Computer Networking Course - Network Engineering (CompTIA Network+) Part 7

Troubleshooting Wireless Network

Configuration issues

SSID (service set identifier) configuration

- symptom: unable to connect to the wireless nw
- probable cause: SSID mismatch
- possible corrective measure: check that SSIDs match exactly (they are case sensitive)

Encryption configuration

- symptom: unable to connect to the wireless nw
- probable cause: encryption type mismatch or incorrect security key
- possible corrective measure: check the encryption settings on the WAP and on the device to make sure they're the same

Incorrect channel or overlapping channels

- symptom: unable to connect or poor performance
- probable cause: incorrect channels or overlap is causing the signal-to-noise ratio (SNR) to be reduced.
- possible corrective measure: adjust WAP settings and device settings (hint: 1, 6, and 11 are the only available non-overlapping channels on the 2.4GHz frequency)

Incompatibilities

- symptom: unable to connect to the wireless nw
- probable cause: 802.11a being used in an 802.11b/g/n/ac environment, or the wrong frequency compatibilities
- possible corrective measure: make sure that you are using equipment with compatible wireless standards

Untested updates

- symptom: unable to connect, or poor performance
- probable cause: conflict between the update and other configuration settings or the wireless nw settings
- possible corrective measure: roll back the system to the prior configuration (hint: it is a best practice to make a backup copy of a system before installing any updates)

Other issues

One of the best things that a technician can do is to see if can recreate the problem.

Interference

- symptom: slow performance and/or intermittent drops
- probable cause: overlapping channels, walls or other equipment that operates in the same frequencies
- possible corrective measure: change the RF channel or frequency, or adjust WAP placement

Poor signal strength

- symptom: slow performance and/or intermittent drops, especially toward the edge of your wireless nw
- probable cause: low RF power settings, antenna type and/or placement, or WAP placement
- possible corrective measure: change RF power settings, or adjust antenna and/or WAP placement
    - caution: increasing the RF power or adjusting equipment placement may cause the signal to go where it was not intended to go

Bandwidth or device saturation

- symptom: slow performance and/or intermittent drops
- probable cause: too many users or applications for the available bw
- possible corrective measure: increase the number of WAP s and/or change to wireless standard with more throughput

Wrong antenna type

- symptom: low or no signal in an area, or signal in an area where it is not supposed to be
- probable cause: wrong antenna type for the coverage
- possible corrective measure: change antenna type to suit the required coverage

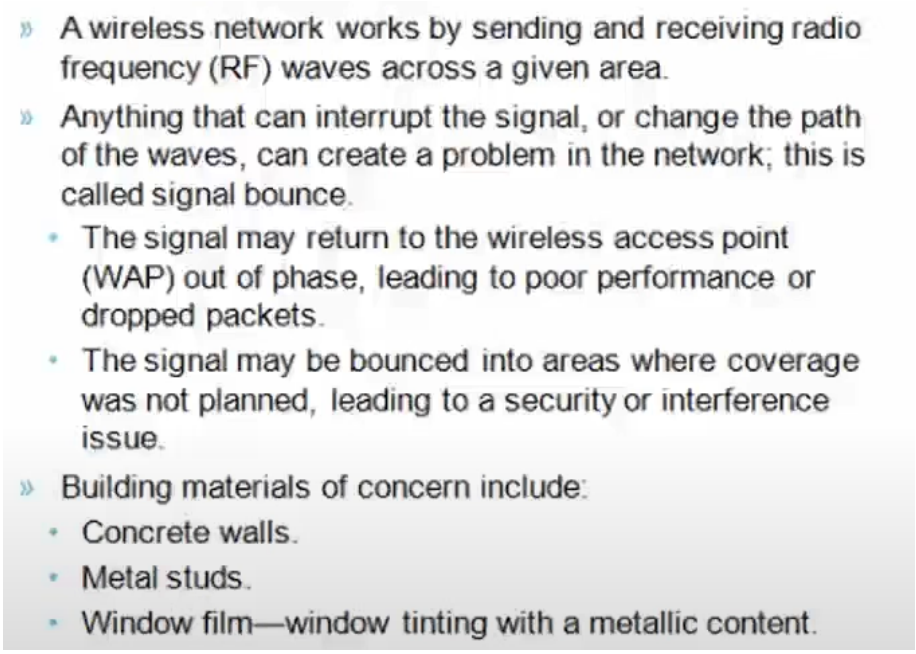
Signal bounce

- symptom: poor performance in unexpected locations, or unexpected extended wireless nw coverage area
- probable cause: RF signals bouncing off of a hard object
- possible corrective measure: adjust WAP placement

Wireless environmental factors

Wireless nw is easy to get distracted by all of the moving pieces of the wireless nw (e.g., SSID configuration, encryption and standards used) and to overlook factors in the env that may impact the quality of the planned nw.

Building materials

- 

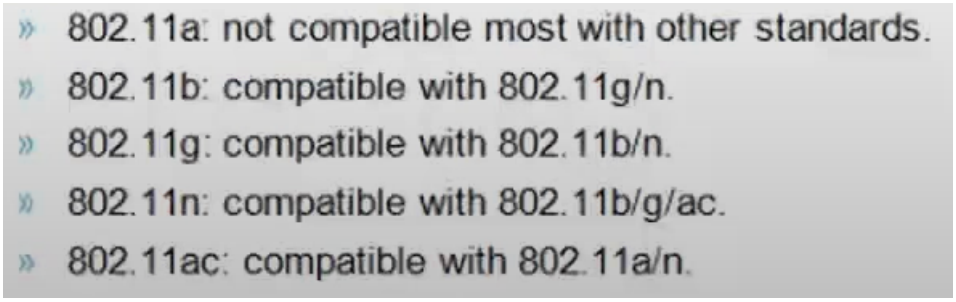
- all hard surfaces have the potential to create an out of phase or bounced signal, including office furnishings and file cabinets.
- using a wireless analyzer and wireless survey tools during the planning stage of a wireless nw will lead to better placement of the wireless equipment.

Wireless standard related factors

Wireless standard compatibility

- not all of the 802.11 standards are compatible with each other
- this is partially due to the RF frequencies used
    - most common RF frequencies: 2.4GHz or 5GHz
- this is partially due to the type of modulation employed
    - **modulation** is the encoding of information to be placed on a carrier wave, employed to put the signal on the nw
    - most common forms of modulation: **orthogonal frequency-division multiplexing (OFDM)** and **direct sequence spread spectrum (DSSS)**

Standard compatibility list for 802.11

- 

Wireless standards

- » **802.11b:** uses the 2.4 GHz RF band and DSSS.
  - Offers up to 11 Mbps networking, with a maximum indoor range of 115 ft. and a maximum outdoor range of 460 ft.
- » **802.11a:** uses the 5 GHz RF band and OFDM.
  - Offers up to 54 Mbps networking, with a maximum indoor range of 115 ft. and a maximum outdoor range of 390 ft.
- » **802.11g:** uses the 2.4 GHz RF band and both OFDM and DSSS.
  - Offers up to 54 Mbps networking, with a maximum indoor range of 125 ft. and a maximum outdoor range of 460 ft.
- » **802.11n:** uses both the 2.4 GHz and 5 GHz RF bands and OFDM.
  - Offers up to 600 Mbps networking, with a maximum indoor range of 230 ft. and a maximum outdoor range of 820 ft.
- » **802.11ac:** uses the 5 GHz RF band and OFDM.
  - Expected to offer up to 1 Gbps networking, with a maximum indoor range of 115 ft.

Troubleshooting Copper Wire Networks

Summary of troubleshooting methodology

- *Seven-step troubleshooting methodology.*
  1) **Identify the problem.**
     - » A mistake in identifying the problem can negate the rest of the steps!
     - » Remember, the problem is not the symptom; the problem is what is causing the symptom to occur.
  2) **Establish a theory of probable cause.**
  3) **Test the theory of probable cause.**
  4) **Establish a plan of action to resolve the problem.**
  5) **Implement the solution, or escalate as necessary.**
  6) **Verify full system functionality.**
  7) **Document findings, actions, and outcomes.**

Common copper wire problems

Electromagnetic interference (EMI)/radio frequency interference (RFI)

- because copper wire transmissions are electrical in nature, their electrical signals can be degraded by sources of EMI and RFI
    - sources of EMI/RFI may corrupt the nw signal, leading to loss of communication or poor communication between end nodes
- **sources of EMI/RFI** include:
    - other electrical wires; nw cables should be kept separate from normal electrical runs and, if possible, nw cabling should cross electrical wires at a 90 degree angle
    - other electrical components may inject EMI and RFI into the env; manufacturing env often have a lot of EMI and RFI present
    - one major source of EMI/RFI is fluorescent lights
- EMI/RFI problems can often be identified by when they occur; for instance, does the problem only happen when somebody turns on all the lights?
    - the solution may be to move from UTP to STP or to re-route the nw cable to avoid the source of EMI/RFI

Distance limitations

- all nw transmission media experience **attenuation** --- *loss of signal strength over distance* --- which can lead to poor communication or loss of communication between end nodes.
    - A *decibel (dB) logarithmic scale* is used to measure the amount of acceptable and unacceptable attenuation
    - as nw transmission speeds increase, the attenuation also increases --- as a ratio of signal-to-signal loss
- possible attenuation issues can be identified when a cable cannot handle the higher transmission speeds for which it is rated
- a cable certifier or time-domain reflectometer (TDR) will usually identify this problem
    - possible solution are to install a nw switch to boost the signal strength, or to re-route the nw run to create a shorter run of cable.

Crosstalk

- even with the steps taken to reduce it, all cables experience crosstalk between the pairs, which can lead to intermittent or constant transmission issues
    - more crosstalk is present at the near end (where the transmission originates) than at the far end (where the transmission is received)
    - as nw transmission speeds increase, the opportunity for crosstalk increases
- a good cable certifier or TDR will identify the problem
    - possible solutions include replacing the nw run with cable rated for a higher transmission speed, replacing the cable with one that has better shielding, or reducing the transmission rate of the nw

Bad connectors

- once a good cable is in use, the end connectors may still become broken --- especially after repeated use, leading to a loss in connectivity
    - the locking tabs on a RJ45 can be easily broken, leading to a loose connection -- creating an *open connection*
- a cable tester may identify this problem as an open connection, a thorough inspection of the cable ends can help to identify the problem

- the solution is to replace the bad connector with a good one

Bad cable

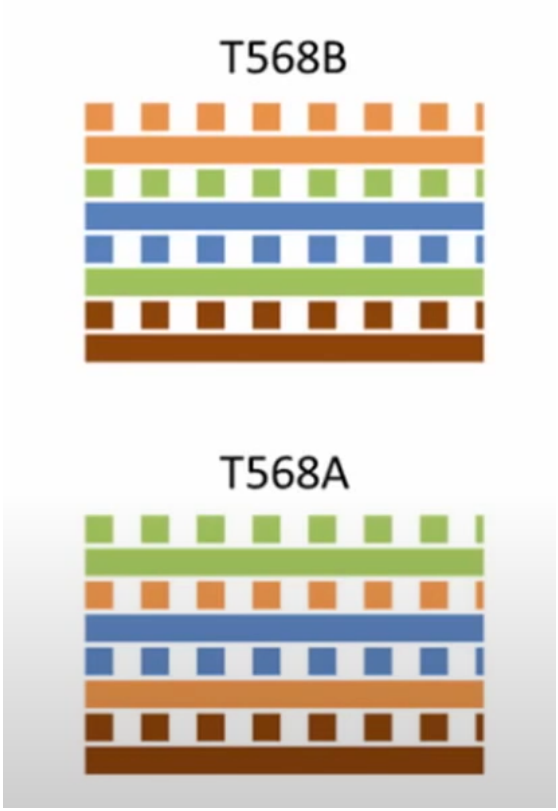
- cables can go bad, especially if they are in places susceptible to damage, leading to loss in connectivity or poor nw communication
- a cable tester can be used to identify the problem as either an open connection or a short
  - an open connection indicates a broken wire
  - a short indicates an electrical signal is traveling down an unintended path -- down the wrong wire
  - the solution is to replace the bad nw cable

What constitutes a bad cable?

- anything that makes a cable fall outside of specifications will make it a bad cable.

Copper wire termination standards

- the **TIA/EIA (Telecommunications industry association/electronics industry alliance)** has developed a set of termination standards for twisted pair copper wire.
  - the standards ensure that nw transmission is consistent across nws.
- the standards involve how the pairs of wires are ordered when placed in the termination device --- usually either an RJ45 or punchdown block.
- the current termination standards are:
  - T568B: white orange-orange, white green-blue, white blue-green, white brown-brown
  - T568A: white green-green, white orange-blue, white blue-orange, white brown-brown



- Cable testers and certifiers can be used to determine if a twisted pair copper wire nw cable meets the standards

Common copper wire problems

Twisted pair termination standards

- a **straight-through cable** is used to connect different types of devices
    - both ends of the cable are terminated to the same standard
- a **crossover cable** is used to connect similar types of devices
    - one end will be terminated to the T568A, the other terminate to the T568B

Mismatched cabling standards

- using the wrong type of cable can lead to nw problems
    - many IT devices use a process called auto-MDI/MDI-X in which they can auto-sense the type of device on the other end of a cable and electronically change their send/receive setup to match the cable used.
- cable testers can be used to help identify the problem

Split pairs

- the problem occurs during the termination process
    - at least 2 pairs of wires that should be grouped together in the termination device get separated
- the problem may not be identifiable with the most basic of cable testers
    - if the split pairs are due to a misunderstanding of the termination standards, it may still test as a straight-through or crossover cable. This often leads to a crosstalk issue
    - a good cable certifier can identify the problem

Tx/Rx (transmit/receive) reverse

- A PC type device uses pins 1 and 2 (one pair of wires) to transmit a signal and pins 3 and 6 (another pair of wires) to receive a signal
    - the receiving device must be configured to either receive on pins 1 and 2 and transmit on pins 3 and 6 or the proper cable must be used. If not, the link will not be created --- Tx/Rx reverse.
        - prevent a transmission link between devices
- if the link fails to be created, check the pinout on the cables to ensure that a Tx/Rx reverse has not occurred.

Troubleshooting Fiber Cable Networks

Using the specific tool for the job

OTDR (Optical time-domain reflectometer)

- tool used for troubleshooting fiber optic cable problems
- expensive

Common fiber cable problems

Attenuation/decibel (dB) loss

- all nw transmissions degrade over distance --- called attenuation or dB loss
    - this loss of signal strength can lead to slower speeds, loss or corruption of nw traffic, or the loss of the nw communications link
- the OTDR can diagnose attenuation and help in the placement of a repeater station

Broken fiber optic cable

- as with all types of cable media, fiber optic cables are subject to breakage
    - certain types of fiber cable can span many kilometers, making it difficult to determine where a break has occured
- OTDR can be used to determine where a break in the fiber optic cable has occurred, allowing the technician to insert a splice at that point
- a common cause of breaks in fiber optic cables is exceeding the bend radius limitations of the cable
    - due to the construction of the fiber optic cable, it is subject to breakage if it is bent beyond a certain point

Bad small form-factor pluggable (SPF) or gigabit interface converter (GBIC) transceiver

- SPF and GBIC transceivers are hot swappable replaceable modules that are used to add gigabit capabilities to switches, routers, and other nwing equipment
- a bad transceiver will prevent communication from occuring
    - an OTDR can be used to help diagnose a bad SPF or GBIC module

Fiber type mismatch

- **Single-mode fiber (SMF)** and **multimode fiber (MMF)** use different methods (transceivers) for placing the signal on the optic fiber
    - if a mismatch occurs, the most common problem is that it will be impossible to make a nw connection
    - this is also referred to as a **wavelength mismatch**, as the wavelength of the light being used is different between the modes of fiber transceivers
- the OTDR can be used to determine the types of transceivers that are being used

Other fiber optic cable issues

- anything that can interrupt the flow of light from transceiver to transceiver will create a problem
    - dirt or smudges on the connectors may cause an issue with fiber optic cable transmissions
    - when this is suspected, using a soft polishing cloth to clean the ends of the cable will solve the problem
    - **caution**: never look directly into the ends of connected fiber optic cable
- connectors are specific to mode of transmission --- SMF or MMF
-
    - connecting the wrong type of connector to a cable will prevent proper communication from occuring

    - also, check to make sure that the proper connectors are being used with the proper type of fiber optic cables
- worn or broken connectors will create an air gap, which will create a nw transmission problem
    - always inspect the connectors for their condition before use
    - OTDR can be used to determine where the loss of signal is occurring, evne if it is at the connector

Troubleshooting Common Network Issues

Problems to escalate

Switching loop

- users complain that nw works fine for a while, then goes down, and then works fine for a while
    - indicates an STP (spanning tree protocol) convergence issue

Broadcast storm

- a failing NIC or application may cause a situation in which a broadcast storm is created
    - the NIC goes down and then comes back up repeatedly --- referred to as a **flapping NIC**. Each time it comes up, it sends out a broadcast advertising its status, which creates traffic congestion.

Routing loop

- similar in nature to the switching loop, but involves the routing process. This is more likely to occur with older routing protocols (e.g., RIP v2) but may also occur due to a misconfiguration of routers (e.g., multiple static routes to the same location)
    - often, switching to a newer routing protocol (e.g., OSPF) will resolve or banish routing loops

Other routing problems

- routing problems can manifest themselves in many different ways including:
    - missing IP routes
    - failure to discover neighboring devices
    - failure to connect to neighboring devices
- when routing problems are suspected, it is necessary to escalate the issue to the proper technical team

Mismatched maximum transmission unit (MTU) or the MTU black hole

- different types of WAN connections have different **MTU setting**s --- the largest allowable size of a packet that can traverse the link or be accepted by the link
    - routers will negotiate the MTU between links using **ICMP**
- if ICMP has been disabled on the routers, when a router receives a packet that exceeds the MTU, it will not respond and will drop the packet
    - the sending router continues to send the oversized packets into the MTU black hole

NIC teaming

- the process of bonding multiple NICs on a single system for the purposes of increasing bw, or for failover purposes
    - a misconfiguration may actually cause a loss of performance or, in a worse case scenario, the total loss of functionality

Power failure or power anomalies

- power failures are easy to diagnose, but may be difficult to recover from. While battery backups and generators may mitigate the issue, they will not resolve the problem
    - if the problem occurs within the building, contact the appropriate group responsible for building maintenance
    - if the problem occurs outside the building, contact the appropriate utility
- electronic devices are sensitive to power issues. Anomalies in the quality of the electricity delivered to a device may cause problems
    - using battery backups combined with power conditioners will help to mitigate power anomalies.

Problems to resolve

Incorrect IP configuration

Default gateway

- local nw's or computer's access to the outside. An incorrect gateway will keep traffic from reaching its destination.
    - verify the correct gateway settings and correct

Duplicate IP address

- when duplicate IP addresses have been configured, the first device booted up will get the address and the second one up will get an address supplied by **APIPA (automatic private IP addressing)**
    - can occur when DHCP address reservation has not been configured correctly
    - verify and correct the configuration

DHCP misconfiguration

- the problem is expressed in a similar manner as the duplicate IP address problem and is caused by a misconfiguration of DHCP
    - verify DHCP settings and correct

DNS misconfiguration

- users complain that they cannot get to resources or destinations on the nw when using the hostname. DNS resolves hostnames to IP addresses, so a misconfiguration will prevent the function of the process
    - verify the correct DNS settings and correct

Incorrect VLAN assignment

- users complain that they cannot get to necessary nw resources
    - tends to be a single host issue or involve a small group of hosts
    - verify VLAN settings and correct as necessary

Incorrect interface configuration

- users complain of poor nw performance, or not being able to connect to resources at all
    - tends to affect a whole nw segment
    - configuration issues could include: mismatched port speeds and/or duplex settings on the interfaces
    - verify the correct interface configurations and correct the settings

Simultaneous wireless and wired connection

- many laptops come with wireless and wired nw capabilities built into them. It is possible for a laptop to attempt to use both at the same time. This may cause the device to quit communicating on the nw.
    - reminding users to turn off wireless capabilities before joining the wired nw will resolve the problem

End-to-end connectivity

- the complexity of nws will just about guarantee that end-to end connectivity --- the ability to reach remote hosts --- will be lost at some point
    - the **ping** and **tracert** utilities can be used to find where the break in communication occurs. This info can be used to determine the next course of action.

Hardware failure

- nwing equipment and devices will fail. When this happens, it is usually denoted by the sudden loss or intermittent(间歇性的) loss -- in the case of failing equipment --- of function or access.
    - determining what failed and replacing it