CSF 432: Intro to Network and System Security

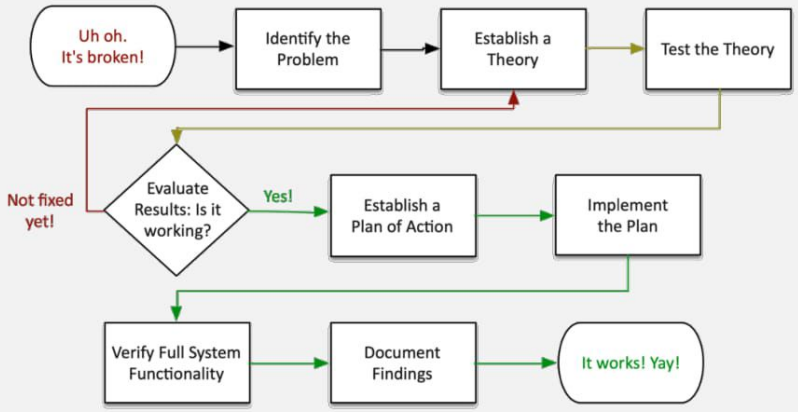
Week 13 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

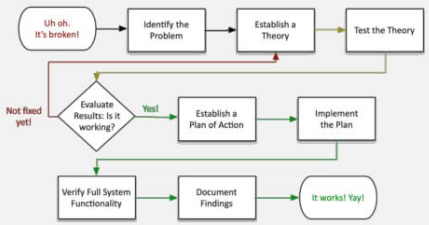
Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Network Troubleshooting Methodology



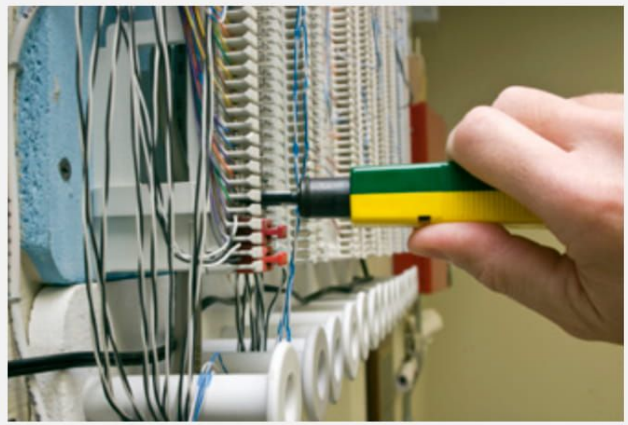
Network Troubleshooting Methodology

Network Troubleshooting Methodology



- ☑ Identify the problem
  - ☑ Information gathering, identify symptoms, question users
- ☑ Establish a theory of probable cause
- ☑ Test the theory to determine cause
- ☑ Establish a plan of action to resolve the problem and identify potential effects
- ☑ Implement the solution or escalate as necessary
- ☑ Verify full system functionality and, if applicable, implement preventative measures
- ☑ Document findings, actions and outcomes

Hardware Tools



Hardware Tools

Cable crimper

- ☑ ”Pinch” the connector onto the wire
- ☑ The final step of a cable installation
- ☑ Metal prongs push through insulation

Cable tester

- ☑ Continuity testing
- ☑ Identify missing pins, crossed wires
- ☑ Not used for advanced testing

Hardware Tools

Punch-down Tool

- ☑ Forces wire into a wiring block
- ☑ Trims the wires and breaks the insulation

TDR / OTDR

- ☑ (Optical) Time Domain Reflectometer
- ☑ Estimate fiber lengths, measure signal loss, determine light reflection, create wire maps, splice locations
- ☑ May require additional training

Hardware Tools

Light meter

- ☑ Send a light from one side
- ☑ Measure the light power on the other

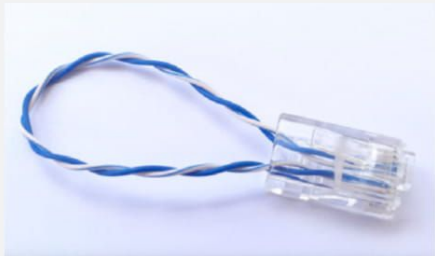
Toner Probe

- ☑ Puts an analog sound on the wire
- ☑ Inductive probe doesn’t need to touch the copper

Hardware Tools

Loopback plug

- ☑ Useful for testing physical ports
- ☑ Serial, Ethernet, T1, fiber
- ☑ These are not crossover cables



Multimeter

- ☑ AC/DC voltages
- ☑ Continuity, wire mapping

Hardware Tools

Spectrum analyzer

- ☑ View the frequency spectrum
- ☑ Identify frequency conflicts
- ☑ View everything communicating in the wireless frequency spectrum

Software Tools

WIRESHARK

NMAP PROJECT

Software Tools

Protocol analyzer

- ☑ Capture and display network traffic
- ☑ Use a physical tap or redirect on the switch

WIRESHARK

Network / Port scanner

- ☑ Scan for open ports and IP addresses
- ☑ Visually map the network
- ☑ Rogue system detection

NMAP PROJECT

Software Tools

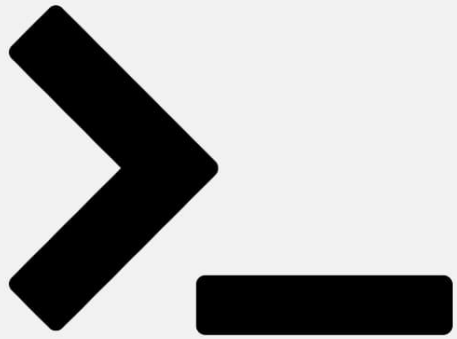
Wireless packet analysis

- ☑ View wireless information
- ☑ Signal-to-noise ratio, channel information, etc.

Speed test sites

- ☑ Bandwidth testing
- ☑ Pre- and post-change analysis
- ☑ Not all sites are the same

Command Line Tools



Command Line Tools

ping - Test reachability

- ☑ *ping <ip address>* - Test reachability to a TCP/IP address
- ☑ *ping -t <ip address>* - Ping until stopped with Ctrl-c
- ☑ *ping -a <ip address>* - Resolve address to a hostname
- ☑ *ping -n <count> <ip address>* - Send # of echo requests
- ☑ *ping -f <ip address>* - Send with 'Don't Fragment' flag set

Command Line Tools

traceroute - Determine the route a packet takes to a destination

- ☑ Takes advantage of ICMP Time to Live Exceeded error message
- ☑ Not all devices will reply with ICMP Time Exceeded messages
- ☑ *traceroute <ip address>*

nslookup and dig - Lookup information from DNS servers

- ☑ *nslookup <ip address>*
- ☑ *dig <ip address>*

Command Line Tools

ipconfig and ifconfig - View and manage IP configuration

- ☑ *ipconfig* - Windows TCP/IP config
- ☑ *ipconfig /all* - Display all IP configuration details
- ☑ *ipconfig /release* - Release the DHCP lease
- ☑ *ipconfig /renew* - Renew the DHCP lease
- ☑ *ipconfig /flushdns* - Flush the DNS resolver cache
- ☑ *ifconfig* - Linux interface configuration

Command Line Tools

iptables - Packet filtering

- Linux iptables - filter packets in the kernel
- Simple data blocks - ignores state
- Usually placed on a device or server

netstat - Display network statistics

- *netstat -a* - Show all active connections
- *netstat -b* - Show binaries
- *netstat -n* - Do not resolve names

Command Line Tools

tcpdump

- Capture packets from the command line
- Available in most Unix/Linux operating systems
  - Included with Mac OS X, available for Windows (WinDump)
- Apply filters, view in real-time
- Written in standard pcap format

pathping - Combination of ping and traceroute

- *pathping <ip address>*

Command Line Tools

Nmap

- Network mapper - find network devices
- Port scan - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device?
    - Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE)

Command Line Tools

route - View the device's routing table

- *route print* - View the Windows routing table

arp - Address resolution protocol information

- *arp -a* - View the local ARP table

Wired Network Troubleshooting

Wired Network Troubleshooting

Signal loss

- Usually gradual
  - Signal strength diminishes over distance
- Attenuation
  - Loss of intensity as signal moves through a medium
- Electrical signals through copper, light through fiber
  - Radio waves through the air

Wired Network Troubleshooting

Decibels (dB)

- Signal strength ratio measurements
  - One-tenth of a bel
  - Capital B for Alexander Graham Bell
- Logarithmic scale
  - Add and subtract losses and gains
- 3 dB = 2x the signal
- 10 dB = 10x the signal
- 20 dB = 100x the signal
- 30 db = 1000x the signal

Wired Network Troubleshooting

dB loss symptoms

- No connectivity
  - No signal!
- Intermittent connectivity
  - Just enough signal to sync the link
- Poor performance
  - Signal too weak
  - CRC errors, data corruption
- Test each connection
  - Test distance and signal loss

Wired Network Troubleshooting

Latency

- A delay between the request and the response
  - Waiting time
- Some latency is expected and normal
  - Laws of physics apply
- Examine the response times at every step along the way
  - This may require multiple measurement tools
- Packet captures can provide detailed analysis
  - Microsecond granularity
  - Get captures from both sides

Wired Network Troubleshooting

Jitter

- Most real-time media is sensitive to delay
  - Data should arrive at regular intervals
  - Voice communication, live video
- If you miss a packet, there's no retransmission
  - There's no time to "rewind" your phone call
- Jitter is the time between frames
  - Excessive jitter can cause you to miss information, "choppy" voice calls

Wired Network Troubleshooting

Troubleshooting excessive jitter

- Confirm available bandwidth
  - Nothing will work well if the tube is clogged
- Make sure the infrastructure is working as expected
  - Check queues in your switches and routers
  - No dropped frames
- Apply QoS (Quality of Service)
  - Prioritize real-time communication services
  - Switch, router, firewall, etc.

Wired Network Troubleshooting

Crosstalk (XT)

- Signal on one circuit affects another circuit
  - In a bad way
- Leaking of signal
  - You can sometimes "hear" the leak
- Measure XT with cable testers
  - Some training may be required
- Near End Crosstalk (NEXT)
  - Interference measured at the transmitting end (the near end)
- Far End Crosstalk (FEXT)
  - Interference measured away from the transmitter

Wired Network Troubleshooting

Troubleshooting crosstalk

- Almost always a wiring issue
  - Check your crimp
- Maintain your twists
  - The twist helps to avoid crosstalk
- Category 6A increases cable diameter
  - Increased distance between pairs
- Test and certify your installation
  - Solve problems before they are problems

Wired Network Troubleshooting

Avoiding EMI and interference

- Electromagnetic interference
- Cable handling
  - No twisting - don't pull or stretch
  - Watch your bend radius
  - Don't use staples, watch your cable ties
- EMI and interference with copper cables
  - Avoid power cords, fluorescent lights, electrical systems, and fire prevention components
- Test after installation
  - You can find most of your problems before use

Wired Network Troubleshooting

Opens and shorts

- A short circuit
  - Two connections are touching
  - Wires inside of a cable or connection
- An open circuit
  - A break in the connection
- Complete interruption
  - Can be intermittent

Wired Network Troubleshooting

Troubleshooting opens and shorts

- May be difficult to find
  - The wire has to be moved just the right way
  - Wiggle it here and there
- Replace the cable with the short or open
  - Difficult or impossible to repair
- Advanced troubleshooting with a TDR
  - Time Domain Reflectometer

Wired Network Troubleshooting

Troubleshooting pin-outs

- Cables can foul up a perfectly good plan
  - Test your cables prior to implementation
- Many connectors look alike
  - Do you have a good cable mapping device?
- Get a good cable person
  - It's an art

Wired Network Troubleshooting

T568A and T568B termination

- Pin assignments from EIA/TIA-568-B standard
  - Eight conductor 100-ohm balanced twisted-pair cabling
- T568A and T568B are different pin assignments for 8P8C connectors
  - Assigns the T568A pin-out to horizontal cabling
- Many organizations traditionally use 568B
  - Difficult to change in mid-stream
- You can't terminate one side of the cable with 568A and the other with 568B
  - It won't be a straight-through cable

Wired Network Troubleshooting

Incorrect cable type

- Excessive physical errors, CRC errors
  - Check your layer 1 first
- Check the outside of the cable
  - Usually printed on the outside
  - May also have length marks printed
- Confirm the cable specifications with a TDR
  - Advanced cable tester can identify damaged cables

Wired Network Troubleshooting

Troubleshooting interfaces

- Interface errors
  - May indicate bad cable or hardware problem
- Verify configurations
  - Speed, duplex, VLAN, etc.
- Verify two-way traffic
  - End-to-end connectivity

Wired Network Troubleshooting

Transceiver mismatch

- Transceivers have to match the fiber
  - Single mode transceiver connects to single mode fiber
- Transceiver needs to match the wavelength
  - 850nm, 1310nm, etc.
- Use the correct transceivers and optical fiber
  - Check the entire link
- Signal loss
  - Dropped frames, missing frames

Wired Network Troubleshooting

Reversing transmit and receive

- Wiring mistake
  - Cable ends
  - Punchdowns
- Easy to find with a wire map
  - 1-3, 2-6, 3-1, 6-2
  - Simple to identify
- Some network interfaces will automatically correct (Auto-MDIX)

Wired Network Troubleshooting

Damaged cables

- Copper cables are pretty rugged
  - But they aren't indestructible
- Cables can be out in the open
  - Stepped on, folded between a table and wall
- Check your physical layer
  - Cables should not be bent or folded
  - Check for any bent pins on the device
- It's difficult to see inside of the cable
  - Check your TDR, replace the cable (if possible)

Wired Network Troubleshooting

Bottlenecks

- There's never just one performance metric
  - A series of technologies working together
- I/O bus, CPU speed, storage access speed, network throughput, etc.
  - One of these can slow all of the others down
- You must monitor all of them to find the slowest one
  - This may be more difficult than you might expect

Wired Network Troubleshooting

Interface configuration problems

- Poor throughput
  - Very consistent, easily reproducible
- No connectivity
  - No link light
- No connectivity
  - Link light and activity light

Wired Network Troubleshooting

Interface configuration

- Auto vs. Manual configuration
  - Personal preference
- Light status
  - No light, no connection
- Speed
  - Must be identical on both sides
- Duplex
  - If mismatched, speed will suffer

Wired Network Troubleshooting

VLAN mismatch

- Switch is configured with the incorrect VLAN
  - Configured per switch interface
- Link light, but no surfing
  - A DHCP IP address may not be on the correct subnet
  - Manually IP addressing won't work at all
- Check the switch configuration for VLAN configuration
  - Each port should have a VLAN setting
  - VLAN 1 is usually the default

Wireless Network Troubleshooting

Wireless Network Troubleshooting

Reflection

- Wireless signals can bounce off some surfaces
  - Depends on the frequencies and the surfaces
- Too much reflection can weaken the signal
  - A little multipath interference actually helps with MIMO
- Position antennas to avoid excessive reflection
  - May not be a problem for MIMO in 802.11n and 802.11ac

Wireless Network Troubleshooting

Refraction

- Signal passes through an object and exits at a different angle
  - Similar to light through water
- Data rates are affected - Signal is less directional
- Outdoor long-distance wireless links
  - Changes in air temperature and water vapor

Wireless Network Troubleshooting

Absorption

- Signal passes through an object and loses signal strength
  - Especially through walls and windows
- Different objects absorb differently as frequencies change
  - 2.4 GHz may have less absorption than 5 GHz
- Put the antennas on the ceiling
  - And avoid going through walls

Wireless Network Troubleshooting

Latency and jitter

- Latency - Delays between transmission and reception
- Jitter - Deviation from a predictable data stream
- Wireless interference and signal issues
  - Slower data rates
  - Increase in retransmissions
- Capacity issues
  - Many people using the same wireless frequencies

Wireless Network Troubleshooting

Attenuation

- Wireless signals get weaker as you move farther from the antenna
  - The attenuation can be measured with a Wi-Fi analyzer
- Control the power output on the access point
  - Not always an option
- Use a receive antenna with a higher gain
  - Capture more of the signal
- Move closer to the antenna - May not be possible

Wireless Network Troubleshooting

Interference

- Interference
  - Something else is using our frequency
- Predictable
  - Florescent lights, microwave ovens, cordless telephones, high-power sources
- Unpredictable - Multi-tenant building
- Measurements
  - *netstat –e*
  - Performance Monitor

Wireless Network Troubleshooting

Incorrect antenna type

- The antenna must fit the room
  - Or the distance between sender and receiver
- Omnidirectional
  - Useful on the ceiling
  - Not very useful between buildings
- Directional
  - Used often between two points
  - Or on a wall-mounted access point
- The access point may provide options
  - Connect different antennas

Wireless Network Troubleshooting

Incorrect antenna placement

- Interference
  - Overlapping channels
- Slow throughput
  - Data fighting to be heard through the interference
- Check access point locations and channel settings
  - A challenge for 2.4 GHz
  - Much easier for 5 GHz

Wireless Network Troubleshooting

Overcapacity

- Device saturation
  - Too many devices on one wireless network
  - There are only so many frequencies
  - The 5 GHz can really help with this
- Bandwidth saturation
  - Large data transfers
- Common in large meeting places
  - Conferences
  - Airports
  - Hotels

Wireless Network Troubleshooting

Frequency mismatch

- Devices have to match the access point
  - 2.4 GHz, 5 GHz
- Verify the client is communicating over the correct channel
  - This is normally done automatically
  - May not operate correctly if manually configured
- Confirm the correct SSID settings
  - Should be listed in the current connection status
- Older standards may slow down the newer network
  - 802.11b compatibility mode on 802.11n networks
- Every access point has an SSID
  - But did you connect to the right one?
- This can be more confusing than you might think
  - Public Wi-Fi Internet
  - Guest Internet
  - Internet

Wireless Network Troubleshooting

Wrong passphrase

- Wireless authentication
  - Many different methods
- Required to connect to the wireless network
  - If not connected, check the authentication
- Shared passphrase
  - Common in a SOHO, not in the enterprise
- 802.1X
  - Used for the enterprise
  - Make sure the client is configured to use 802.1X

Wireless Network Troubleshooting

Security type mismatch

- Encryption on wireless is important
  - Make sure the client matches the access point
- This is much easier these days
  - Almost everything is at the level of WPA2
- Some legacy equipment may not be able to keep up
  - If you change the access point, you may not be able to support it
- Migrate all of your WEP to WPA2
  - And any WPA

Wireless Network Troubleshooting

Signal to noise ratio

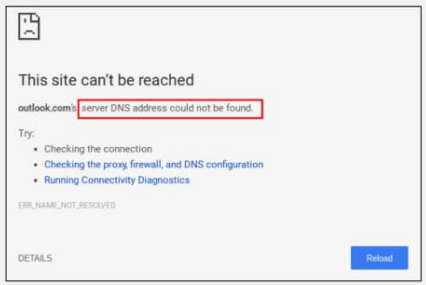
- Signal
  - What you want
- Noise
  - What you don't want
  - Interference from other networks and devices
- You want a very large ratio
  - The same amount of signal to noise (1:1) would be bad

Network Service Troubleshooting

Network Service Troubleshooting

Names not resolving

- Web browsing doesn't work
  - The Internet is broken!
- Pinging the IP address works
  - There isn't a communication problem
- Applications aren't communicating
  - They often use names and not IP addresses



Network Service Troubleshooting

Troubleshooting DNS issues

- Check your IP configuration
  - Is the DNS IP address correct?
- Use nslookup or dig to test - Does resolution work?
- Try a different DNS server - Google is 8.8.8.8 & 8.8.4.4

Network Service Troubleshooting

IP configuration issues

- Communicate to local IP addresses
  - But not outside subnets
- No IP communication - Local or remote
- Communicate to some IP addresses - But not others

Network Service Troubleshooting

Troubleshooting IP configurations

- Check your documentation
  - IP address, subnet mask, gateway
- Monitor the traffic
  - Examine local broadcasts
  - Difficult to determine subnet mask
- Check devices around you
  - Confirm your subnet mask and gateway
- Traceroute and ping
  - The issue might be your infrastructure
  - Ping local IP, default gateway, and outside address

Network Service Troubleshooting

Duplicate IP addresses

- Static address assignments - Must be very organized
- DHCP isn't a panacea
  - Static IP addressing
  - Multiple DHCP servers overlap
  - Rogue DHCP servers
- Intermittent connectivity
  - Two addresses "fight" with each other
- Blocked by the OS - Checks when it starts

Network Service Troubleshooting

Troubleshooting duplicate IP addresses

- Check your IP addressing - Did you misconfigure?
- Ping an IP address before static addressing
  - Does it respond?
- Determine the IP addresses
  - Ping the IP address, check your ARP table
  - Find the MAC address in your switch MAC table
- Capture the DHCP process
  - What DHCP servers are responding?

Network Service Troubleshooting

Duplicate MAC addresses

- Not a common occurrence
  - MAC addresses are designed to be unique
  - May be a man-in-the-middle attempt
- Mistakes can happen
  - Locally administered MAC addresses
  - Manufacturing error
- Intermittent connectivity
  - Confirm with a packet capture, should see ARP contention
- Use the ARP command from another computer
  - Confirm the MAC matches the IP

Network Service Troubleshooting

Expired IP addresses

- A DHCP address should renew well before the lease expires
  - The DHCP server(s) could be down
- Client gives up the IP address at the end of the lease
  - APIPA address is assigned
  - Checks in occasionally for a DHCP server
- Look for an APIPA assigned address
  - 169.254.*.*
- Check the status of your DHCP server

Network Service Troubleshooting

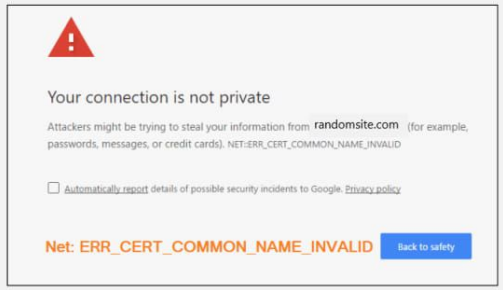
Rogue DHCP server

- IP addresses assigned by a non-authorized server
  - There's no inherent security in DHCP
- Client is assigned an invalid or duplicate address
  - Intermittent connectivity, no connectivity
- Disable rogue DHCP communication
  - Enable DHCP snooping on your switch
  - Authorized DHCP servers in Active Directory
- Disable the rogue
  - Renew the IP leases

Network Service Troubleshooting

Untrusted SSL certificate

- Browsers trust signatures from certain CAs
  - A certificate was signed by a CA that's not in our list
- Error message on the browser
  - Certificate Authority Invalid
- Check the certificate details
  - Look for the issuing CA
  - Compare to the CA list on your computer
- If it's an internal server, it may be internally signed
  - Add your internal CA certificate to the list



Network Service Troubleshooting

Incorrect time

- Some cryptography is very time sensitive
  - Active Directory requires clocks set within five minutes of each other
- Kerberos communication uses a time stamp
  - If the ticket shown during authentication is too old, it's invalid
- Client can't login
  - Check the timestamp of the client and the server
- Configure NTP on all devices
  - Automate the clock setting

Network Service Troubleshooting

Exhausted DHCP scope

- Client received an APIPA address
  - Local subnet communication only
- Check the DHCP server
  - Add more IP addresses if possible
- IP address management (IPAM) may help
  - Monitor and report on IP address shortages
- Lower the lease time
  - Especially if there are a lot of transient users

Network Service Troubleshooting

Blocked TCP/UDP ports

- Applications not working
  - Slowdowns with other applications
- Firewall or ACL configuration
  - Security choke points
- Confirm with a packet capture
  - No response to requests
- Run a TCP- or UDP-based traceroute tool
  - See how far your packet can go

Network Service Troubleshooting

Incorrect host-based firewall setting

- Applications not working
  - Based on the application in use and not necessarily the protocol and port
- Check the host-based firewall settings
  - Accessibility may be limited to an administrator
  - Managed from a central console
- Take a packet capture
  - The traffic may never make it to the network
  - Dropped by the operating system

Network Service Troubleshooting

Incorrect ACL setting

- Only certain IP addresses accessible
  - Or none
- Access Control Lists
  - IP address, port numbers, and other parameters
  - Can allow or deny traffic by filtering packets
- Confirm with packet captures and TCP/UDP traceroutes
  - Identify the point of no return

Network Service Troubleshooting

Unresponsive service

- No response to an application request
  - No answer
- Do you have the right port number?
  - And protocol (TCP/UDP)?
- Confirm connectivity
  - Ping, traceroute
- Is the application still working?
  - Telnet to the port number and see if it responds

Network Service Troubleshooting

Hardware failure

- No response
  - Application doesn't respond
- Confirm connectivity
  - Without a ping, you're not going to connect
- Run a traceroute
  - See if you're being filtered
  - Should make it to the other side
- Check the server
  - Lights? Fire?

CSF 432: Intro to Network and System Security

Week 13 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes