts.
    - Rubbing alcohol contains a higher water content—approximately 30 percent.
  - » Never use a standard vacuum cleaner when vacuuming electrical components is necessary.
    - Due to the design of standard vacuums, electrostatic discharges are a common occurrence.
    - There are specially designed vacuums that can be used.

The MSDS (material safety data sheet)

- MSDSs contain safety info on materials and chemicals found in the workplace, contain all known health issues associated with a particular material, outlines what protective measures must be taken to reduce risks from exposure and what actions must be taken if the chemical is ingested.
- also detail the physical properties of the material and the proper steps to take when disposing of it.

Emergency preparations

- these preparations should be detailed in a set of emergency procedure documents. The procedures should contain escape plans, including where employees will meet to ensure that all are accounted for, info on the types of fire suppression sys that are present, as well as what steps have been taken to increase the day-to-day safety in the workplace.

Building layout considerations

- All walls should have a minimum two-hour fire rating.
  - This is the amount of time it takes for a fire to burn through the wall.
- Exterior doors and other secure doors must be designed to resist forcible entry.
  - The doorways should also be designed to be able to handle the amount of expected traffic in an emergency.
- Fire suppression systems should be appropriate for the types of assets they are protecting.
  - A wet pipe system is not appropriate for a server room or data center. However, a Halon system may not be the correct one for an open cubicle area.
- Backup power should also be incorporated into the building layout.
  - Not all areas are going to require backup power, but for some it is going to be essential.

Escape plans

- Each area or room should have an escape plan map posted in a prominent area (ideally, by the main access doorway into that area) that shows the preferred route out of the facility.
  - The map should also include the meeting area outside of the danger zone; this allows for supervisors or managers to account for all personnel.

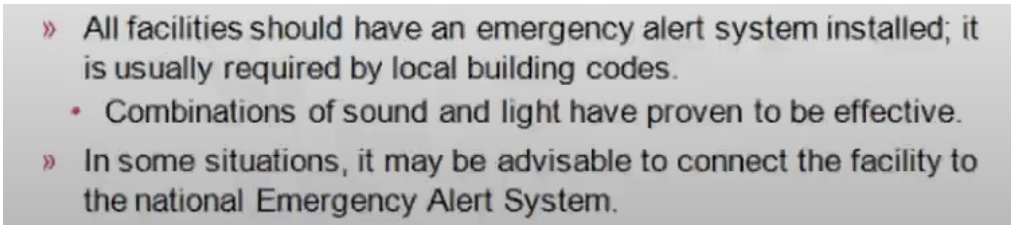
Safety or emergency exits

- Should be clearly marked.
  - Should also be well lit, with independent battery power sources.
- Should be wide enough to handle the expected traffic.
- Should always be kept clear of obstructions.

Fail open or fail close

- What happens to doors with electronic locks when the power is out needs to be considered.
  - Fail close: the locks engage—suitable for keeping secure areas secure in an emergency.
  - Fail open: the locks disengage—suitable for non-secure areas, or for areas where two-way traffic is going to occur in an emergency.
- In many facilities, fail close type fire doors are used. The doors are kept in an open position—kept open by electromagnets. Once the fire alarm has been tripped or the power is cut, the doors close.
  - They usually do not lock when closed, but are used to help slow the spread of fire or other dangers.

Emergency alert systems

- 

Rack and Power management

Rack management

- Rack systems are specially designed racks used to hold nwing and computing equipment. Sometimes are referred to as server racks.
- The rack systems follow one of several different designs, however, they all follow the same height specification.
    - the specification is the standard unit (U) and it involves the amount of vertical space that can be used to hold equipment.
    - A U = 1.75 inches.

Types of racks

- are normally two-post or four-post racks
- server rail racks have slide mounts to make it easy to pull out servers to perform necessary maintenance

Device placement

- devices that generate the most amount of heat, or are not heat sensitive, should be placed toward the top of the rack
- all equipment cold air intakes should face the same direction; exhaust outlets should face the same direction (i.e., host aisle/cold aisle)

Airflow

- when mounting equipment in racks, vertical space should be left between the equipment to promote adequate airflow
- when multiple rows of racks are implemented, a hot aisle/cold aisle approach should be used to promote proper airflow and cooling

Rack monitoring

- racks should be monitored for environmental factors to help ensure the health of the servers and other equipment
    - monitors should be in place for: temperature, humidity, vibration, water leaks, smoke and intrusion

Rack security

- most rack systems do not come with rack security in mind, but it can be easily added after rack installation
    - rack doors can be added that have either keyed or electronic locks
    - 

Power management

- It is important to know the power requirements and loads for all of the equipment that will be in place. This helps to ensure that the proper electrical circuits are installed, so that sufficient power is delivered where it is needed.

Power converters

- convert electrical energy from one form to another
- **power inverters:** specifically **converts voltages DC to AC**

UPS (uninterruptable power supply)

- uses power converters to receive electrical current from an AC electrical source and pass it to a battery for storage
- uses power inverters to receive DC current and pass it to another devices as conditioned (well regulated) AC flow
- used to provide a steady stream of conditioned electrical power to components
    - helps to protect sensitive electrical components from power anomalies (e.g., power spikes or power sags)

Power redundancy

- critical components should include redundant power supplies
    - if one of the power supplies fails, the other one takes over immediately

Cable management

Cable distribution

Main distribution frame (MDF)

- the location where the demarc, demarc extension, main switch/router, and patch panel are placed
- the MDF is where outside traffic enters a location and then is distributed to the internal nw

Intermediate distribution frame (IDF)

- a location's solution when a single MDF is not sufficient
- usually in a multistory building
- the IDFs are connected to the MDF by vertical cross-connect (VCC) cables
- it is common for an MDF to contain separate IDF panels for each floor of a building

VCC (vertical cross-connect)

- the main patch panel for a location.
- usually resides in the same location as (or very close to) the demarc and main switch/router

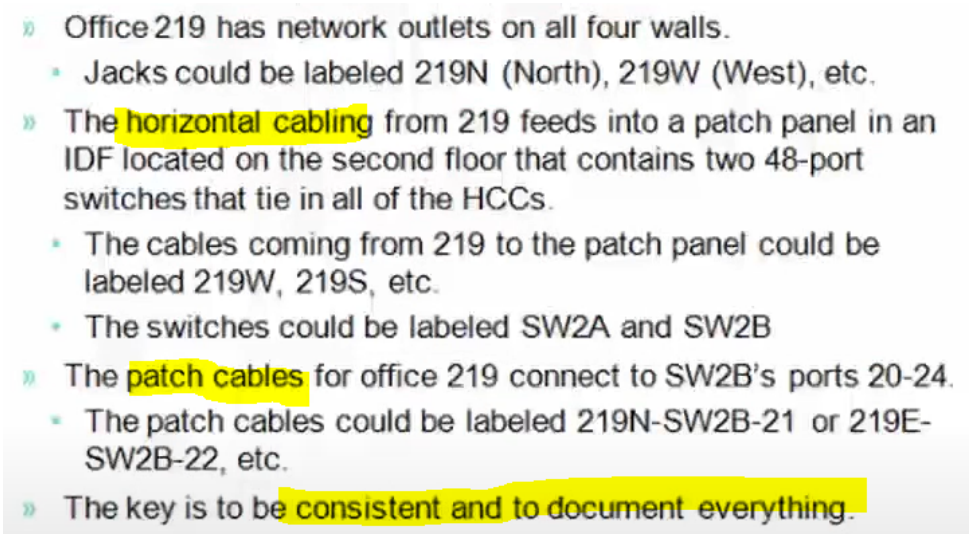
Patch panel

- used to terminate nw cable runs, usually within a building (from the wall jacks to a central location)
- used to organize and administer the physical aspects of the nw cables
- nw runs are punched down to the back of the patch panel (normally a 66 or 110 block) with an associated port on the front of the patch panel
- patch cables are used to connect the patch panel ports to nwing gear
- workstations connect to a patch panel using horizontal cabling; this location is called the **horizontal cross-connect (HCC)** and is usually located in the IDF. Switches may or may not be present
    - if a workstation needs to be relocated to a different switch, all that needs to be done is to make a change in the location of the patch cable

Cable management components

- Labeling is an important part of cable management. It can cause stress when working with nws, but it doesn't have to.
- the key to **proper labeling** is to create a naming convention that makes sense for the situation. Proper labeling will ease the management of the physical aspects of the nw, especially when dealing with cables.

Naming convention example

- 

Cable trays

- masses of cables can block airflow and act as an insulator that allows for excessive heat to build up
- cable trays are used to organize cabling and to keep it away from areas where cabling may cause heat buildup

Basic of change management

The reason for change management

- It is quite possible that a single change will have a ripple effect on the whole system. Change management processes are used to introduce changes to a system in a controlled manner to minimize possible disruptions and potential pandemonium(骚动).

Different change management processes

Document the reason for a change

- proposed changes should have a solid reason for occurring
    - a best practice is to include why the change is needed for IT reasons and also for business reasons
- as the change proceeds through the process, more documentation may be added to the reasons for a change

Change request

- a formal change request procedure is used during the approval process and should include several other subdocuments that can be used to gain approval
- **Configuration procedures**
    - document the exact steps required to implement the change, including affected devices, applications, and processes

- **Rollback process**
  - as all change carries risk, a plan to reverse change is required
- **Potential impact**
  - a good-faith effort to identify all possible impacts to the overall sys, both the positive and the negative
- **Notification procedures**
  - after the potential impacts have been identified, the people responsible for the affected sys must receive notification of the proposed change

Approval process

- » Proposed changes should be vetted and approved, not only by management, but also senior IT personnel, security experts, and a selection of those affected by the change.
- » Some companies create change control boards to, not only evaluate proposed changes, but to also:
  - Implement a means of approving changes.
  - Assure that all approved changes have been fully tested and documented.
  - Meet periodically to assess the status of an approved change—to help keep it on track for implementation.
  - Maintain responsibility for the change and verify that the process is proceeding according to the configuration procedure.
  - Help ensure that approved changes are implemented correctly.

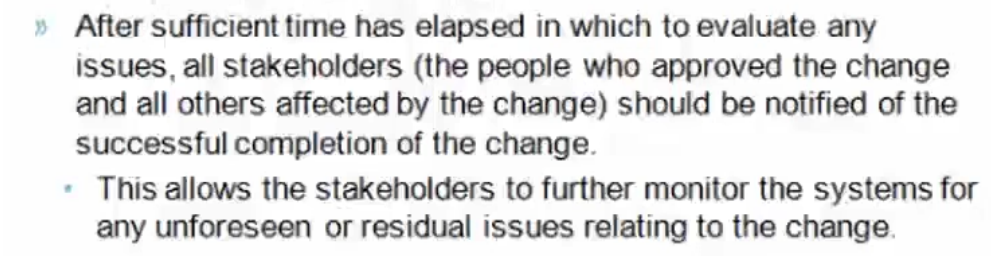
Maintenance window procedure

- » A maintenance window is the amount of time that a system will be down or unavailable during the proposed change.
  - Before the final schedule is developed, an evaluation of all affected systems must be performed with particular attention paid to mission critical systems.
  - It is possible that the proposed maintenance window may exceed the allowable downtime for critical systems, which will affect when the maintenance window can be scheduled.

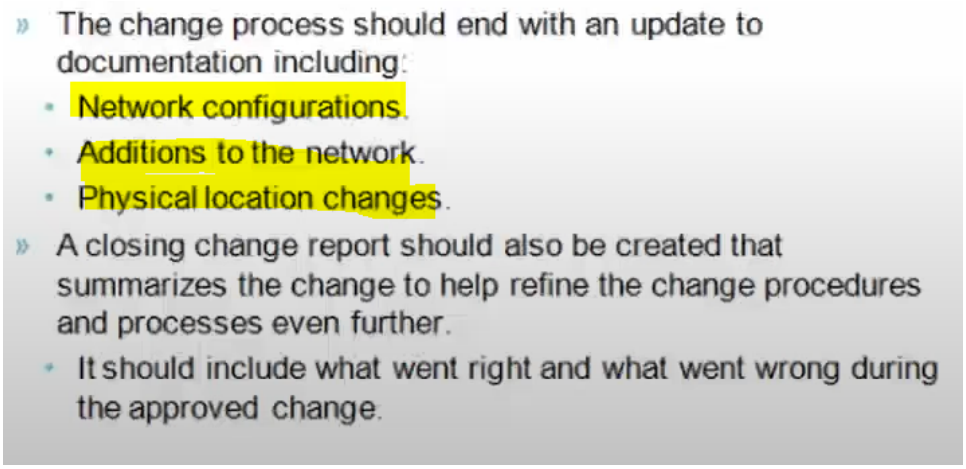
Authorized downtime

- » Once the maintenance window has been identified, it is then possible to determine the optimum time to implement the change.
  - In many cases, system changes need to occur during off-hours (e.g., after the close of business or during weekends).

Notification of change

- 
  - After sufficient time has elapsed in which to evaluate any issues, all stakeholders (the people who approved the change and all others affected by the change) should be notified of the successful completion of the change.
    - This allows the stakeholders to further monitor the systems for any unforeseen or residual issues relating to the change.

Final documentation

- 
  - The change process should end with an update to documentation including:
    - Network configurations.
    - Additions to the network.
    - Physical location changes.
  - A closing change report should also be created that summarizes the change to help refine the change procedures and processes even further.
    - It should include what went right and what went wrong during the approved change.

Common Network Protocol

TCP and UDP

- both are L4 protocols, responsible for the delivery of nw data between nodes

TCP (transmission control protocol)

- *reliable* delivery method
- ensures that all packets are received
- uses ACK as a means of error correction
- establishes flow control to reduce error rate and ensure proper delivery

UDP (user datagram protocol)

- *best effort* delivery method
- sends data, but not care if the packets are all received
- no error correction
- speed and low nw overhead is what concerns UDP

Common ports and protocols

HTTP (Hypertext transfer protocol)

- the primary protocol used to transfer data over the Internet
- assigned to **port 80**

HTTPS (Hypertext transfer protocol secure)

- the primary protocol to securely transfer data over the Internet using SSL or TLS technology. (SSL is no longer be used)
- assigned to **port 443**

NetBIOS (Network basic Input/Output system)

- originally developed to allow hosts to be able to communicate with servers
- assigned to **ports 137-139**

SMTP (Simple mail transfer protocol)

- used to transfer email from a client to an email server
- used to transfer email between servers
- assigned to **port 25**

POPS (Post office protocol v3)

- used by clients to retrieve email from servers. once engaged, POP3 downloads all messages from the servers. The user cannot access email messages until they have been downloaded
- assigned to **port 110**

IMAP (Internet message access protocol)

- used by clients to access email on email servers. allows the client to administer and organize email on the server into folders
- assigned to **port 143**

SIP (Session initiation protocol)

- most commonly used to set up and tear down multimedia communication sessions (e.g., a VoIP session uses SIP to establish and terminate the session)
- assigned to **ports 5060 and 5061**

RTP (Real-time transport protocol)

- commonly used to format and deliver multimedia or streaming content (e.g., RTP handles the flow of packets in a VoIP session after SIP has established the connection)
- assigned to **ports 5004 and 5005**

MGCP (Media Gateway Control Protocol)

- defines the means of communication between a packet switched nw and circuit switched nw (e.g., the PSTN). It can be used to set up, maintain, and terminate calls between multiple endpoints (e.g., teleconferencing)
- assigned to **ports 2427 and 2727**

H.323

- provides a standard for delivering video over IP nws.
- defines how real-time audio, video, and data are to be transmitted
- provides signaling and bandwidth control
- assigned to **port 1720**

The difference between ports and protocols

Ports

- a method of specifying what protocol or service to access
    - protocols and services use default ports so they are easy to locate
- there are 65,536 ports available to be used for communication, but port 0 is reserved.
    - the first 1024 ports are specifically assigned and are called **well known ports**

Protocols

- can be thought of as the language that the two applications on either side of the connection agree to speak
- translate requests into services
- most protocols use pre-defined ports, but some protocols must be user configured

Note

- Ports are used to request services or applications.
- Protocols are the services or applications that are being requested.
- When a requestor seeks to connect to a specific port, the requestor is dynamically assigned a port number to listen to for the response. This also allows computers to have many concurrent connections.

Common ports and protocols

FTP (File transfer protocol)

- transfer files between computing systems; requires user authentication
- assigned to **port 20 and 21** (mostly uses port 20)

TFTP (Trivial file transfer protocol)

- transfer files between servers and clients; no user authentication required
- assigned to **port 69**

SNMP (Simple network management protocol)

- used to monitor and manage local area nws
- assigned to **port 161**

Telnet

- used for remote access to systems; is unsecure
- is a bidirectional terminal service
- assigned to **port 23**

SSH (Secure Shell)

- used to encrypt data traffic on a nw
- can be used in place of Telnet to provide a secure bidirectional terminal connection
- assigned to **port 22**

DNS (Domain name system)

- used to map computer names to their IP addresses
- assigned to **port 53**

DHCP (Dynamic host configuration protocol)

- used within nws to automatically configure computers with the correct IP configurations (e.g., IP address, subnet mask, default gateway, and DNS server location)
- **Requests** are assigned to **port 67**
- **Responses** are assigned **port 68**

RDP (Remote desktop protocol)

- used in Microsoft nws by remote desktop connection and remote assistance to make remote connections
- assigned to **port 3389**

SMB (Server message block)

- used to transfer files over a nw; the process is transparent to the user
- can be configured to run over NetBIOS on ports 137-139
- assigned to **port 445**