Computer Networking Course - Network Engineering (CompTIA Network+) Part 4

Configuring Switches

Unmanaged vs. managed switches

Switch basics

- most switches operate at L2 of OSI model.
- An **Application-specific integrated circuit (ASIC**) chip is used to make switching decisions in place of software.
  - allows sw to break-up collision domains
  - allows sw to run in full-duplex mode
  - allows sw to make faster decision than either bridges or routers
- When a sw receives a frame on a port, it makes some simple decisions based on its MAC table.
  - **Forward**: the frame is directed out the port
  - **Filter**: the frame is not directed out ports which are not associated with the dst MAC address
  - **Flood**: the frame is flooded out all ports if the MAC address is not in the MAC address table

unmanaged switch

- is a simple switch -- plug it in and it works. There is no method provided for configuration.
- is designed with ease of installation as its main attribute.

managed switch

- can be configured through command line or a browser based interface.
- provide high degree of nw customization and control.
- can be set up so that an administrator can monitor its performance remotely and use protocols such as **SNMP v3 (Simple Network Management Protocol)** to make some modifications to its configuration.

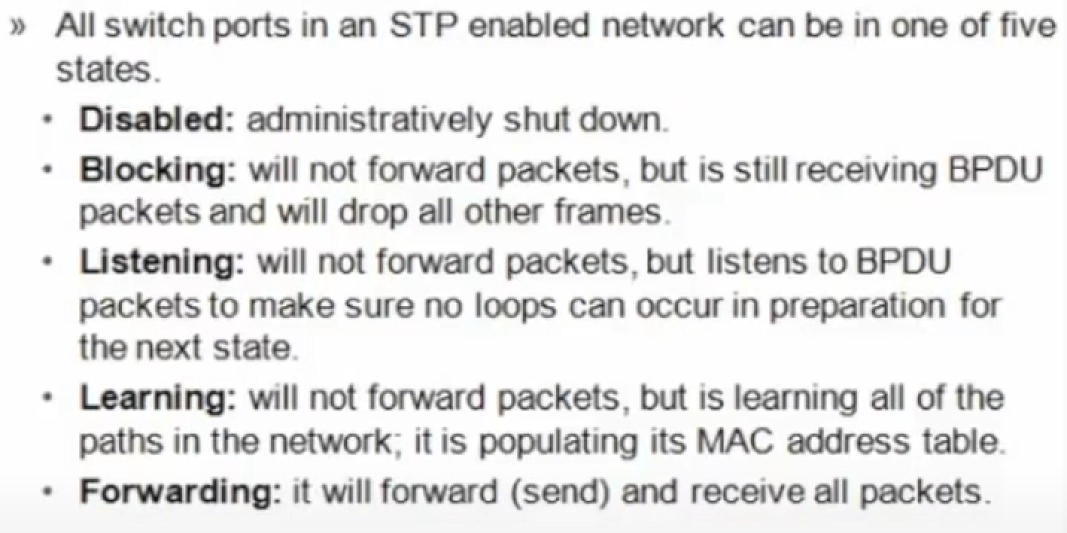
Spanning Tree Protocol (STP)

Loop avoidance

- a switching loop can occur on nw where there are multiple paths to reach dst MAC address.
- **DEC (Digital Equipment Corporation)** created the **STP** to reduce the possibility of switching loops.
  - The sw elect a root bridge to control the switched nw
  - the sw will shut down ports that are not the best path to the root bridge -- reduce the risk of loops

    - <u>no nw can flow</u> until after the STP process has taken place and a <u>stable state</u> has been achieved. This is called **convergence**, which can take a significant amount of time --- up to 50 seconds.
    - after convergence, the STP selected sw ports send out **Bridge Protocol Data Unit (BPDU)** packets to help <u>maintain the stable state</u>.

    ### STP port states

    - 

      » All switch ports in an STP enabled network can be in one of five states.
      - **Disabled:** administratively shut down.
      - **Blocking:** will not forward packets, but is still receiving BPDU packets and will drop all other frames.
      - **Listening:** will not forward packets, but listens to BPDU packets to make sure no loops can occur in preparation for the next state.
      - **Learning:** will not forward packets, but is learning all of the paths in the network; it is populating its MAC address table.
      - **Forwarding:** it will forward (send) and receive all packets.

- **802.1d**
    - the **IEEE version of STP**
    - all modern L2 switches run 802.1d by default
- The slow convergence time of 802.1d led to the creation of **Rapid Spanning Tree Protocol (RSTP)**, which is known as **802.1w**.
    - with RSTP enabled on all sw, a nw can <u>achieve its stable state in approximately 5 seconds.</u>
    - RSTP is not turned on by default on L2 sw.
    - 802. 1w defines <u>3 possible port states</u>:
        - **discarding**: the port may be administratively disabled or may be in a blocking mode or listening mode
        - **learning**: the port is populating its MAC address table in preparation for forwarding packets
        - **forwarding**: the port is actively forwarding packets

Installation considerations

VLAN (Virtual Local Area Network)

- <u>switches break up collision domains</u>, but not broadcast domains
    - VLANs take a single nw env and <u>create smaller nw segments by **subnetting** the nw address range</u>
- VLANs are used in a switched nw env for a variety of reasons
    - <u>break up broadcast domains</u> into smaller pieces
    - <u>increase security</u> by limiting access to nw resources
- the administrator configures the VLANs and assigns users, nodes, or ports to a specific VLAN

  - all managed sw do come with a **Native VLAN** --- which is determined by the manufacturer --- it is used to help manage the sw.
  - VLAN traffic is allowed to cross sw ports -- as long as the VLAN info matches -- through the use of **trunk ports**.
- **VTP (Virtual Trunk Protocol)** is a Cisco proprietary method of creating a virtual trunk port, which allows VLAN traffic to pass between sw and to automatically manage the VLAN env.
- a router or some other L3 device must be installed in order for different VLANs to communicate with each other.

Switch management

- sw may be managed **out-of-band** (no nw connection required)
  - through the use of the **console port** on the sw
- the console port is a specific port on managed sw used to connect to and configure or manage a sw
  - a rollover cable may be required to make the connection to the console port
- sw may be configured to be managed **in-band** (a nw connection is used to manage the sw)
  - one of the most common methods of allowed in-band management is through the use of **virtual terminals (VTY) connections**
- the most common VTY connections are telnet or ssh sessions.
- A **default gateway address** must be placed on an interface that belongs to the native VLAN (default VLAN) in order to allow for in-band sw management.
  - the default gateway on a sw is different than the default gateway on a router. On a sw, it is only used to manage the sw, not to pass other nw traffic.
- An administrator should configure which users and passwords are allowed to connect to the sw and what their level of access to the configuration is going to be.
- if **AAA (Authentication, Authorization, Accounting) protocols** are used in the nw, the sw must be configured to use them.

Configuring the switch port

Speed and duplexing

- most modern sw ports can auto-negotiate both the speed of the link and the duplexing mode used.

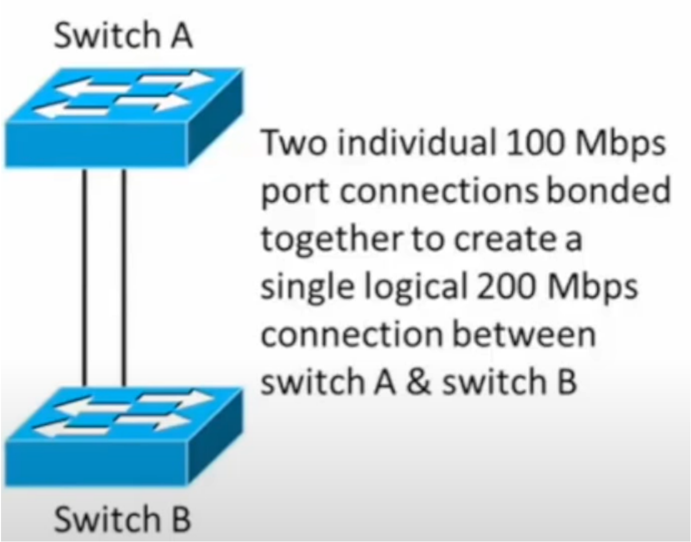
VLAN assignment

- all sw ports will belong to a VLAN, either an *administrator configured* one or the *native VLAN*.
  - the native VLAN can be administratively changed, which should be done to increase the security level of the sw.

Trunking

- sw ports that are designed to carry VLAN traffic between switches.
  - the standard protocol used is **802.1q**, which strips off the VLAN tag (actually changes the tag to the native VLAN) and allows the traffic to cross. Then the 802.1q port on the other side reinserts the original VLAN tag.

Port bonding

- **LACP (Link Aggregation Control Protocol)** is the protocol used to create a single logical channel from redundant connections between sw. This will increase the bw between the sw.
  - 

    Two individual 100 Mbps port connections bonded together to create a single logical 200 Mbps connection between switch A & switch B

PoE (Power over Ethernet)

- The PoE ports can use one of two methods to provide current over the nw cable as well as carry data, allowing the ports to power small nw devices, while at the same time communicating with them.
- the port itself may provide the current
- the port may allow the use of a *power injector* to provide the power instead of the port
- there are multiple PoE standards, the most common are:
  - PoE (802.3af)
  - PoE+(802.3at)

Port mirroring

- this allows the configured port to receive all nw traffic going to and from a specific port.
- is most often used in conjunction with a packet analyzer (e.g., a nw sniffer or packet sniffer)
- can create a significant amount of nw overhead, so it should be used sparingly on an active nw.

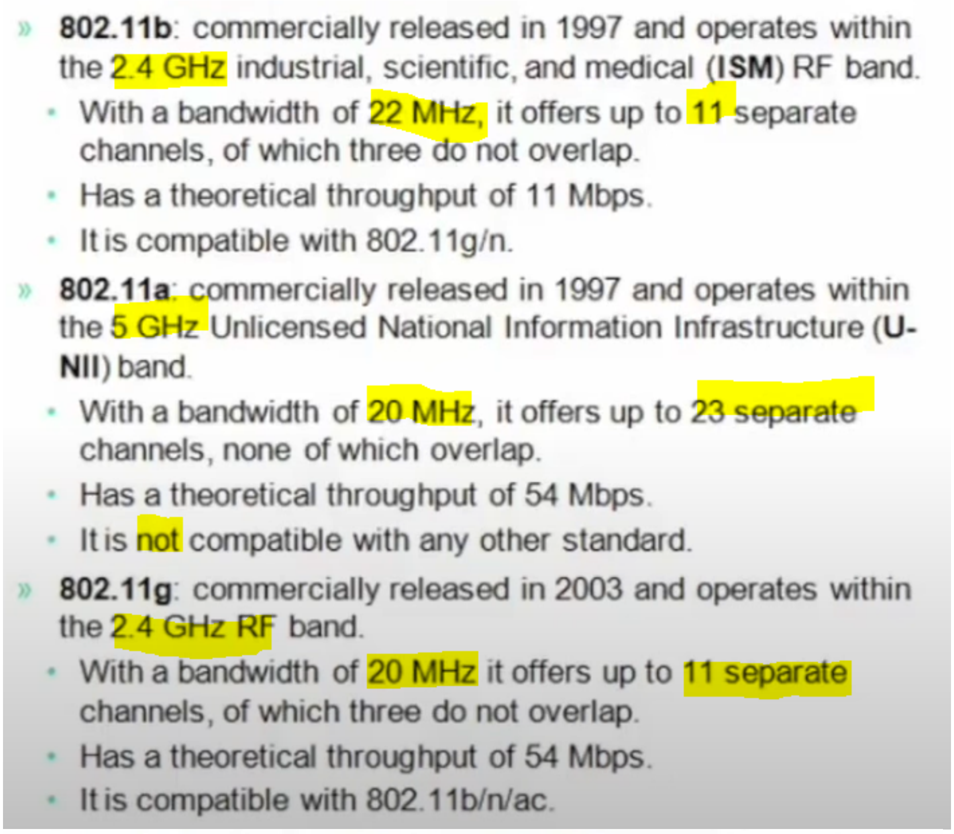
Wireless LAN infrastructure

Introduction to wireless network standards

Intro to IEEE 802.11

- A set of specifications at the L2 and L1 that establishes how wireless nw communication can occur.
  - specifies the use of unlicensed radio frequency (RF) bands as the carrier for nw traffic.
- specifies half-duplex nw communication through the use of **carrier sense multiple access with collision avoidance (CSMA/CA)** as the method of access.
  - CSMA/CA tech requires that devices only transmit data when no other data transmission signal is present on the carrier wave.

IEEE 802.11 standards



» **802.11b**: commercially released in 1997 and operates within the 2.4 GHz industrial, scientific, and medical (**ISM**) RF band.

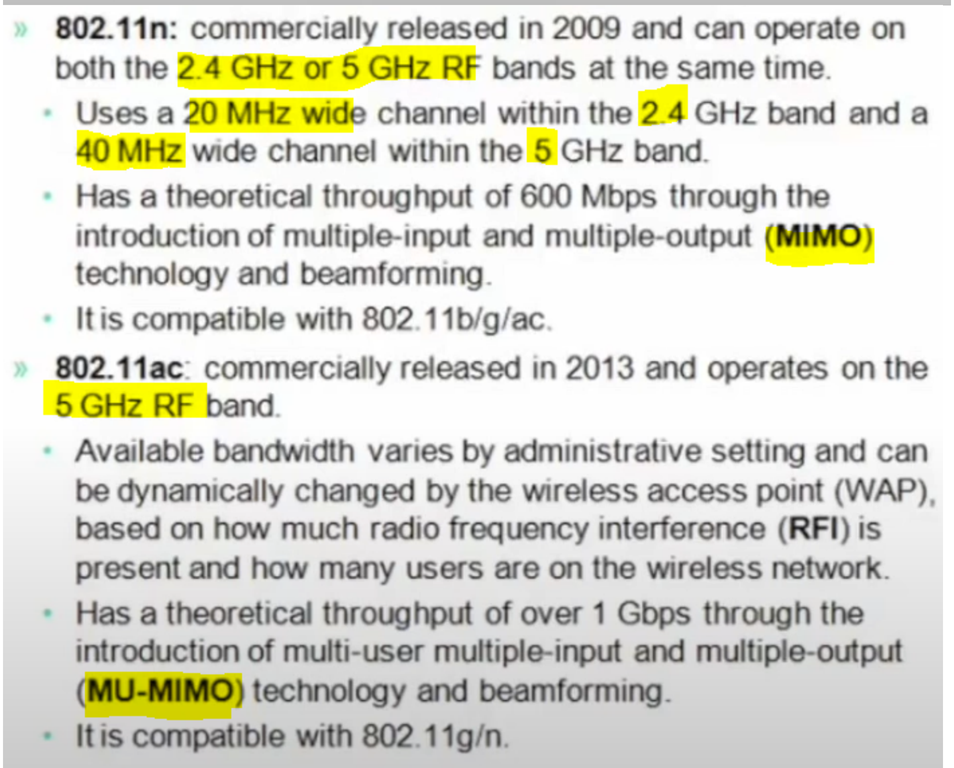
- With a bandwidth of 22 MHz, it offers up to 11 separate channels, of which three do not overlap.
- Has a theoretical throughput of 11 Mbps.
- It is compatible with 802.11g/n.

» **802.11a**: commercially released in 1997 and operates within the 5 GHz Unlicensed National Information Infrastructure (**U-NII**) band.

- With a bandwidth of 20 MHz, it offers up to 23 separate channels, none of which overlap.
- Has a theoretical throughput of 54 Mbps.
- It is not compatible with any other standard.

» **802.11g**: commercially released in 2003 and operates within the 2.4 GHz RF band.

- With a bandwidth of 20 MHz it offers up to 11 separate channels, of which three do not overlap.
- Has a theoretical throughput of 54 Mbps.
- It is compatible with 802.11b/n/ac.



» **802.11n:** commercially released in 2009 and can operate on both the 2.4 GHz or 5 GHz RF bands at the same time.

- Uses a 20 MHz wide channel within the 2.4 GHz band and a 40 MHz wide channel within the 5 GHz band.
- Has a theoretical throughput of 600 Mbps through the introduction of multiple-input and multiple-output (**MIMO**) technology and beamforming.
- It is compatible with 802.11b/g/ac.

» **802.11ac**: commercially released in 2013 and operates on the 5 GHz RF band.

- Available bandwidth varies by administrative setting and can be dynamically changed by the wireless access point (WAP), based on how much radio frequency interference (**RFI**) is present and how many users are on the wireless network.
- Has a theoretical throughput of over 1 Gbps through the introduction of multi-user multiple-input and multiple-output (**MU-MIMO**) technology and beamforming.
- It is compatible with 802.11g/n.

Beamforming

- once a device makes a connection to an **access point (AP)** that is capable of beamforming, the AP will *auto-tune* its antenna and transmitter to more specifically target the device when communication occurs. This can reduce RFI and increase throughput on the WLAN.

Antenna technology

The basics

- Antennas are used to broadcast and receive RF signals and they fall into 2 basic categories:
    - **omnidirectional** antennas
        - to broadcast and receive signals in all directions
    - **unidirectional** antennas
        - to broadcast and receive signals in a specific direction

MIMO/MU-MIMO

- A tech that allows for more than one spatial stream to be transmitted and received by a single device through the use of multiple antennas.
    - MIMO allows for up to 4 spatial channels, MU-MIMO allows for up to 8 spatial channels.
    - MU-MIMO allows for a single signal to be spread across multiple transmitters --- accounts for the multiple user part of the name.

Wireless access points

A foundation of the wireless LAN (WLAN)

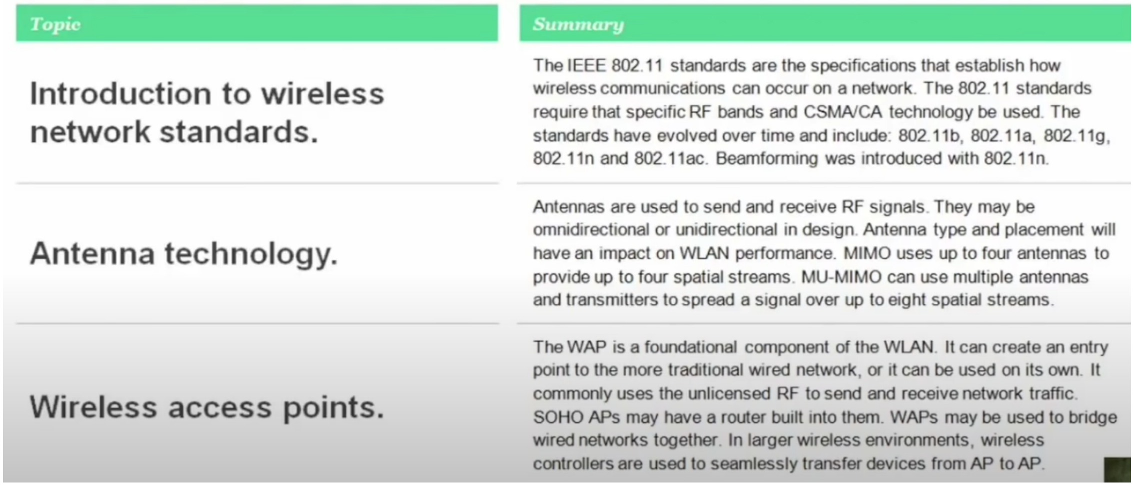
- The **wireless access point (WAP)**, also known as just an access point (AP) can create a point of entry for wireless to enter the more traditional wired nwing env.
    - can also be used to join other types of nw.
- WAPs, use *RF bands* in order to communicate with devices
- one ore more antenna is used in order to radiate and receive RF signals in a half-duplex manner (data can move in 2 directions, but not simultaneously)
- wireless routers are common in the SOHO env. They are WAPs that have a router built into them, reducing the need for nwing components.
- wireless bridges are APs that can bridge wired nw segments together in certain situations.
- WAP performance is impacted by the number of wireless devices that are attempting to access the nw.
    - can be mitigated by adding additional APs to the nw.
- strategically adding WAPs to the WLAN can allow users to migrate from one wireless signal to the next (called **roaming**)

Wireless controllers

- are commonly found in wireless nws of medium sized and larger businesses.
- are used to control WLANs that have multiple WAPs that all function as part of a larger WLAN through the use of special protocols and can increase the usability of the WLAN.
    - **LWAPP (Lightweight Access Point Protocol)** is used by Cisco wireless controllers.
- **Dynamic or static VLAN pooling** can be established with a wireless controller.
    - taking the WLAN signals and creating and controlling VLANs to allow more devices to connect to a single AP.
- are often used to create a wireless nw mesh that seamlessly spans more area than is normally possible.

  - mobile wireless devices are seamlessly(无缝的) handed off from one AP to another when they reach the edges of the signal.

Conclusions

- 

Topic	Summary
Introduction to wireless network standards.	The IEEE 802.11 standards are the specifications that establish how wireless communications can occur on a network. The 802.11 standards require that specific RF bands and CSMA/CA technology be used. The standards have evolved over time and include: 802.11b, 802.11a, 802.11g, 802.11n and 802.11ac. Beamforming was introduced with 802.11n.
Antenna technology.	Antennas are used to send and receive RF signals. They may be omnidirectional or unidirectional in design. Antenna type and placement will have an impact on WLAN performance. MIMO uses up to four antennas to provide up to four spatial streams. MU-MIMO can use multiple antennas and transmitters to spread a signal over up to eight spatial streams.
Wireless access points.	The WAP is a foundational component of the WLAN. It can create an entry point to the more traditional wired network, or it can be used on its own. It commonly uses the unlicensed RF to send and receive network traffic. SOHO APs may have a router built into them. WAPs may be used to bridge wired networks together. In larger wireless environments, wireless controllers are used to seamlessly transfer devices from AP to AP.

Basic WLAN topologies

Ad hoc topology

- A basic WLAN that does *not* require the use of a wireless access point (*WAP*) --- also known as an AP.
- devices negotiate the wireless connection between themselves. (e.g., laptops connect wirelessly without the use of a WAP)

Infrastructure topology

- A common type of WLAN that *uses a WAP or WAPs* to create a connection point for wireless devices.
  - most often connects a WLAN to a more traditional wired nw, but not absolutely required.

Mesh topology

- employs the use of multiple APs to create a larger seamless nw converage area.
  - commonly deployed with wireless controllers and WAPs.

Note

- the higher the wireless device density, the more WAPs that will be required to handle the load.
  - APs only have a certain amount of capacity
  - adding more WAPs, a wireless controller can greatly ease the load and increase the efficiency of the nw.

WLAN concepts and terms

IBSS (Independent Basic Service Set)

- is created when an ad hoc nw topo is created. The devices use the IBSS in order to control the communication that occurs between connected devices.

BSS (Basic Service Set)

- When a single WAP is in infrastructure mode, it will create a BSS. It can control the flow of communication between every device that connects to the SSIDs under its control.

ESS (Extended Service Set)

- is created when two or more APs share a common SSID and have overlapping coverage. The WAPs will negotiate how to hand off a wireless device between them as it roams the nw through ESS.

SSID (Service Set Identifier)

- All active WAPs will use a beacon transmission to advertise the nws that they belong to. What they advertise is their SSIDs (their **nw names**). Those beacons are how devices know which nws they can connect to.

802.11a-ht and 802.11g-ht

- both relate to the 802.11n standard
  - denote the type of connection --- high throughput, and the radio frequency --- either 2.4GHz or 5GHz of the connection

Goodput

- the actual amount of application data passed through a connection with the overhead removed, measured in bytes per second.
- it is different than throughput
  - **throughput** measures the total amount of data capable of being passed through a connection

Signal strength

- A measure of the strength of the RF signal from an AP, which can help to determine coverage area.
  - as a general rule, the closer a device is to the WAP, the stronger the signal received
- the strength of a signal can be affected by WAP or antenna placement, type of antenna, and interference sources, etc.

Heat mapping tools

- A wireless site survey with heat mapping tools can help in the set up of a WLAN or pinpoint problem areas.
- It builds a visual map by measuring **received signal strength indicator (RSSI)** and **signal to noise ratio (SNR)**, which can be directly correlated to data throughput.
- allows the administrator to find gaps in coverage as well as areas where the coverage extends beyond the desired boundaries.

Risk and Security related concepts

The big picture of recovery

Disaster recovery plan (DRP)

- A disaster is any event or emergency that goes beyond the normal response resources. (e.g., earthquake or flood)
- DRPs detail the steps to recover from a disaster situation (e.g., offsite backups and fallback sites)
  - as well as how to help ensure employee safety

Business continuity plan (BCP)

- A sub-element of the DRP, a BCP includes an impact analysis of the business effects of down systems.
  - helps to identify single points of failure in the business sys.
- a BCP helps to guide the creation of the DRP.

Concepts and terms

Single point of failure

- A sys or component that, if it goes down, has a major impact on operations.
- can be mitigated through several different methods:
  - redundant sys (e.g., a backup router or redundant power supply)
  - sys redesign (e.g., removal of the point of failure through a redesign of the sys)

UPS (Uninterruptable power supply)

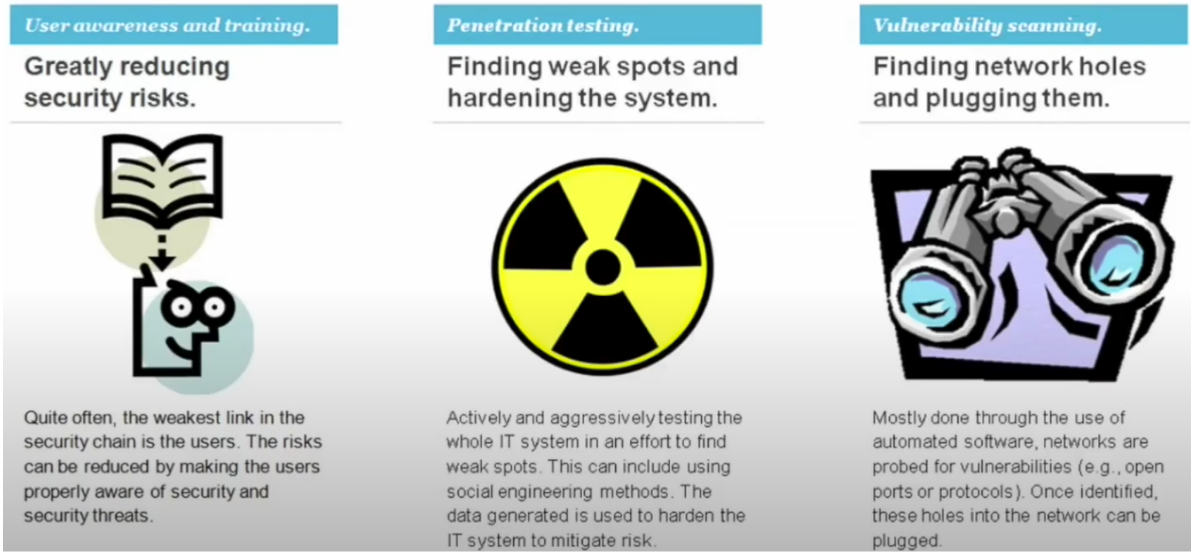
- will mitigate power issues that can have a negative impact on sensitive nwing components.
  - conditions the incoming power to remove spikes and sags in the current, ensuring that the current flow is even.
  - helps to ensure continues operation for a given period of time in the case of complete electrical power supply loss.

First responders

- the first people to discover or respond to the security issue.

Data breach

- any unauthorized access to data, particularly to sensitive data.
  - breach may be unintentional or intentional
  - may occur internally or externally



User awareness and training.

Greatly reducing security risks.

Quite often, the weakest link in the security chain is the users. The risks can be reduced by making the users properly aware of security and security threats.

Penetration testing.

Finding weak spots and hardening the system.

Actively and aggressively testing the whole IT system in an effort to find weak spots. This can include using social engineering methods. The data generated is used to harden the IT system to mitigate risk.

Vulnerability scanning.

Finding network holes and plugging them.

Mostly done through the use of automated software, networks are probed for vulnerabilities (e.g., open ports or protocols). Once identified, these holes into the network can be plugged.

Communication network vulnerabilities

Vulnerabilities associated with unsecure protocols

Telnet

- A protocol that is used to create a virtual terminal connection that is commonly used in troubleshooting.
- it is unsecure because all communication occurs in clear text --- not support encryption
  - should use SSH

SNMP (Simple Network Management Protocol) v.1 and 2.

- used to remotely manage and configure nw devices
- due to a lack of encryption support, v1 and v2 are unsecure and are susceptible to packet sniffers
  - should use v3

FTP (File Transfer Protocol)

- used to transfer files across a nw connection
- username and password are required, but FTP doesn't support encryption.
  - use **SFTP** which creates an SSH FTP session

TFTP (Trivial File Transfer Protocol)

- a simple stripped down version of FTP that doesn't support authentication like standard FTP. It is used to download configuration files to nwing equipment.
  - should only be used when a connection to nwing equipment is made through the console port, thus eliminating the possibility of eavesdropping.

HTTP (Hypertext Transfer Protocol)

- used to send and receive data over the Internet
- is unsecure in its basic format and susceptible to being intercepted due to its lack of encryption
    - use **HTTPS** (provide encryption and other security services)

SLIP (Serial Line IP)

- an early protocol developed for communicating over serial ports and modem connections that requires a static IP address.
- outdated and unsecure, not support encryption
    - use **PPP (Point-to-Point Protocol)**

Vulnerable network practices

Unpatched or legacy systems

- unpatched sys are unsecure
- sometimes, it is necessary to keep legacy sys alive which can create vulnerabilities in the sys, as weaknesses in these sys tend to be well known.

Open ports

- an open port -- either a physical or application port -- on the nw is a hole in the security of the nw that may be exploited.
- While not all open ports can be or should be closed, security should be placed on those ports that need to remain open to reduce the vulnerability of the nw.
    - a good practice is to use a port scanner periodically to verify that only absolutely required application ports are open.

Unnecessary running services

- A periodic review of all running services should be conducted on all equipment that attaches to the nw. All unnecessary running services should be disabled.

Clear text credentials

- periodically review all applications and sys to determine which ones use clear text credentials, then either limit their use or figure out how to encrypt the transmissions.

Unencrypted channels

- any method of communication on the nw that is not encrypted is an unencrypted channel that is subject to being breached.
    - not all communication channels need to be encrypted, so need to figure out which ones need to be encrypted.
- all wireless nw channels should be encrypted --- no exceptions.

RF (Radio frequency) emanation (泄射)

- one method of intercepting(拦截) communication is to analyze signal leakage (e.g., RF emanations). Many forms of communication are subject to these signal emanations, but there are steps that can be taken to reduce them.
    - **TEMPEST** is a set of standards established by the NSA and NATO that outlines steps that can be used to reduce the opportunity for interception and analysis of communication.