Computer Networking Course - Network Engineering (CompTIA Network+) Part 6

Physical Network Security Control

The why of physical network security

The dangers of unauthorized physical access

- theft of nw resources: they're expensive to replace
- damaged nw resources: only takes a spilled drink to destroy a server, or a router, or a sw
- reconfigured nw resources: can result in a breached nw

Credential workaround

- some nwing equipment comes with a known workaround for when administrator credentials needs to be recovered
    - an administrator leaves an organization without disclosing login credentials
    - or an administrator forget credentials
- Cisco even publishes the steps of its workaround on its website
    - this well known vulnerability is an easy exploit for anyone with physical access to the equipment

Physical network security practices

Basic physical security

- know who is in the building and who has access to equipment
    - employee badges
    - security check-in for visitors
    - all vulnerable nw resources --- servers and nwing equipment --- are kept in a secure area

Intermediate physical security

- Access to all vulnerable nw resources is controlled and logged
    - RFID (radio frequency identification badges) or cipher locks are used to gain access to the resources
- sw and routers are secured separately from servers with different access levels

Advanced physical security

- A zoned approach to physical security
    - a layering of security in which multiple barriers --- security tests --- must be passed before physical access is granted

Methods of physical security

- security guards
- door locks
  - simple keyed locks: the analog approach
  - cipher locks: allow for logging who has unlocked the lock
  - RFID magnetic locks
  - biometric keyed locks
- video monitoring
  - remember to store the recordings separately from the resources being monitored
- separation of resources
  - nwing equipment is separated from servers, and the methods of access are different
- mantraps
  - usually involved at least two doors. access is granted through one door, but the next door cannot be opened until further verification has been achieved, ideally, the person between the two doors is trapped until some action is taken.

Firewall Basics

Types of firewalls

Host based firewalls

- installed on the node -- usually a desktop computer -- that needs the protection. Often used in conjunction with a nw-based firewall.
  - are always software applications

Network based firewalls

- usually installed on the perimeter(周边) of the nw segment that needs the protection
  - are used to protect private nws from public nws
  - can be a nw application --- specially designed and deployed to provide firewall services
  - can be a software application --- either as part of a router's OS or as a specialty application on a server that is providing routing functions

Small office/home office (SOHO) firewalls

- in most cases, the nw firewall is provided by a WAN connection device. (e.g., router)

Stateless inspection firewalls

- examine all packets either entering or leaving the nw against a set of rules -- called an **access control list (ACL)**
  - the ACL rules are defined as static values by an administrator
  - starting from the first rule in the ACL, if a packet matches a rule, the rule is enforced and the ACL is exited.
  - do not care about the state of the connection, all packets are examined

Stateful inspection firewalls

- connections are not allowed to be made from outside of the local nw segment being protected
- only the initial packets going from inside the nw to an outside nw are inspected against an ACL
- once the connection is established, the firewall monitors the state of the connection
    - allows packets to flow between the inside node and outside address, as long as the state of the connection remains valid.

Application aware firewalls

- firewalls that not only examine the packets, but also the application protocol that is being used
    - allow or deny decisions are made based on the application layer protocol as well as other ACL rules
    - slower but more thorough in protecting the private nw

Context aware firewalls

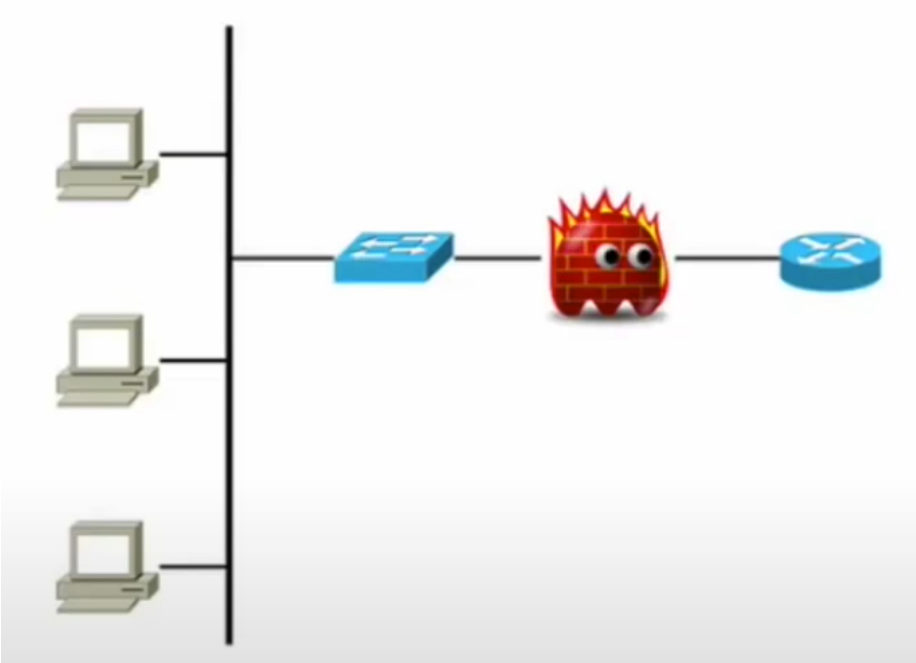
- fws that can identify not only applications, but also users and/or devices -- the context
    - can be used to restrict or allow traffic based on the context as well as other ACL rules

UTM (Unified threat management) devices

- nw appliances that include not only a fw service, but other services as well -- intrusion(入侵) detection services or intrusion prevention services
    - one concern with a UTM device is that it can create a single point of failure

Virtual wire firewall

- most often, fws are implemented on a router's interface or at a host level. when implemented on the router interface, the fw takes part in the routing process. when implemented at the host level, the fw protects the host on which it resides.
- An exception is the implementation of a **virtual wire fw**. It is a nw based fw that resides between 2 devices and provides neither routing nor switching functions. It contains 2 interfaces and, as traffic passes between the interfaces, the packets are compared to an ACL.
    -



Firewall settings and techniques

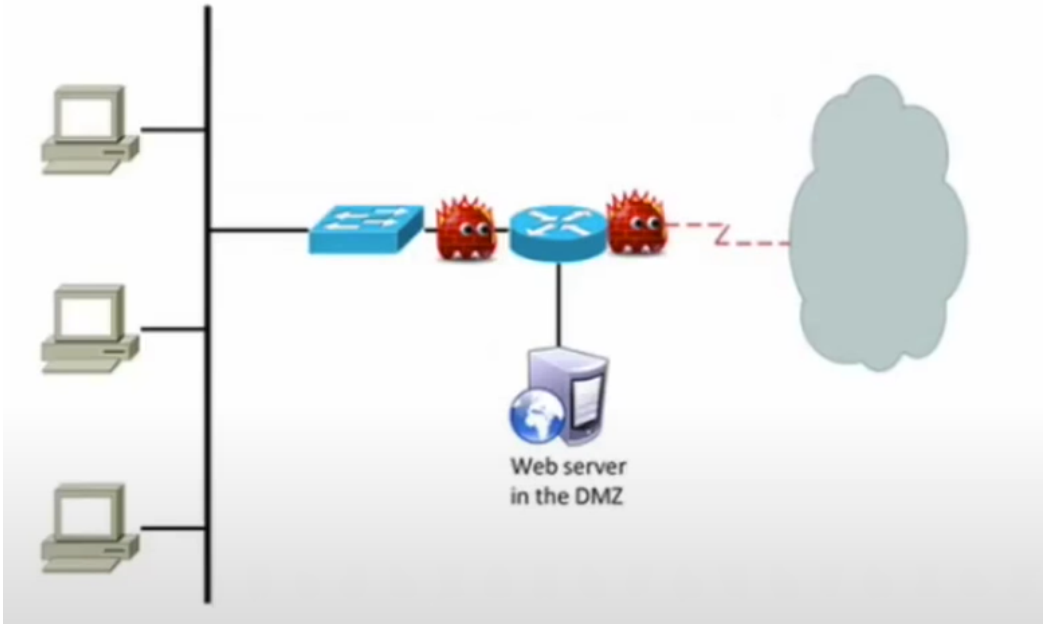
ACL (Access control list)

- each fw interface may have *2 ACLs* associated with it
  - **inbound**: examines all packets inbound on the interface
  - **outbound**: … all packets outbound …
- contains a set of administrator defined rules that either allow or block (deny) packet traffic
  - rules can be based on such criteria as source or dst IP address, MAC address, protocol, and time of day
  - packets are examined against the set of rule; once a rule is matched, the rule is enforced and the ACL is exited.
- *the last rule of any ACL is an implicit deny*
  - if the packet being evaluated does not match any of the explicit rules of the ACL, the implicit deny is enacted and the packet is blocked/dropped.
  - care and caution should be used when creating an ACL because of the implicit deny that terminates every list.

Firewall placement

- Perimeter (external) placement requires that the fw be placed at the outside edge --- usually at the WAN connection --- of the LAN segment.
  - *stateful inspection fws work well on the perimeter*. They are usually slower to make the initial connection, but once it is achieved, they offer better performance.
- Internal placement requires that the fw be placed in a logical central location --- usually used to route between different internal private nws.
  - *stateless inspection fws work well for internal placement*. They are faster to make connections and require less memory.

Demilitarized zone (DMZ)

- a specific zone created --- usually between 2 fws --- that allows outside access to nw resource (e.g., web server), while the internal nw is still protected from outside traffic.
    - the external facing router allows specific outside traffic into the DMZ, while the internal router prevents that same outside traffic from entering the internal nw.
    - 

Conclusions

Topic	Summary
Types of firewalls.	Host-based firewalls protect a single host. Network-based firewalls protect a network segment. In most SOHO situations, there is a combination of a network-based firewall (at the WAN connection) and software host-based firewalls (on the hosts). Stateless firewalls inspect all packets, while stateful inspection firewalls track the state of a connection. Application aware firewalls examine the application level protocols being used. Context aware firewalls can also determine user and type of device. UTM devices offer more than just firewall services (e.g., IDS and IPS), but may also create a single point of failure. Virtual wire firewalls are a type of network based firewall that doesn't take part in the routing or switching functions.
Firewall settings and techniques.	Each firewall interface may have two ACLs—one on the inbound side and one on the outbound side. An ACL is a set of rules that either allow or block traffic based on a set of administrator defined rules. The last rule in an ACL is an implicit deny statement. Stateful inspection firewalls work well for external placement, while stateless inspection firewalls work well for internal network placement. A DMZ is a zone created—usually between two firewalls—that allows some outside access to network resources, while th the internal network remains protected.

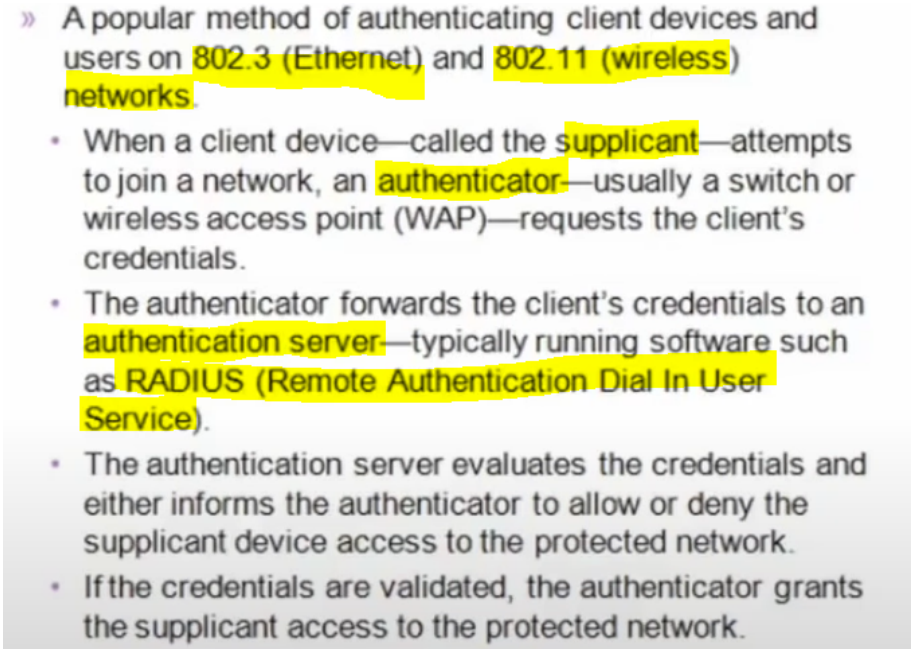
Network Access Control

Edge vs. access control

- the access control measures do not replace the need for fws. They allow the fws to concentrate on controlling the nw traffic into and out of the nw and not be concerned about who or what type of devices can connect.

Access control concepts

Authentication via 802.1x

- 
  - A popular method of authenticating client devices and users on 802.3 (Ethernet) and 802.11 (wireless) networks.
    - When a client device—called the supplicant—attempts to join a network, an authenticator—usually a switch or wireless access point (WAP)—requests the client's credentials.
    - The authenticator forwards the client's credentials to an authentication server—typically running software such as RADIUS (Remote Authentication Dial In User Service).
    - The authentication server evaluates the credentials and either informs the authenticator to allow or deny the supplicant device access to the protected network.
    - If the credentials are validated, the authenticator grants the supplicant access to the protected network.

Posture assessment

- the process of evaluating more than just the client's credentials
  - commonly used to evaluate the type of device (e.g., tablet or pc)
  - used to evaluate the type of anti-malware software on the device and how updated the software is and check if malware if present on the device
  - used to evaluate the OS and how updated the OS is; will also evaluate the registry settings of the OS
- if the client passes the assessment, it is allowed onto the protected nw
- if the client does not pass, usually one of two actions are taken:
  - the client is notified of the rejection and what has to occur before it can pass the assessment
  - the client is passed on to a remediation server, which attempts to resolve the cause of failed posture assessment, with no user interaction.

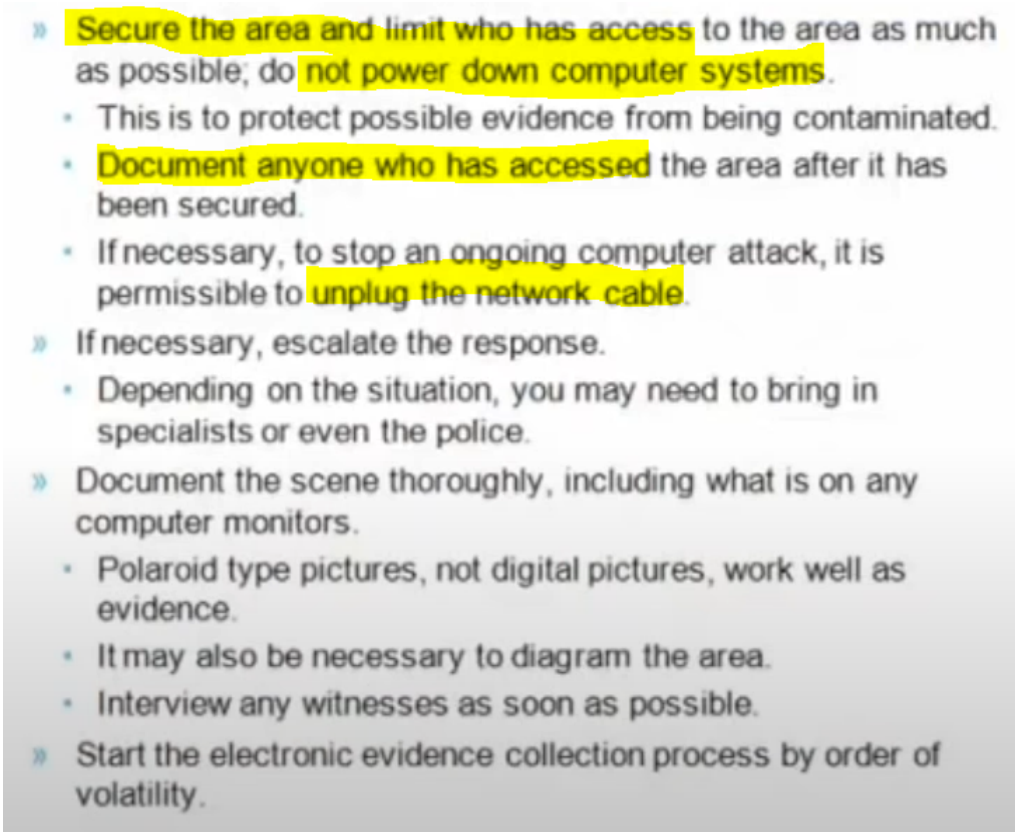
Posture assessment process

- one of 2 types of agents (software code) is used on client devices during the assessment process
  - a **persistent agent**: *permanently loaded on the device* and starts when the OS loads. It can provide more functionality than the other version (e.g., sys alerts and auto remediation)
  - with **non-persistent agent**, when the client device attempts to access the nw, the agent is *loaded onto the device* to help in the assessment process. Once the assessment process is completed, the agent is *removed* from the device.
  - when the device attempts to connect to the protected nw, it is placed on a **guest nw** with very limited access until the assessment process is completed.
  - in some cases, the client device may be placed in a **quarantine nw** with access to a remediation server until the client device pass the assessment.

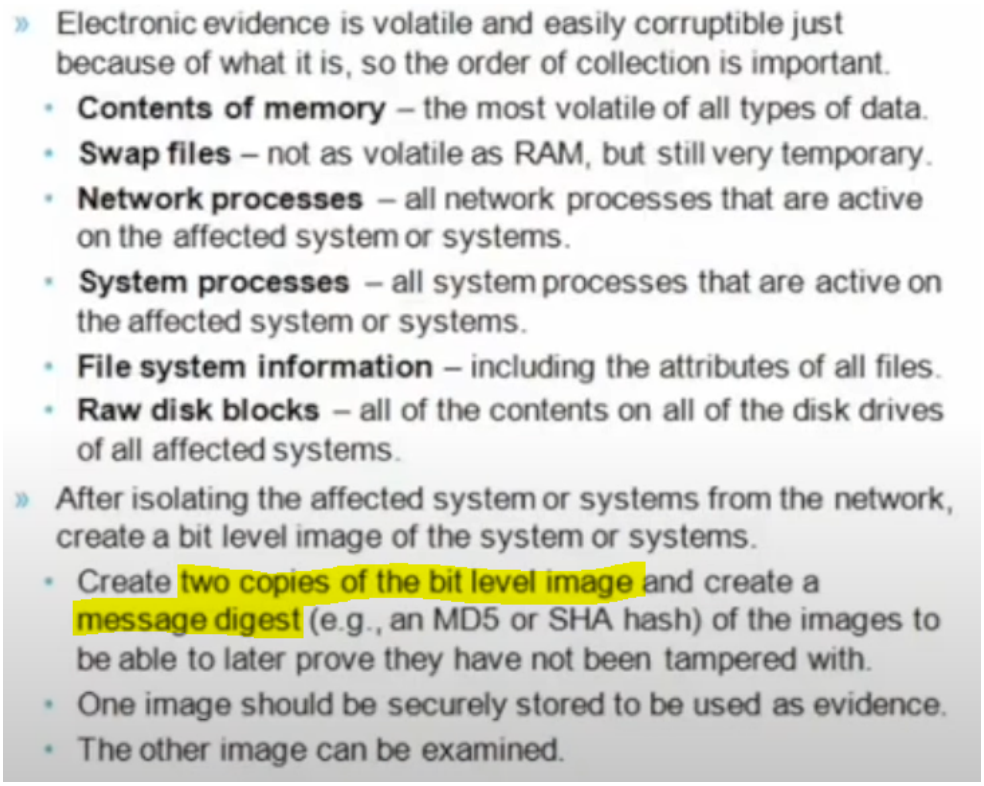
Basic forensic concepts

Collecting the evidence

First responder responsibilities

- 
  - Secure the area and limit who has access to the area as much as possible; do not power down computer systems.
    - This is to protect possible evidence from being contaminated.
    - Document anyone who has accessed the area after it has been secured.
    - If necessary, to stop an ongoing computer attack, it is permissible to unplug the network cable.
  - If necessary, escalate the response.
    - Depending on the situation, you may need to bring in specialists or even the police.
  - Document the scene thoroughly, including what is on any computer monitors.
    - Polaroid type pictures, not digital pictures, work well as evidence.
    - It may also be necessary to diagram the area.
    - Interview any witnesses as soon as possible.
  - Start the electronic evidence collection process by order of volatility.

Evidence/data collection

- 
  - Electronic evidence is volatile and easily corruptible just because of what it is, so the order of collection is important.
    - **Contents of memory** – the most volatile of all types of data.
    - **Swap files** – not as volatile as RAM, but still very temporary.
    - **Network processes** – all network processes that are active on the affected system or systems.
    - **System processes** – all system processes that are active on the affected system or systems.
    - **File system information** – including the attributes of all files.
    - **Raw disk blocks** – all of the contents on all of the disk drives of all affected systems.
  - After isolating the affected system or systems from the network, create a bit level image of the system or systems.
    - Create two copies of the bit level image and create a message digest (e.g., an MD5 or SHA hash) of the images to be able to later prove they have not been tampered with.
    - One image should be securely stored to be used as evidence.
    - The other image can be examined.

After the evidence has been collected

Chain of custody(监护)

- a document that identifies who collected the evidence, when it was collected, and who had access to it.
    - can prove that evidence has been accurately preserved and can be considered part of the evidence
    - help to ensure that all evidence is admissible in court

eDiscovery

- in legal situations, the discovery process involves the exchange of evidence between both sides of a litigation or prosecution situation
- refers to the discovery process as it pertains to electronic data(e.g., email or chat records)
    - once identified in the eDiscovery process, a legal hold is placed on data identified

Legal hold

- if data is deemed to be possibly relevant in either a prosecution or litigation situation, all normal processing of that data needs to cease
    - requires that backup tapes not be recycled and that the normal archival process for that data be suspended until the legal hold is removed

Data transport

- if physical evidence is required to be transported, a chain of custody document must be created for the transportation process and it needs to include:
    - a description of the evidence
    - the means of transport
    - who received the evidence
    - who has had access to the evidence
- if electronic means of transport are used, a **message digest** should also be included to prove that the exact evidence sent is the evidence that is received

Forensic report

- should be able to completely reconstruct and document the incident
- may be used in the litigation or prosecution process
- help in the creation of a better response plan for use in the future

Network Troubleshooting Methodology

The importance of a methodology

Seven-step troubleshooting methodology

Step 1: Identify the problem

- » Gather information. What is actually occurring or not occurring? Is the problem extremely local, relegated to your network, or out of your control?
- » Identify symptoms. Remember, the symptoms are not the problem; they just point toward the underlying issue.
- » Approach multiple problems individually.
- » Question the users. This needs to be done both politely and firmly. Many problems that are reported within a network are the result of the end user needing to be educated or re-educated in proper procedures.
  - Also, remember that most end users don't have your level of technical knowledge, so be patient, but don't patronize.
- » Determine if anything has changed. This also requires a systematic approach, so be thorough.

Step 2: establish a theory of probable cause

- » Make a list of all of the possible causes of the problem.
  - Consider multiple approaches to the problem (e.g., from bottom to top and then from top to bottom of the OSI model)
- » Divide the list into three ranked sections of: not likely, likely, and most likely; this provides a great place to start.
- » Remember to question the obvious. If the network printer doesn't work, check to be sure that it is turned on.

Step 3: test the theory of probable cause

- » If the theory is confirmed, move on to the next step.
- » If the theory is proven to be incorrect, then reestablish a new theory of probable cause.
- » If you run out of probable causes, or the situation worsens, it may be time to escalate the issue up the troubleshooting chain.

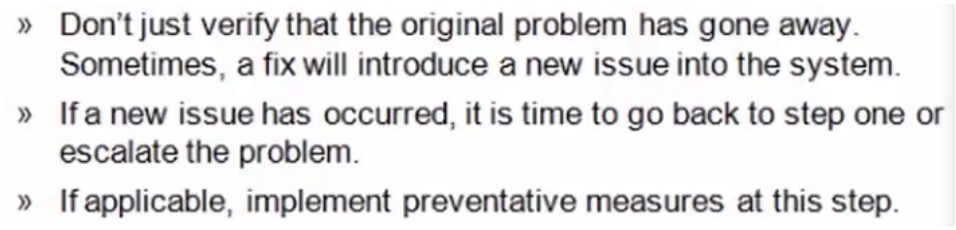
Step 4: establish a plan of action and identify potential effects

- » Simple problems may require a simple plan (e.g., turn on the network printer).
- » More complex problems will require more complex plans. In some cases, it is a good idea to write the plan out step by step in order to determine the best course of action and to identify any possible repercussions from the resolution.

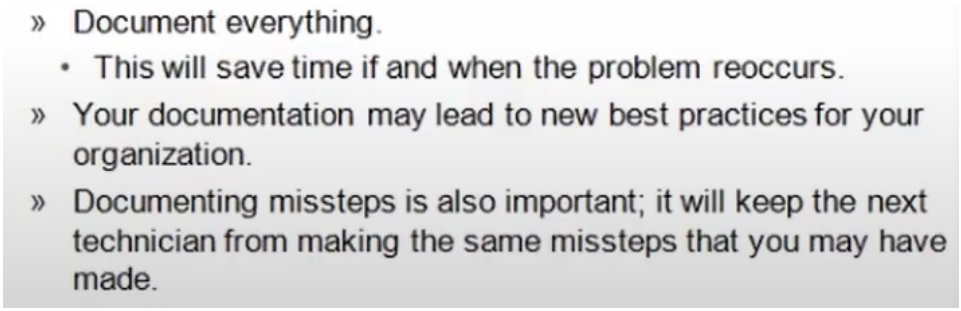
Step 5: implement the plan or escalate

- » If you have the authority, put the plan into action.
  - If you don't have the authority, escalate the problem up the troubleshooting chain; include all facts and determinations when doing so.

Step 6: verify full system functionality

- 

Step 7: document findings, actions, and outcomes

- 

Troubleshooting Connectivity with Utilities

Connectivity utilities defined

- a connectivity utility is a utility or application that is used to establish connectivity and/or to diagnose or fix a connectivity issue.

Connectivity utilities explained

- All modern OS come with prepackaged connectivity utilities designed to diagnose and repair connectivity issues.
- you can use the following applications from the command prompt (C:>)

ping

- simple utility used to determine if there is connectivity between two nodes
- uses ICMP echo requests
- the 2 basic formats are ping [ip address] or ping [hostname]
    - use ping6 or ping -6 will ping IPv6 hosts

tracert/traceroute

- used to determine the path used between two nodes
- tracert = windows and traceroute = Linux/UNIX/OS X
- use ICMP echo requests with an incrementing TTL field to form queries and get responses
- can be limited value, as many routers have ICMP diabled
- uses the same basic format as ping
    - traceroute6 or traceroute -6 for IPv6

PathPing

- Microsoft; builds upon the functionality of ping by combining it with tracert.
- perform a tracert (define the path to the last node) and perform a ping text on each hop
- one disadvantage is that is requires 25 seconds per hop to show the ping results.

ipconfig/ifconfig

- ipconfig (Win), ifconfig (Linux)
- used to determine the IP configuration of a given node
- used to change the IP configuration of a given node
- when using to diagnose connectivity, look for incorrect IP address, incorrect subnet mask, incorrect DNS address, and/or incorrect default gateway

arp

- stands for address resolution protocol
- used to correlate IP addresses to MAC address
- help to determine when there is an issue with the arp table on a given node

nslookup

- stands for name server loopup
- used to diagnose DNS issues
- helpful in determining if a DNS server is having problems

dig

- UNIX/LINUX/OS X command that is similar to nslookup
- use different switch modifiers and return different results

route

- windows specific command
- used to view and manipulate the routing tables on a Windows OS node

nbtstat

- stands for NetBios over TCP statistics
- Windows implements the NBT protocol for backward compatibility
- use if a NetBios issue is suspected

netstat

- stands for nw statistics
- used to display protocol statistics and current TCP/IP nw connection
- useful for determining if a connection has been made and the status of that connection

Additional software

Throughput testers

- used to determine the data flow (bw) of a nw
- used internally to test the flow within a LAN
- used externally to test the flow of a WAN connection
- often used to create a baseline of nw performance

Protocol analyzers

- often called *packet sniffers*
- examine the nw behavior at a very basic level
- can examine all of the packets coming into and out of an interface
- can be used to see what is consuming nw resources
- **wireshark** is a common protocol analyzer

Troubleshooting Connectivity with Hardware

What makes a cable bad?

- It can be difficult to visually tell if the cables are wired correctly and a break in the wire. Additionally, anything that makes the cable fall outside of specifications will make it a bad cable.

Cable testing tools

Multimeter

- used to test for breaks in copper wiring
    - good nw cables have a very *low resistance* value from one end to the other
    - a high ohms value indicates a break in the cable
    - 

Crimper

- used for attaching cable ends onto cables
- can either be specific to a particular type of cable end, or may work for more than one type
    - not uncommon to replace the ends of twisted pair wiring
-

Cable tester/cable certifier

- can be either fairly simple or very complex
- will test for continuity (is there a break?)
- will test for proper pinouts (are all the wires in the right places?)
- test for wiring standard (T568A or T568B)
- cable certifier will also test for more nw related items (e.g., speed and duplex settings)
    - used to certify a given nw segment
-

Toner probe

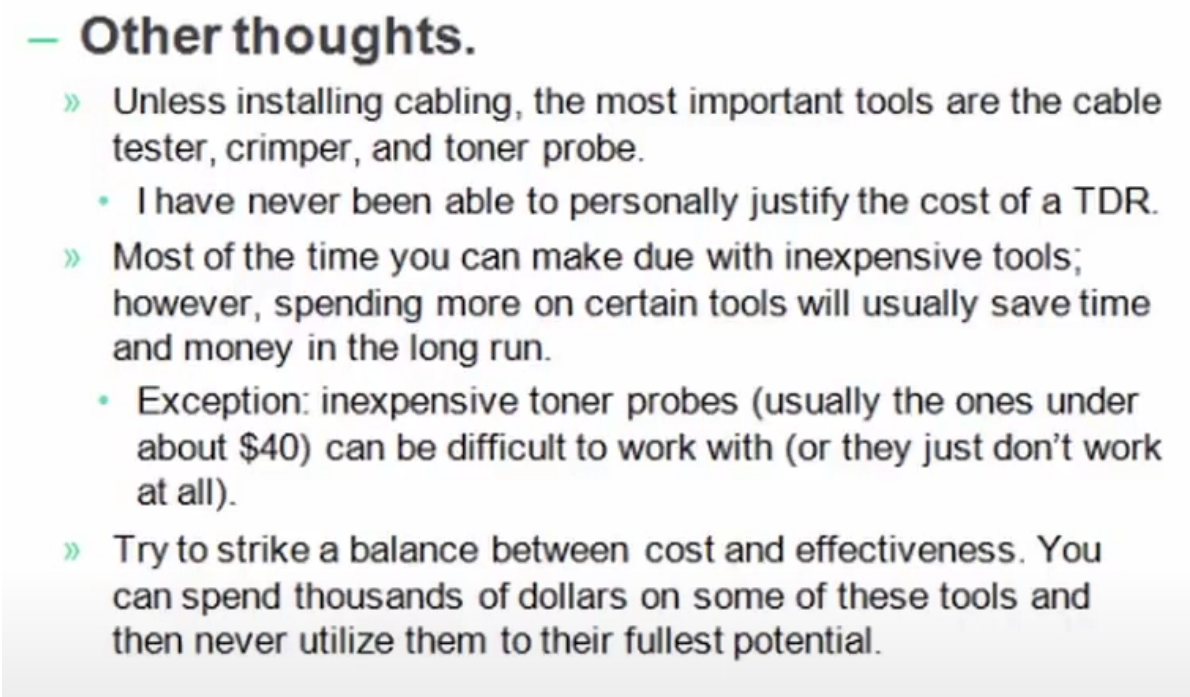
- usually a two-piece set (an injector places a signal onto a wire; the probe detects the signal and emits a tone)
- used to find and trace wires
    - useful when having to replace a single wire in a bundle of wires; can place the injector on one end to figure out which wire it is at the other end

Time-Domain Reflectometer (TDR)

- a cable tester that can also determine the length of a segment
- can tell where a break is in a segment
    - more expensive than a standard cable tester

Optical Time-Domain Reflectometer (OTDR)

- Performs the same functions as a TDR, but is used for fiber cabling
    - often called a **light meter** --- it can measure the quantity and quality of the light going through a fiber optic cable



Additional tools

Wireless analyzer

- a similar tool to the protocol analyzer, but is used for wireless nws.
    - sniffs out packets on wireless nws; this info can be used to help solve wireless connectivity issues
- can also perform other functions
    - check for bw usage, channel usage, top talkers, top listeners
    - identify nws by passively scanning the radio frequencies (RFs)
    - identify hidden nws, if given enough time
    - can infer non-beaconing nws based on data traffic

Looking Glass (LG) sites

- publically available sites that can be used to view routing info remotely as viewed by an LG server
    - create a read only portal on which routing statistics can be generated and viewed
    - can be helpful in determing if the connectivity issue is occurring because of problems on the local nw, or if the remote connection is the issue