Computer Networking Course - Network Engineering (CompTIA Network+) Part 3

Implementing a basic network

Plan the network

- A nw plan is vital whem implementing any nw more complicated than the most basic.
- **list of requirements**
  - define why the nw is needed
  - define what nw features are required
  - define the scope of the nw
  - eastablish a budget
- **nw design**
  - what equipment is needed to implement the nw
  - how the nw be organized
  - how the shared resources be placed on the nw
- **compatibility issues**
  - what standards are in play now and in the future
  - does current equipment require specific cabling or connection types
- **internal connections**
  - how many node connections
  - how will future expansion be planned
- **external connections**
  - how will the nw connect to the outside
- **nw equipment placement**
  - is there a wiring/equipment closet
  - what env considerations
- **how will nw security be implemented**
  - firewall type and placement considerations
  - VLANs required or not
  - how the port security be implemented

Configure the network

- Network configuration considerations
  - How clients receive their IP addr:
    - static IP addr configuration creates more security, but harder to manage
    - DHCP to automatically assign IP addr from a pre-configured pool
  - **MAC filtering**: only allow specified MAC addr onto the nw. It is effective but difficult to control
  - A **demilitarized zone (DMZ)** will be required if a server will be hosted on the nw that needs to be accessed from outside the nw.
    - the DMZ is an area of the nw in which outside connections are allowed, while the internal nw remains protected

        - will require a custom configuration of the firewall; in most implementations, 2 firewalls are used
    - Firewall placement and configuration considerations
        - if a DMZ needs to be deployed, the best method is to introduce an additional router and firewall into the nw, with the DMZ residing between the WAN equipment and the new router/firewall combination
        - if a DMZ is deployed, port forwarding should also be used at the router/firewall level
    - router/firewall config considerations
        - **port forwarding** is used to direct requests for specific resources to the computer that has the resource
    - wireless nw config considerations
        - **Service set identifier (SSID)**: the name of the wireless nw
            - SSID can be set to broadcast in the clear
            - SSID can alternatively be set for the broadcast to be hidden
        - **Encryption**: needs to be tunred on (by default wireless routers and WAPs do not have encryption enabled) and, at the minimum, WPA2-Personal should be enabled
        - some wireless nw equipment comes with **Wi-Fi protected setup (WPS)** enabled by default. This **should be turned off and not used**, as it creates a weakness in the wireless nw.
            - WPS can be easily exploited by an attacker
- Document any changes

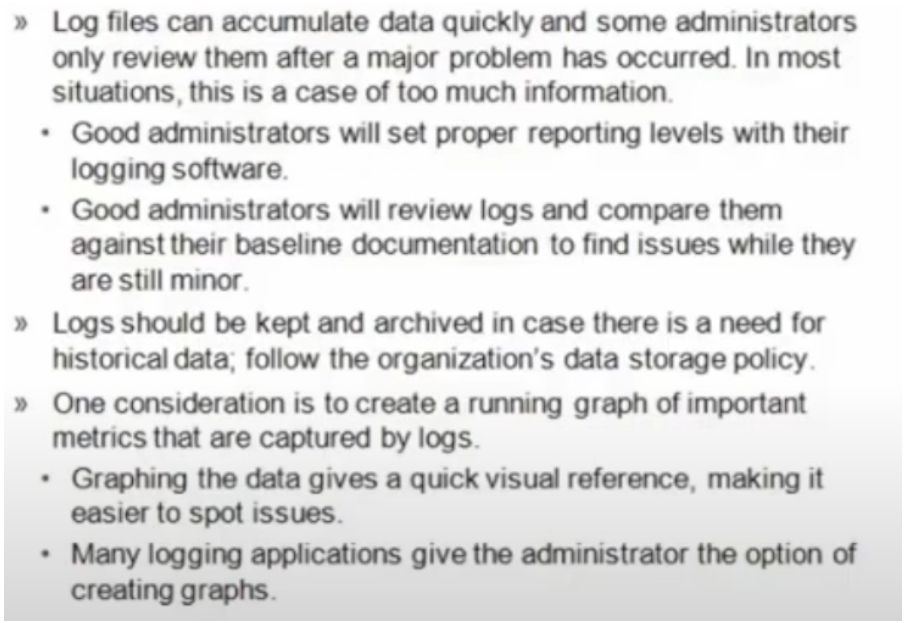
Analyzing monitoring reports

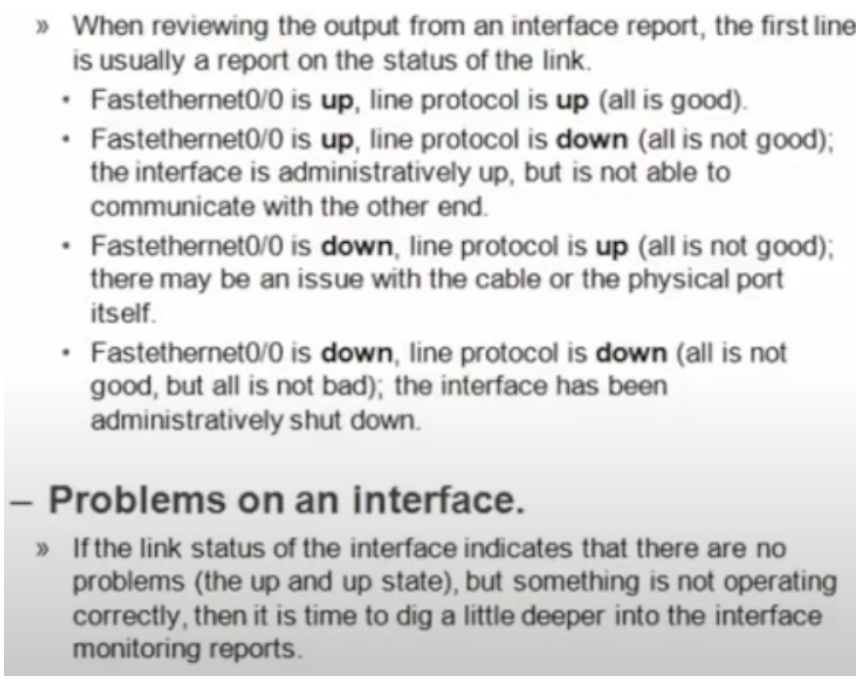
Baselines

- Baseline documentation provides a snapshot of the nw when it is running efficiently. Baselines are usually kept as a log file, although they may also be graphical in nature.
- Baselines should be established on CPU utilization and nw utilization. **Periodic tests** should be conducted to determine if the baseline has changed. You can use Windows Performance Monitor to help establish the baseline.
- **Items to consider for baselines**
    - **nw device CPU utilization**
        - help to determine when a nw device is going to fail
        - help to determine when more nw devices should be installed in a growing nw
    - **nw device memory utilization**
        - help to determine when it is time to expand the memory of nw devices
    - **bandwidth utilization**
        - help to determine the overall health of a nw
        - help to determine when nw segmentation should occur
        - help to determine if a nw device is failing
        - help to identify when a security breech has occured
    - **storage device utilization**
        - help to determine when storage utilization has become a bottleneck on the nw
        - help to determine when to increase the storage capacity of the nw
    - **wireless channel utilization**

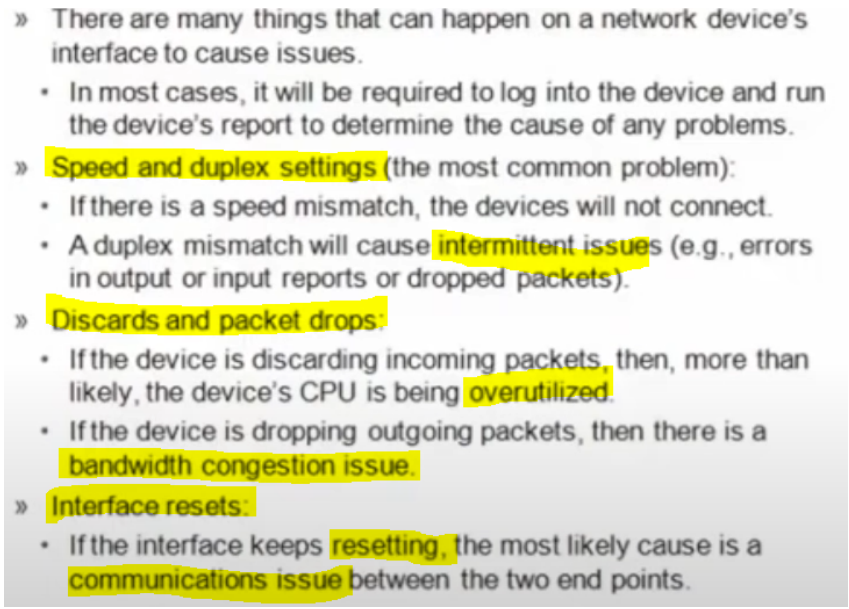
- help to determine how saturated the wireless channels have become; a new **wireless access point (WAP)** can be installed to alleviate the pressure if saturated
- help to determine if there is unauthorized wireless access occurring

Reports

- **Log management**
  - 

- **Interface link status**
  - 

- **Interface monitoring reports**

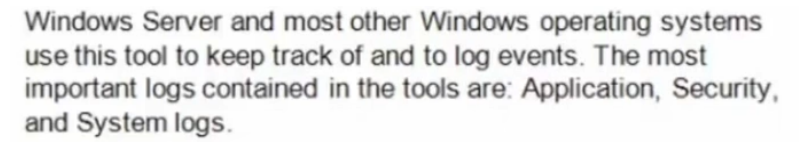
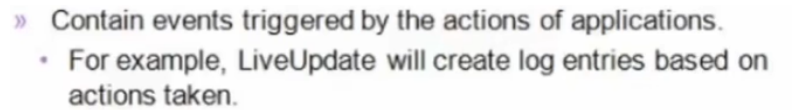
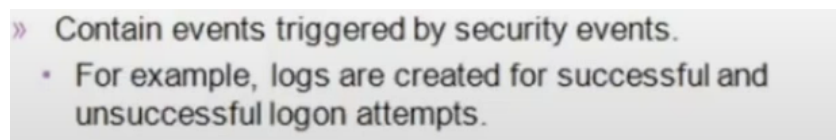
- 
  - There are many things that can happen on a network device's interface to cause issues.
    - In most cases, it will be required to log into the device and run the device's report to determine the cause of any problems.
  - Speed and duplex settings (the most common problem):
    - If there is a speed mismatch, the devices will not connect.
    - A duplex mismatch will cause intermittent issues (e.g., errors in output or input reports or dropped packets).
  - Discards and packet drops:
    - If the device is discarding incoming packets, then, more than likely, the device's CPU is being overutilized.
    - If the device is dropping outgoing packets, then there is a bandwidth congestion issue.
  - Interface resets:
    - If the interface keeps resetting, the most likely cause is a communications issue between the two end points.

Network Monitoring

The why of network monitoring

- to not be surprised by failures in nws

Tools to monitor the network

- **Log files**
  - all OS offer a means of viewing events that occur to that specific machine, includes nwing equipment
  - some applications have been developed to monitor sys and nw that also generate log files
  - log files can be used to help pinpoint when a problem occurred and help to narrow down the cause of an issue
  - log giles can be used to help create a baseline of nw behavior
  - can usually be classified as being: sys logs, general logs, history logs
    - are an after-the-fact means of monitoring the nw, not very good for real time analysis
- **Logging tools**
  - Event viewer
    - 
      Windows Server and most other Windows operating systems use this tool to keep track of and to log events. The most important logs contained in the tools are: Application, Security, and System logs.
  - Application logs
    - 
      - Contain events triggered by the actions of applications.
        - For example, LiveUpdate will create log entries based on actions taken.
  - Security logs
    - 
      - Contain events triggered by security events.
        - For example, logs are created for successful and unsuccessful logon attempts.
  - System logs

- Contain events triggered by Windows system components.
  - For example, when drivers start or fail to start, a log entry will be created.

- **Sysklog**
  - non-microsoft log
    - Developed in the 1980s, provides devices that normally would not be able to communicate with a means of delivering performance and problem information to system administrators.
    - Permits there to be separation between the software that generates the message, the storage of the message, and the software that analyzes the generated message.
      - This allows syslog to be highly configurable and has allowed it to continue to be a vital tool for monitoring networks.
    - The Internet Engineering Task Force (IETF) standardized syslog in 2009.
    - It generates log messages based on the types of service and includes a severity level from zero (most severe) to seven (least severe).
    - Syslog can generate a lot of log messages, most network administrators configure it so that they only get alerted when a minimum severity level has been reached.
      - Network administrators may receive alerts via SMS or email.
  -

Code	Severity	Description	Description
0	Emergency	System is unstable	An emergency condition usually affecting multiple systems.
1	Alert	Action must be taken immediately	Corrective action should be taken immediately, usually condition is affecting primary systems
2	Critical	Critical conditions	Corrective action should be taken immediately, usually condition is affecting secondary systems
3	Error	Error conditions	Non-urgent failures
4	Warning	Warning conditions	Not an error but an error may occur anytime
5	Notice	Normal but significant conditions	An unusual condition but not to the level of a warning
6	Informational	Informational messagess	Normal operational messages
7	Debug	Debug-level messages	Information used for debugging an application or system

- **SNMP (Simple Network Management Protocol)**
  - an application layer protocol used to monitor and manage a nw's health
  - nw or sys admin configures monitors (called **traps**) on devices that view the operation of a specific item
    - the monitors periodically communicate with a **nw management station (NMS)** through **GET msg** that NMS sends out
    - the response from the monitors is stored in a **Management Information Base (MIB)**, which is a type of log file.
    - the admin can configure the monitors with **SET msg** sent from the NMS.
  - when an event occurs (interface goes down), the trap is tripped and the event is logged
    - can be configured to just log the event or contact a nw admin

        - the ability provides a more real time monitoring method
    - **SIEM (Security information and event management)**
        - combine **security information management (SIM)** and **security event management (SEM)**
        - used to monitor and provide real-time analysis of security alerts
            - an example of SEM functionality
        - used as a tool to analyze long-term data and log files
            - an example of SIM functionality
        - highly configured to the needs of the individual nw needs

Active network monitoring tools

- **Port scanners**
    - used to scan a nw for open ports and protocols, then info is then used to harden the nw
    - are a great method of finding vulnerabilities in the nw infrastructure and plugging them before a security breech can occur.
    - only use a port scanner on a nw or a sys that you are authorized to scan
- **Interface monitoring/packet flow monitoring**
    - are usually deployed as **active software tools to monitor and analyze nw traffic within a nw segment**
        - commonly called ***packet sniffers*** or ***protocol analyzers***, allow for an in depth look at what traffic is on the nw and may reveal security issues that the nw admin can then mitigate
    - can identify top talkers on a nw segment
        - the interfaces that are sending the most nw traffic or utilizing the most bw for sending packets
    - can identify top listeners on a nw segment
    - **Microsoft Message Analyzer** and **Wireshark** are examples of free packet flow monitoring tools

Wireless monitoring tools

- **WiFi analyzer**
    - a similar tool to the protocol analyzer, but for wireless nws
        - sniffs out packets on wireless nws
    - can check for bw usage, channel usage, top talkers etc.
    - can identify nws by passively scanning the radio frequencies (RFs)
    - can identify hidden nws if given enough time
    - can infer non-beaconing nws based on data traffic
- **Wireless survey tools**
    - most commonly used as a design tool for setting up high quality wireless nws
        - the survey tools can help to establish the required amount of access points (APs), ideal antenna placement, and optimum channel overlap
        - can be used to identify possible causes of RF
    - used to eliminate wireless nw performance and security issues before they even occur.

Environmental monitoring

- A nw's health can be affected by more than just a nw interface failing or a possible security breech
- enviromental factors: electrical power, heat and humidity
- **power monitoring**
    - systems and tools can be used to evaluate the amount of and the quality of the electrical power being delivered to the system.
        - power monitoring is often deployed with, or alongside, an **uninterrruptable power supply (UPS)**
        - the monitor will issue an alert when an issue with electrical power has been identified
- **environmental monitors**
    - **heat monitors**
        - all electrical components are designed to operate within a specified heat range, they also generate heat when in use
    - **humidity monitoring**
        - too little humidity increases the risk of electrostatic discharge and too much humodity increases the risk of condensation

Supporting configuration management

Configuration management (CM)

- CM is a discipline that is used to evaluate, coordinate, approve, deny, or implement change in or to an IT system.
- helps to ensure that the nw runs efficiently and smoothly.

Documentation

- Documentation plays a key role in any CM sys that get developed.
- used to help evaluate and plan proposed changes, and also used in asset management, nw maintenance, and vendor evaluations.
- **Policies and procedures**
    - Policies are a set of guidelines that establish how the nw is to be configured and operated. They also set the expected behavior of the people within the organization.
    - Procedures are a set of documents that detail how the policies are to be implemented.
- **Asset management documentation**
    - broad category of documentation often used to help in the change management process.
    - detailed info on what assets are present, also includes the maintenance history for those assets.
    - used to help track update and upgrade cycles
- **Physical nw diagrams**
    - a map of all nw devices and how they connect
    - specifies the cabling, connectors, and physical cabling runs

    - cabling management documentation is a subcategory
        - A **wiring scheme** establishes the types of cabling and the connectors used, and also defines the allowed standards.
- **Logical nw diagrams**
    - similar to a physical nw diagram but more detailed
    - details IP addresses, ports, protocols, etc.
    - details connected nws (e.g., LANs, VLANs, and WLANs)
    - details IP address utilization
        - IP address utilization can greatly affect the efficiency and performance of the nw
    - physical and logical nw diagrams may be combined into a single document
- **Vendor documentation**
    - a broad category of documentation that can include:
        - approved vendor list
        - vendor approval process
        - purchase order documentation
- **Common vendor 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.
    - **Statement of work** (**SOW**): a detailed document that specifies what work is to be performed, the expected outcome, and the timelines to perform the work.
    - **Master license agreement** (**MLA**): a legal agreement between two entities in which one agrees to pay the other for the use of a specific piece of software (or software package) for 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.

Backups

- Backups are an essential part of any CM system
    - play a key role in recovering from unexpected consequences or from the failure of a component.
    - Backup schedules must be implemented and periodic tests should be conducted to ensure that the backup process is working.
- **Types of backups**
    - **Full**
        - all data on the targeted sys is backed up
        - slowest backup method with the highest storage requirements, but leads to the fastest recovery method.
        - recovery requires the full backup files
    - **Incremental**
        - only the new or modified files are backed up

        - fastest backup method with the lowest storage requirements, but slowest recovery method
        - recovery requires the last full backup file and all of the incremental backup files
    - **Differential**
        - only data that has changed since the last full backup is saved
        - time is moderate, requires a moderate amount of storage, but also is the middle ground on the length of time for recovery
        - recovery requires the last full backup file and the last differential backup file
- The configuration files of a nw device should also be backed up.
    - helps to speed up the recovery time in cases of equipment failure or when a change to the configuration has introduced unexpected consequences.

Bring your own device (BYOD)

- BYOD policies allow employees to use their personal devices on an organization's nw.
    - IT departments are tasked with keeping a nw safe, yet they have very little control over the devices that employees bring in. In some cases, BYOD policies have led to the introduction of malware into an organization's nw environment.
    - **Network Admission Control (NAC)** has been implemented in an effort to reduce the risks associated with BYOD policies and to introduce CM to those devices.
- **NAC**
    - NAC is a Cisco process. Microsoft uses Network Access Protection (NAP)
    - includes more than just authenticating users and devices on the nw
    - all devices requesting access to nw resources are screened for:
        - type of device
        - OS used, including updates
        - security software, including updates
        - presence of malware
        - other security vulnerabilities
    - in some cases, if the connection request has been rejected, the device is redirected to a *remediation（补救） server*, which attempts to resolve the known issue.

The importance of network segmentation

The OSI model and segmentation

- Segmentation: taking a single nw or a sys and breaking it into smaller discrete units.
    - can be achieved physically or logically
    - reasons to segment a nw
        - to ease administrative tasks
        - to achieve performance gains
        - to increase security
        - to comply with regulations
- Segmenting the nw at different OSI model levels
    - **OSI (open system interconnection)** model
        - Physical layer (L1)
        - Data link (L2)

        - Network (L3)
        - Transport (L4)
        - Session (L5)
        - Presentation (L6)
        - Application (L7)

Reasons for segmentation

- **Compliance**
    - some rules and regulations require that certain data be kept separate and secure
        - segmentation allows for the regulated data to flow across its own nw keeping it more secure
- **Network performance optimization**
    - the size of nws increases, the amount of data flows also increases which slow down the performance of the nw.
        - segmentation breaks the larger nw into smaller units, which can lead to an increase in performance on those new segments
- **Creating high performance nws**
    - some applications require more bw in order to perform at a desired higher level
        - VoIP, video teleconferencing (VTC), media nets (streaming services) perform better on their own segments
- **Separate private from public networks**
- **Legacy systems**
    - some organizations use systems that are considered critical, but are not capable of residing on the modern nw.
        - segmentation allows the legacy(遗留) sys to reside(居住) on its own subnet.
- **Testing labs**
    - the labs can be used to test new applications, os, update patches, etc.
        - segmentation allows for testing to occur in a secure, easily controllable env.
- **Security**
    - one of the main reasons
        - segmentation allows nw and sys administrators to more easily control the flow of data between sys and access to nw resources.
- **Honeynets**
    - nw segments that are created with the sole purpose of attracting any nw attacks through the use of multiple honeypots
        - the nw segment of honeypots allows the main nw to remain secure, and gives nw administrators an opportunity to study an attack so that countermeasures can be developed to prevent future breeches.
- **SCADA (Supervisory Control and Data Acquisition) systems**
    - the most widespread of **ICS (industrial control sys)**
        - the use of coded signals over communications channels to provide control of remote equipment.
        - commonly used in industrial applications to monitor and control sys.
    - utilities often use SCADA sys to control their operations, through the use of a **DCS (distributed control sys)** nw.

        - The DCS allows for the control of multiple SCADA sys from a single location
    - The *Stuxnet virus* attacks SCADA sys and can spread through the DCS, leading to more damage from the virus
        - segmentation of the DCS can limit the amount of damage caused by such a virus attack on industrial processes.

Applying patches and updates

Patches and updates

The complexity of the modern OS has led to the necessity for updates, patches, and hotfixes. These are used to add features, fix bugs, and repair security holes that become know.

The goal is to keep sys as up to date as possible through the use of updates, patches, and hotfixes ---- reduce the sys's vulnerability and increase its functionality, while reducing costs.

- **Patches, updates, hotfixes, and service packs**
    - A **patch**: is small section of code that is used to either increase functionality or fix a problem within a software package.
    - An **update**: is a large section of code that is used to either increase functionality or fix problems within a software package.
    - A **hotfix**: (also called a **vulnerability patch**) is similar to a patch, but is smaller than a patch. They are designed to be deployed to fix very specific issues within an OS or other software package.
    - A **service pack**: is a cumulative Windows update package that contains all patches, updates, and hotfixes between two points in time.
        - Microsoft releases service packs as a method of easing the installation of an OS, helping to keep it current.
- It is possible to *automate* the patch and update process through registering the product with the vendor who created it.
    - In a production setting, all patches and updates should be installed and tested in isolation (e.g., testing lab) before they are installed on production equipment.

Upgrading vs. downgrading

- Sometimes issues arise with the installation of a patch or update, leading to problems that were not caught during the testing phase.
    - backup copies of all sys and configuration files should be maintained in order to downgrade (roll back) when this occurs.