Professor Messer

Professor Messer's

CompTIA Network+

N10-008

Course Notes

James "Professor" Messer

Professor Messer's CompTIA N10-008 Network+ Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's CompTIA N10-008 Network+ Course Notes
Written by James "Professor" Messer

https://www.ProfessorMesser.com

First Edition: August 2021
This is version 1.05.

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA N10-008 Network+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

Introduction

The network is the foundation of information technology. Careers in workstation management, server administration, IT security, or data center operations will all include an aspect of networking. If you're going to do anything technical, then you're also going to use the network.

CompTIA's Network+ certification provides an overview of network devices, infrastructure and wiring, network security, and much more. These Course Notes will help you with the details you'll need for the exam. Best of luck with your studies!

- Professor Messer

The CompTIA Network+ certification

To earn the Network+ certification, you must pass a single N10-008 certification exam. The exam is 90 minutes in duration and includes both multiple choice questions and performance-based questions. Performance-based questions can include fill-in-the-blank, matching, sorting, and simulated operational environments. You will need to be very familiar with the exam topics to have the best possible exam results.

Here's the breakdown of each technology section and the percentage of each topic on the N10-008 exam:

Section 1.0 - Networking Fundamentals - 24%
Section 2.0 - Network Implementations - 19%
Section 3.0 - Network Operations - 16%
Section 4.0 - Network Security - 19%
Section 5.0 - Network Troubleshooting - 22%

CompTIA provides a detailed set of exam objectives that provide a list of everything you need to know before you take your exam. You can find a link to the exam objectives here:

https://www.professormesser.com/objectives/

How to use this book

Once you're comfortable with all of the sections in the official CompTIA N10-008 exam objectives, you can use these notes as a consolidated summary of the most important topics. These Course Notes follow the same format and numbering scheme as the official exam objectives, so it should be easy to cross reference these notes with the Professor Messer video series and all of your other study materials.

Study Tips

Exam Preparation

- Download the exam objectives, and use them as a master checklist
- Use as many training materials as possible. Books, videos, and Q&A guides can all provide a different perspective of the same information.
- It's useful to have some hands-on, especially with network troubleshooting commands.

Taking the Exam

- Use your time wisely. You've got 90 minutes to get through everything.
- Choose your exam location carefully. Some sites are better than others.
- Get there early. Don't stress the journey.
- Wrong answers aren't counted against you. Don't leave any blanks!
- Mark difficult questions and come back later. You can answer the questions in any order.


Professor
Messer

Professor Messer's

CompTIA Network+

N10-008 Course Notes

http://www.ProfessorMesser.com

1.1 - Understanding the OSI Model

Open Systems Interconnection Reference Model
- It's a guide (thus the term "model")
  - Don't get wrapped up in the details
- This is not the OSI protocol suite
  - Most of the OSI protocols didn't catch on
- There are unique protocols at every layer
- You'll refer to this model for the rest of your career

Layer 1 - The Physical Layer
- The physics of the network
  - Signaling, cabling, connectors
  - This layer isn't about protocols
- You have a physical layer problem."
  - Fix your cabling, punch-downs, etc.
  - Run loopback tests, test/replace cables, swap adapter cards

Layer 2 - Data Link Layer
- The basic network "language"
  - The foundation of communication at the data link layer
- Data Link Control (DLC) protocols
  - MAC (Media Access Control) address on Ethernet
- The "switching" layer

Layer 3 - The Network Layer
- The "routing" layer
- Internet Protocol (IP)
- Fragments frames to traverse different networks

What is IP Fragmentation?
- Fragments are always in multiples of 8 because of the number of fragmentation offset bits in the IP header

Layer 4 - Transport Layer
- The "post office" layer
  - Parcels and letters
- TCP (Transmission Control Protocol) and UDP (UserDatagram Protocol)

Layer 5 - Session Layer
- Communication management between devices
  - Start, stop, restart
- Half-duplex, full-duplex
- Control protocols, tunneling protocols

Layer 6 - Presentation Layer
- Character encoding
- Application encryption
- Often combined with the Application Layer

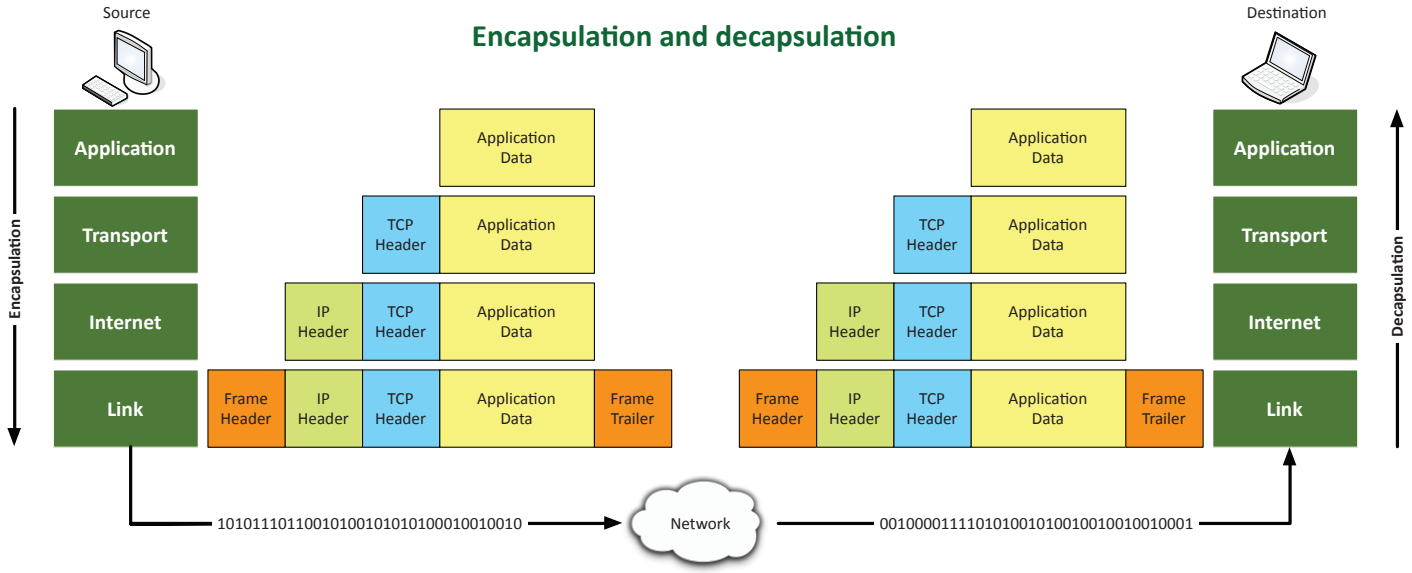
Layer 7 - Application Layer
- The layer we see - HTTP, FTP, DNS, POP3

Follow the conversation
- Application: https://mail.google.com
- Presentation: SSL encryption
- Session: Link the presentation to the transport
- Transport: TCP encapsulation
- Network: IP encapsulation
- Data Link: Ethernet
- Physical: Electrical signals

OSI Model Mnemonics
- Please Do Not Trust Sales Person's Answers
- All People Seem To Need Data Processing
- Please Do Not Throw Sausage Pizza Away!

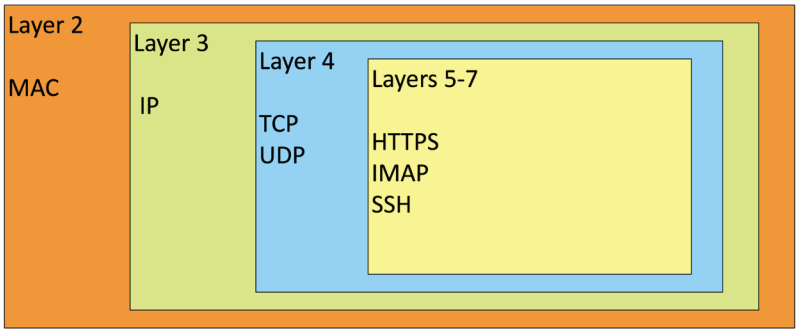
Layer 7 - Application	The layer we see - Google Mail, Twitter, Facebook
Layer 6 - Presentation	Encoding and encryption (SSL/TLS)
Layer 5 - Session	Communication between devices (Control protocols, tunneling protocols)
Layer 4 - Transport	The "post office" layer (TCP segment, UDP datagram)
Layer 3 - Network	The routing layer (IP address, router, packet)
Layer 2 - Data Link	The switching layer (Frame, MAC address, EUI-48, EUI-64, Switch)
Layer 1 - Physical	Signaling, cabling, connectors (Cable, NIC, Hub)

1.1 - Data Communication



Transmitting data

- Transmission units
  - A different group of data at different OSI layers
- Ethernet operates on a frame of data
  - It doesn't care what's inside
- IP operates on a packet of data
  - Inside is TCP or UDP, but IP doesn't really care
- TCP or UDP
  - TCP segment
  - UDP datagram



TCP flags

- The header describes or identifies the payload
  - Here's what you're about to see…
- The TCP header contains important control information
  - Includes a set of bits called TCP flags
- The flags control the payload
  - SYN - Synchronize sequence numbers
  - PSH - Push the data to the application without buffering
  - RST - Reset the connection
  - FIN - Last packet from the sender


```
Flags: 0x010 (ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: ·····A····]
```

Maximum Transmission Unit (MTU)

- Maximum IP packet to transmit
  - But not fragment
- Fragmentation slows things down
  - Losing a fragment loses an entire packet
  - Requires overhead along the path
- Difficult to know the MTU all the way through the path
  - Automated methods are often inaccurate
  - Especially when ICMP is filtered

```
Internet Protocol Version 4, Src: 10.1.10.249, Dst: 10.1.10.234
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x0000 (0)
  Flags: 0x4000, Don't fragment
    0... .... .... .... = Reserved bit: Not set
    .1.. .... .... .... = Don't fragment: Set
    ..0. .... .... .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.1.10.249
  Destination: 10.1.10.234
```

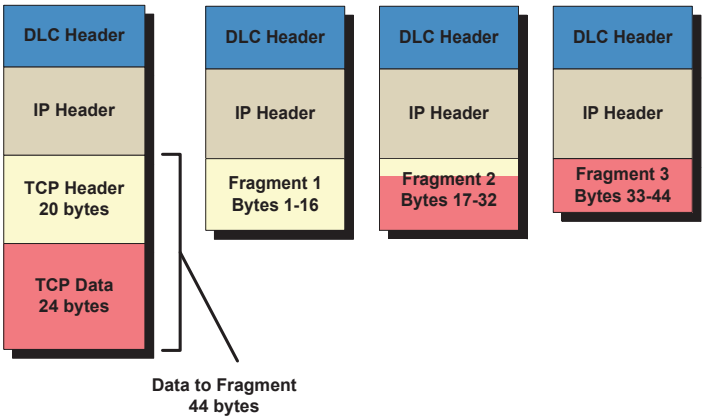
1.1 - Data Communication (continued)

Troubleshooting MTU

- MTU sizes are usually configured once
  - Based on the network infrastructure and don't change often
- A significant concern for tunneled traffic
  - The tunnel may be smaller than your local Ethernet segment
- What if you send packets with Don't Fragment (DF) set?
  - Routers will respond back and tell you to fragment
  - Hope you get the ICMP message!
- Troubleshoot using ping
  - Ping with DF and force a maximum size of 1472 bytes

    1500 bytes - 8 byte ICMP header
    - 20 bytes IP address = 1472 bytes

  - Windows: `ping -f -l 1472 8.8.8.8`



- Fragments are always in multiples of 8 because of the number of fragmentation offset bits in the IP header

1.2 - Network Topologies

Network Topologies

- Useful in planning a new network
  - Physical layout of a building or campus
- Assists in understanding signal flow
  - Troubleshooting problems

Star

- Hub and spoke
- Used in most large and small networks
- All devices are connected to a central device
- Switched Ethernet networks
  - The switch is in the middle

Ring

- Used in many popular topologies
  - Token Ring is no longer with us
- Still used in many Metro Area Networks (MANs) and Wide Area Networks (WANs)
  - Dual-rings
  - Built-in fault tolerance

Bus

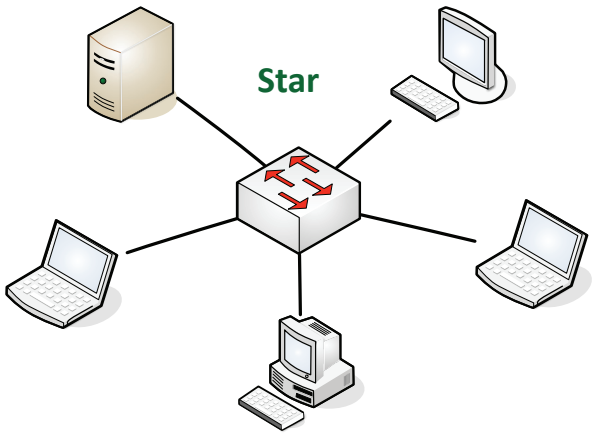
- Early local area networks
  - Coaxial cable was the bus
- Simple, but prone to errors
  - One break in the link disabled the entire network
- Controller Area Network
  - CAN bus

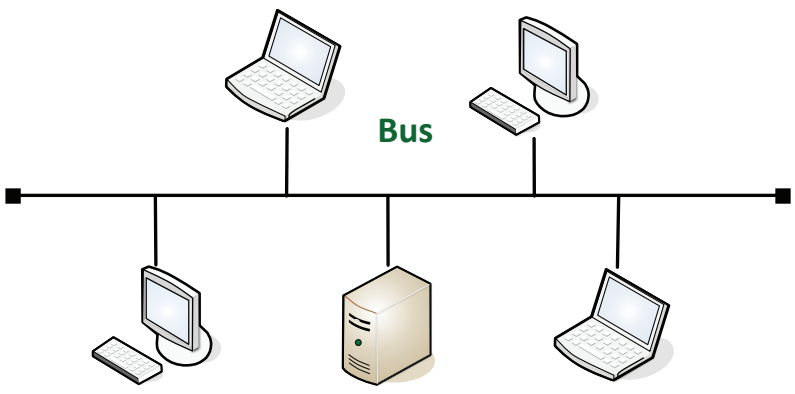
Mesh

- Multiple links to the same place
  - Fully connected
  - Partially connected
- Redundancy, fault-tolerance, load balancing
- Used in wide area networks (WANs)
  - Fully meshed and partially meshed

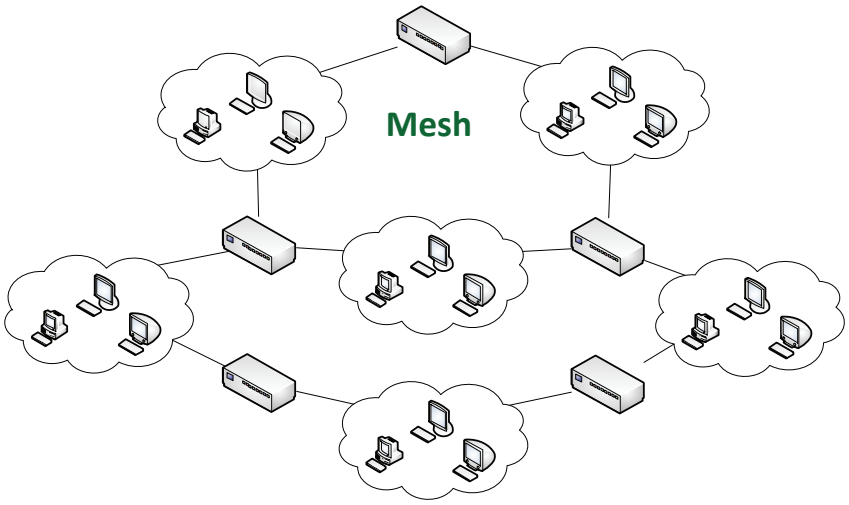
Hybrid

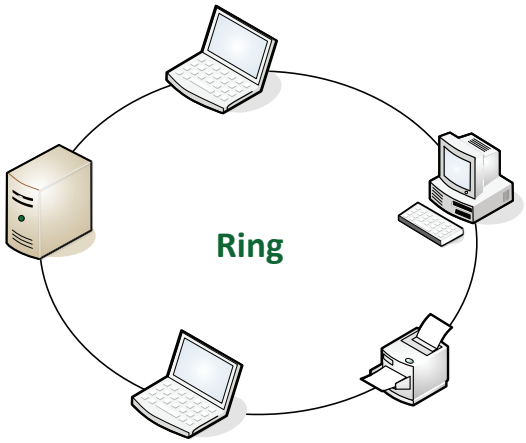
- A combination of one or more physical topologies
  - Most networks are a hybrid

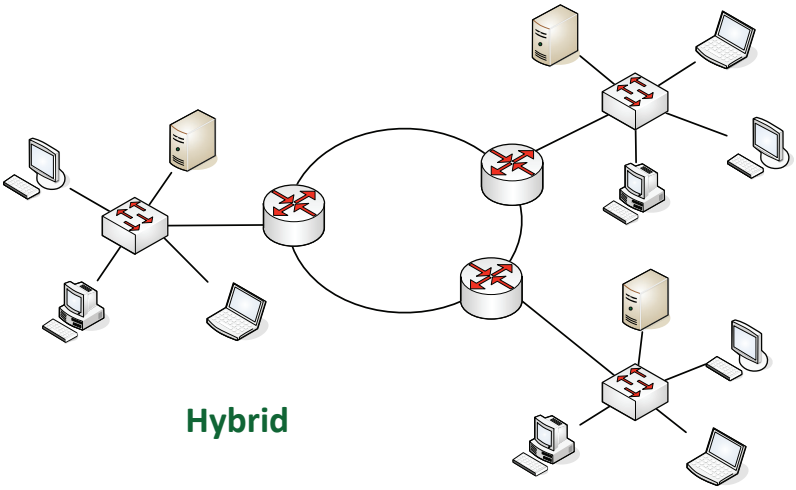




1.2 - Network Topologies (continued)







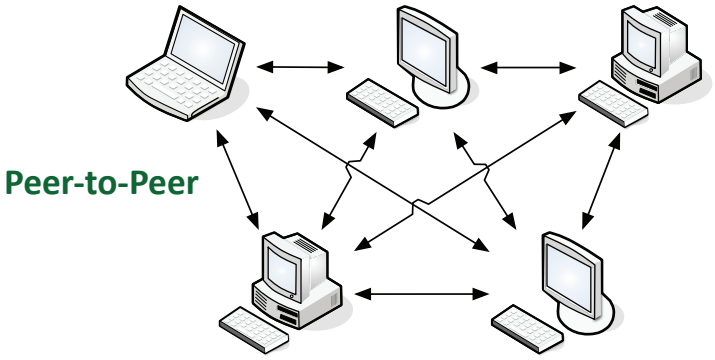
Wireless topologies

- Infrastructure
  - All devices communicate through an access point
  - The most common wireless communication mode
- Ad hoc networking
  - No preexisting infrastructure
  - Devices communication amongst themselves
- Mesh
  - Ad hoc devices work together to form a mesh "cloud"
  - Self form and self heal

1.2 - Network Types

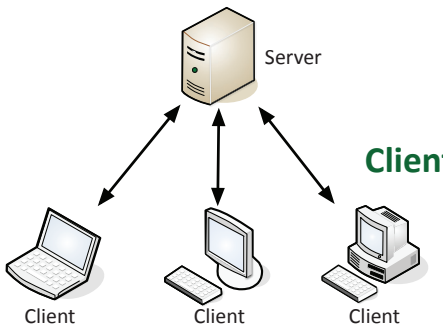
Peer-to-peer

- All devices are both clients and servers
  - Everyone talks to everyone
- Advantages
  - Easy to deploy, Low cost
- Disadvantages
  - Difficult to administer
  - Difficult to secure



Client-server

- Central server
  - Clients talk to the server
- No client-to-client communication
- Advantages
  - Performance, administration
- Disadvantages
  - Cost, complexity



1.2 - Network Types (continued)

LAN - Local Area Network
- A building or group of buildings
  - High-speed connectivity
- Ethernet and 802.11 wireless
  - Any slower and it isn't "local"

MAN - Metropolitan Area Network
- A network in your city
  - Larger than a LAN, often smaller than a WAN
- Common to see government ownership
  - They "own" the right-of-way

WAN - Wide Area Network
- Generally connects LANs across a distance
  - And generally much slower than the LAN
- Many different WAN technologies
  - Point-to-point serial, MPLS, etc.
  - Terrestrial and non-terrestrial

WLAN - Wireless LAN
- 802.11 technologies
- Mobility within a building or geographic area
- Expand coverage with additional access points

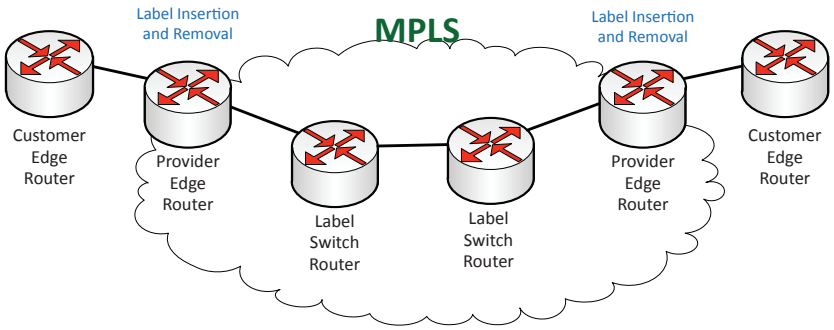
PAN - Personal Area Network
- Your own private network
  - Bluetooth, IR, NFC
- Automobile
  - Audio output
  - Integrate with phone
- Mobile phone
  - Wireless headset
- Health
  - Workout telemetry, daily reports

CAN - Campus Area Network
- Corporate Area Network
- Limited geographical area
  - A group of buildings
- LAN technologies
  - Fiber connected, high speed Ethernet
- Your fiber in the ground
  - No third-party provider

NAS vs. SAN
- Network Attached Storage (NAS)
  - Connect to a shared storage device across the network
  - File-level access
- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block-level access
  - Very efficient reading and writing
- Requires a lot of bandwidth
  - May use an isolated network and high-speed network

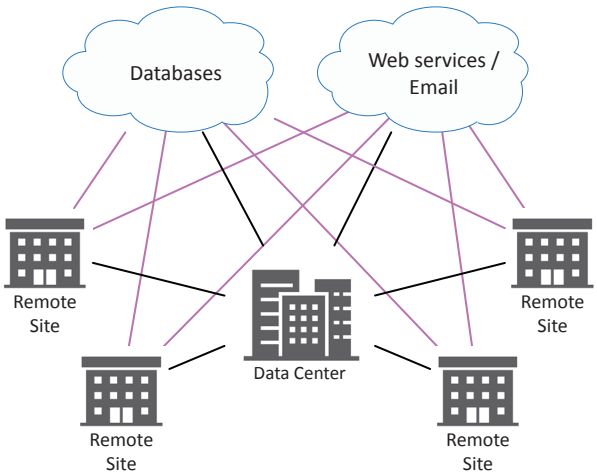
MPLS
- Learning from ATM and Frame Relay
- Packets through the WAN have a label
  - Routing decisions are easy
- Any transport medium, any protocol inside
  - IP packets, ATM cells, Ethernet frames
  - OSI layer 2.5 (!)
- Increasingly common WAN technology
  - Ready-to-network

MPLS pushing and popping
- Labels are "pushed" onto packets as they enter the MPLS cloud
- Labels are "popped" off on the way out



mGRE
- Multipoint Generic Router Encapsulation
  - Used extensively for Dynamic Multipoint VPN (DMVPN)
  - Common on Cisco routers
- Your VPN builds itself
  - Remote sites communicate to each other
- Tunnels are built dynamically, on-demand
  - A dynamic mesh

SD-WAN
- Software Defined Networking in a Wide Area Network
  - A WAN built for the cloud
- The data center used to be in one place
  - The cloud has changed everything
- Cloud-based applications communicate directly to the cloud
  - No need to hop through a central point



1.2 - WAN Termination

Demarcation point

- The point where you connect with the outside world
  - WAN provider
  - Internet service provider
  - The demarc
- Used everywhere
  - Even at home
- Central location in a building
  - Usually a network interface device
  - Can be as simple as an RJ-45 connection
- You connect your CPE
  - Customer premises equipment or "customer prem"

Smartjack

- Network interface unit (NIU)
  - The device that determines the demarc
  - Network Interface Device, Telephone Network Interface
- Smartjack
  - More than just a simple interface
  - Can be a circuit card in a chassis
- Built-in diagnostics
  - Loopback tests
- Alarm indicators
  - Configuration, status

1.2 - Virtual Networks

Virtual networks

- Server farm with 100 individual computers
  - It's a big farm
- All servers are connected with enterprise switches and routers
  - With redundancy
- Migrate 100 physical servers to one physical server
  - With 100 virtual servers inside
- What happens to the network?

Network function virtualization (NFV)

- Replace physical network devices with virtual versions
  - Manage from the hypervisor
- Same functionality as a physical device
  - Routing, switching, load balancing, firewalls, etc.
- Quickly and easily deploy network functions
  - Click and deploy from the hypervisor
- Many different deployment options
  - Virtual machine, container, fault tolerance, etc.

The hypervisor

- Virtual Machine Manager
  - Manages the virtual platform and guest operating systems
- Hardware management
  - CPU, networking, security
- Single console control
  - One pane of glass

vSwitch

- Virtual switch
  - Move the physical switch into the virtual environment
- Functionality is similar to a physical switch
  - Forwarding options, link aggregation, port mirroring, NetFlow
- Deploy from the hypervisor
  - Automate with orchestration

Virtual Network Interface Card (vNIC)

- A virtual machine needs a network interface
  - A vNIC
- Configured and connected through the hypervisor
  - Enable additional features
  - VLAN, aggregation, multiple interfaces

1.2 - Provider Links

Satellite networking

- Communication to a satellite
  - Non-terrestrial communication
- High cost relative to terrestrial networking
  - 50 Mbit/s down, 3 Mbit/s up are common
  - Remote sites, difficult-to-network sites
- High latency
  - 250 ms up, 250 ms down
- High frequencies - 2 GHz
  - Line of sight, rain fade

Copper

- Extensive installations
  - Relatively inexpensive,
  - Easy to install and maintain
- Limited bandwidth availability
  - Physics limits electrical signals through copper
- Wide area networks
  - Cable modem, DSL, T1/T3 local loop
- Often combined with fiber
  - Copper on the local loop, fiber in the backbone

1.2 - Provider Links (continued)

DSL

- ADSL (Asymmetric Digital Subscriber Line)
  - Uses telephone lines
- Download speed is faster than the upload speed (asymmetric)
  - ~10,000 foot limitation from the central office (CO)
  - 200 Mbit/s downstream / 20 Mbit/s upstream are common
  - Faster speeds may be possible if closer to the CO

Cable broadband

- Broadband
  - Transmission across multiple frequencies
  - Different traffic types
- Data on the "cable" network
  - DOCSIS (Data Over Cable Service Interface Specification)
- High-speed networking
  - 50 Mbits/s through 1,000+ Mbit/s are common
- Multiple services
  - Data, voice, video

Fiber

- High speed data communication
  - Frequencies of light
- Higher installation cost than copper
  - Equipment is more costly and more difficult to repair
  - Communicate over long distances
- Large installation in the WAN core
  - Supports very high data rates
  - SONET, wavelength division multiplexing
- Fiber is slowly approaching the premises
  - Business and home use

Metro Ethernet

- Metro-E
  - Metropolitan-area network
  - A contained regional area
- Connect your sites with Ethernet
  - A common standard
- The provider network is optical
  - Local fiber network
  - Wavelength-division multiplexing
  - High speed, multiple wavelengths of light

1.3 - Copper Cabling

The importance of cable

- Fundamental to network communication
  - Incredibly important foundation
- Usually only get one good opportunity at building your cabling infrastructure
  - Make it good!
- The vast majority of wireless communication uses cables
  - Unless you're an amateur radio operator

Twisted pair copper cabling

- Balanced pair operation
  - Two wires with equal and opposite signals
  - Transmit+, Transmit- / Receive+, Receive-
- The twist keeps a single wire constantly moving away from the interference
  - The opposite signals are compared on the other end
- Pairs in the same cable have different twist rates

Coaxial cables

- Two or more forms share a common axis
- RG-6 used in television/digital cable
  - And high-speed Internet over cable
- RG-59 used as patch cables
  - Not designed for long distances

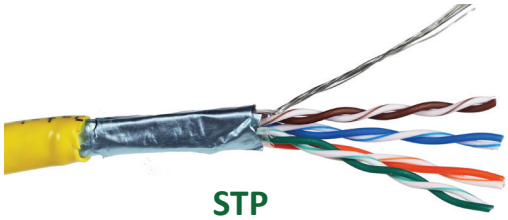
Twinaxial cables

- Two inner conductors (Twins)
- Common on 10 Gigabit Ethernet SFP+ cables
  - Full duplex, five meters, low cost, low latency compared to twisted pair

Unshielded and shielded cable

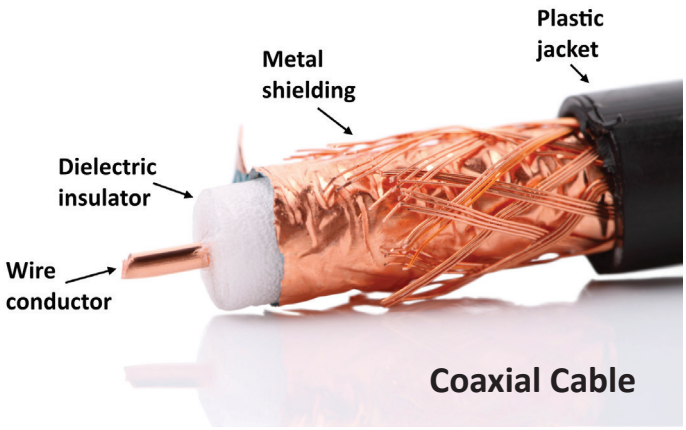
- UTP (Unshielded Twisted Pair)
  - No additional shielding
  - The most common twisted pair cabling
- STP (Shielded Twisted Pair)
  - Additional shielding protects against interference
  - Shield each pair and/or the overall cable
  - Requires the cable to be grounded
- Abbreviations
  - U = Unshielded, S = Braided shielding, F = Foil shielding
- (Overall cable) / (individual pairs)TP
  - Braided shielding around the entire cable and foil around the pairs is S/FTP
  - Foil around the cable and no shielding around the pairs is F/UTP

UTP
Unshielded Twisted Pair



STP
Shielded Twisted Pair

1.3 - Copper Cabling (continued)



Structured cabling standards

- International ISO/IEC 11801 cabling standards
  - Defines classes of networking standards
- Telecommunications Industry Association (TIA)
  - Standards, market analysis, trade shows, government affairs, etc.
  - ANSI/TIA-568: Commercial Building Telecommunications Cabling Standard
  - http://www.tiaonline.org
- Commonly referenced for pin and pair assignments of eight-conductor 100-ohm balanced twisted pair cabling
  - T568A and T568B

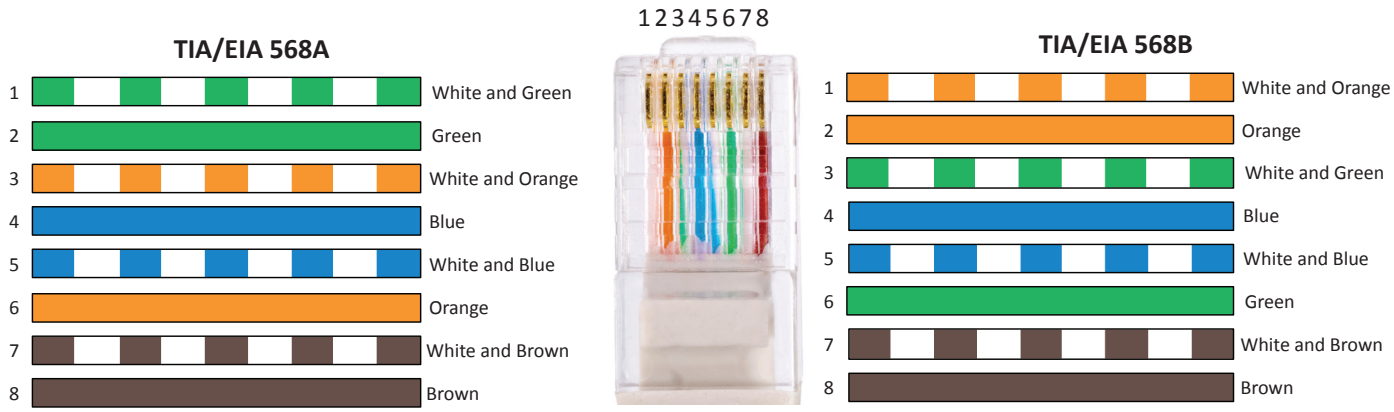
Copper Cable Categories

Ethernet Standard	Cable Category	Maximum Supported Distance
1000BASE-T	Category 5	100 meters
1000BASE-T	Category 5e (enhanced)	100 meters
10GBASE-T	Category 6	Unshielded: 55 meters Shielded: 100 meters
10GBASE-T	Category 6A (augmented)	100 meters
10GBASE-T	Category 7 (Shielded only)	100 meters
40GBASE-T	Category 8 (Shielded only)	30 meters

Source: IEEE 802.3 Standard

T568A and T568B termination

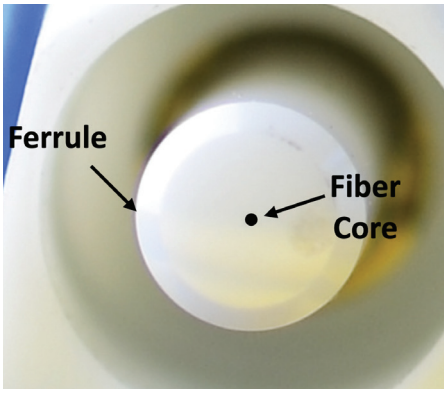
- Pin assignments in EIA/TIA-568-B - Eight conductor 100-ohm balanced twisted-pair cabling
- 568A and 568B are different pin assignments for 8P8C connectors
  - Specification assigns the 568A pin-out to horizontal cabling - Many organizations have traditionally used 568B
- You can't terminate one side of the cable with 568A and the other with 568B
  - You'll run into confusion and technical problems

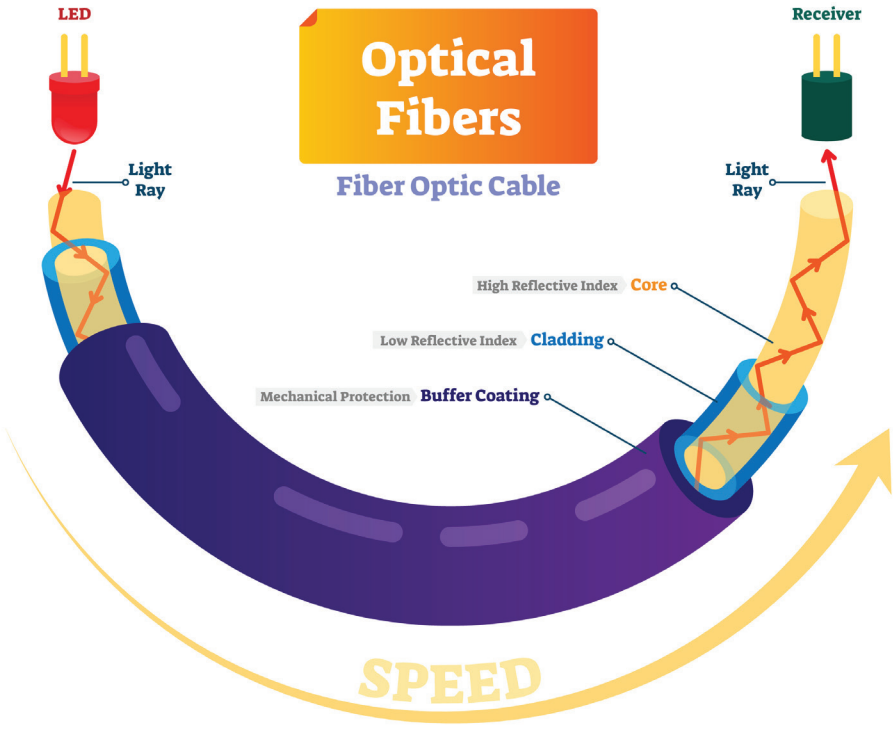


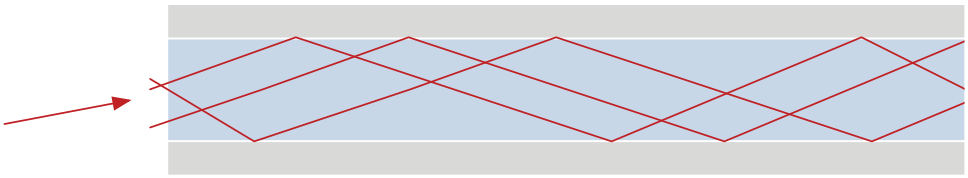
1.3 - Optical Fiber

Fiber communication

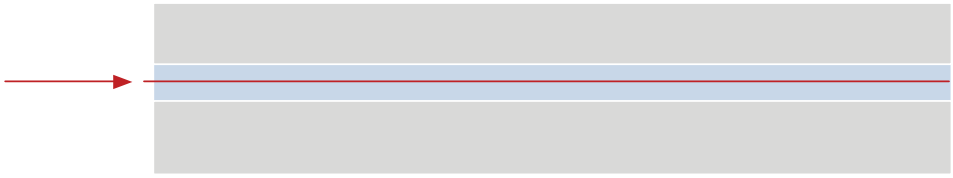
- Transmission by light
  - The visible spectrum
- No RF signal
  - Very difficult to monitor or tap
- Signal slow to degrade
  - Transmission over long distances
- Immune to radio interference
  - There's no RF







Multi-mode Fiber
Short-range communication, up to 2 km

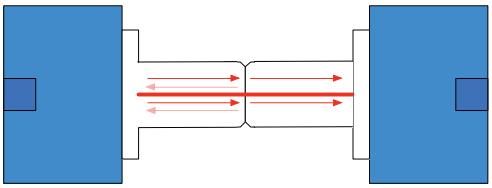


Single-mode Fiber
Long-range communication, up to 100 km

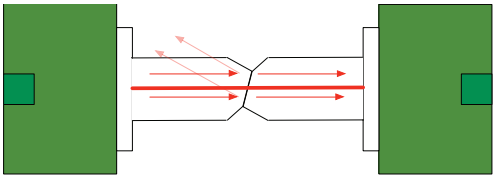
1.3 - Network Connectors

UPC vs. APC

- Controlling light-Laws of physics apply
- Return loss-Light reflected back to the source
- UPC (Ultra-polished connectors)
  - Ferrule end-face radius polished at a zero degree angle
  - High return loss
- APC (Angle-polished connectors)
  - Ferrule end-face radius polished at an eight degree angle
  - Lower return loss, generally higher insertion loss than UPC

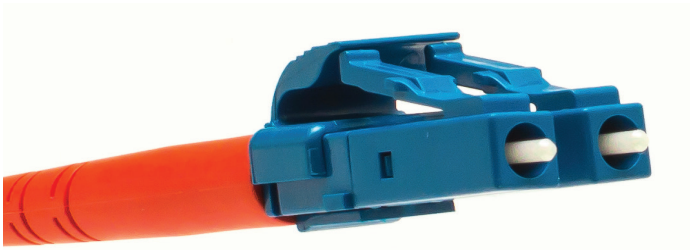


UPC - Ultra-Polished Connectors



APC - Angle-Polished Connectors

1.3 - Network Connectors (continued)

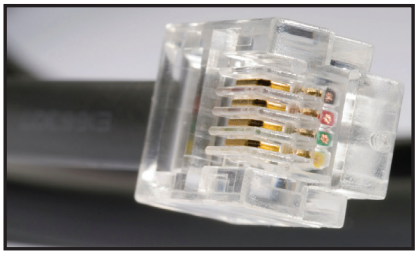


LC - Local Connector

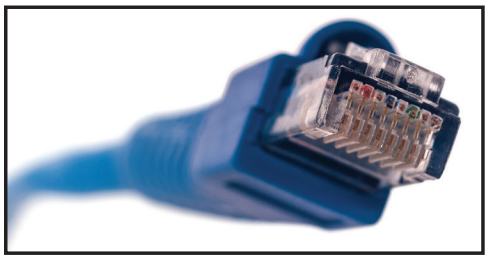
ST - Straight Tip

SC - Subscriber Connector

MT-RJ - Mechanical Transfer Registered Jack



RJ-11 Connector



RJ-45 Connector

F-connector

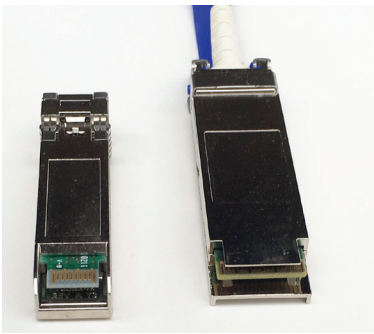
1.3 - Network Transceivers

Media Converter

- OSI Layer 1
  - Physical layer signal conversion
- Extend a copper wire over a long distance
  - Convert it to fiber, and back again
- You have fiber
  - The switch only has copper ports
- Almost always powered
  - Especially fiber to copper

Transceiver

- Transmitter and receiver
  - Usually in a single component
- Provides a modular interface
  - Add the transceiver that matches your network



SFP QSFP

SFP and SFP+

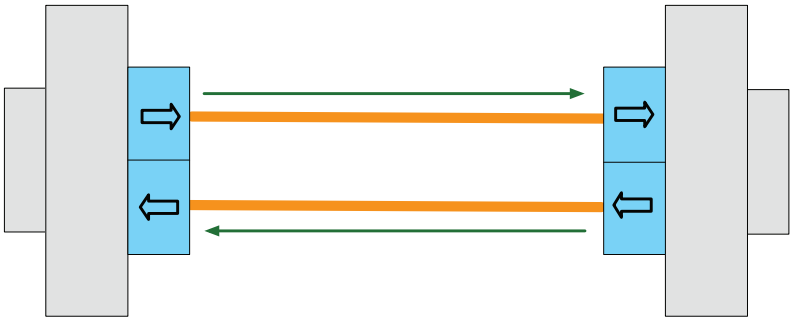
- Small Form-factor Pluggable (SFP)
  - Commonly used to provide 1 Gbit/s fiber
  - 1 Gbit/s RJ45 SFPs also available
- Enhanced Small Form-factor Pluggable (SFP+)
  - Exactly the same size as SFPs
  - Supports data rates up to 16 Gbit/s
  - Common with 10 Gigabit Ethernet

QSFP

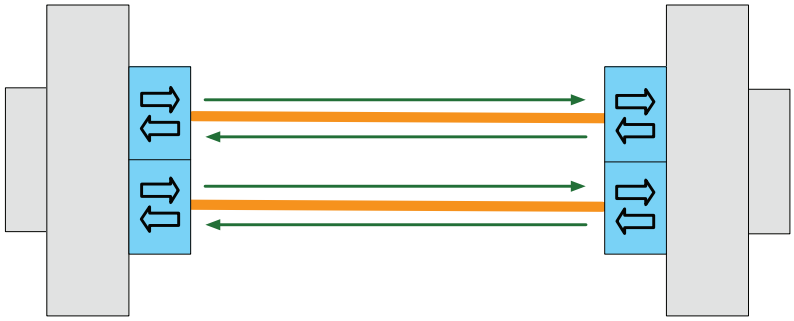
- Quad Small Form-factor Pluggable
  - 4-channel SFP = Four 1 Gbit/s = 4 Gbit/s
  - QSFP+ is four-channel SFP+ = Four 10 Gbit/sec = 40 Gbit/sec
- Combine four SFPs into a single transceiver
  - Cost savings in fiber and equipment
- Bi-Directional (BiDi) QSFP and QSFP+
  - Additional efficiency over a single fiber run

1.3 - Network Transceivers (continued)

Duplex communication
- Two fibers
  - Transmit and receive

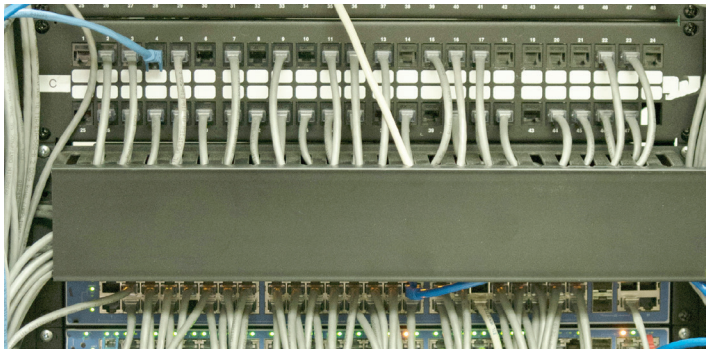


Bi-Directional (BiDi) transceivers
- Traffic in both directions with a single fiber
  - Use two different wavelengths
- Reduce the number of fiber runs by half

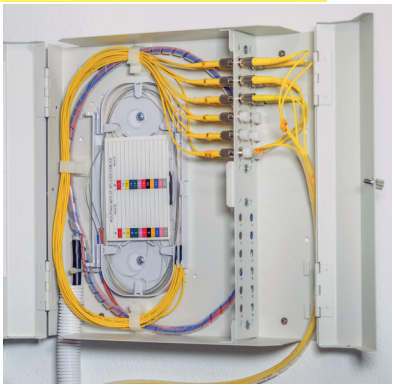


1.3 - Cable Management

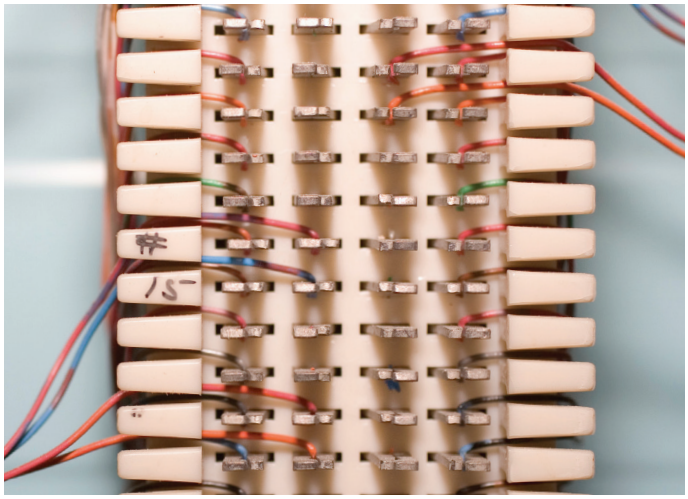
Copper patch panel
- Punch-down block on one side, RJ45 connector on the other
- Move a connection around - Different switch interfaces
- The run to the desk doesn't move



Fiber distribution panel
- Permanent fiber installation - Patch panel at both ends
- Fiber bend radius - Breaks when bent too tightly
- Often includes a service loop
  - Extra fiber for future changes



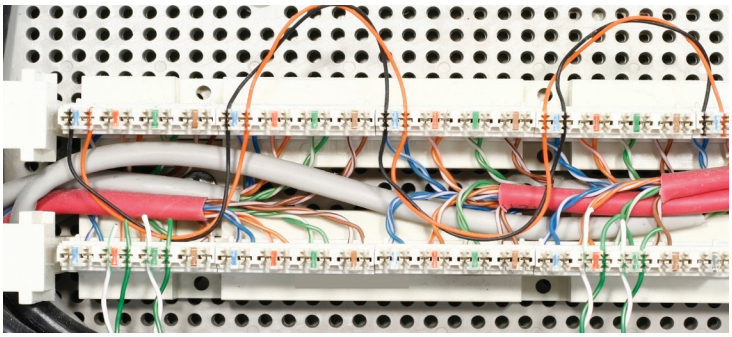
66 block
- A patch panel for analog voice
  - And some digital links
- Left side is patched to the right
  - Easy to follow the path
- Wire and a punch-down tool
  - No additional connectors required
- Generally replaced by 110 blocks
  - Still seen in many installations



1.3 - Cable Management (continued)

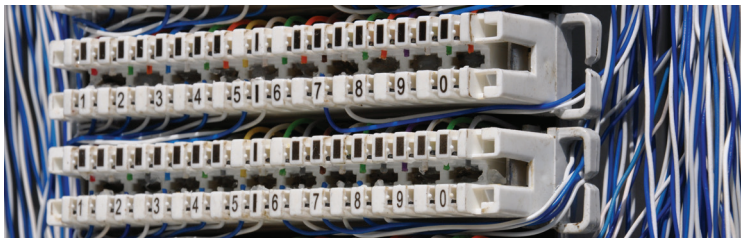
110 block

- Wire-to-wire patch panel
  - No intermediate interface required
- Replaces the 66 block
  - Patch Category 5 and Category 6 cables
- Wires are "punched" into the block
  - Connecting block is on top
- Additional wires punched into connecting block
  - Patch the top to the bottom



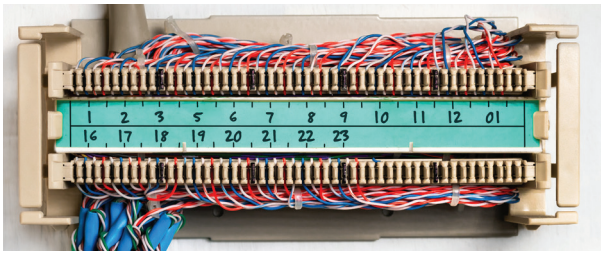
Krone block

- An alternative to the 110 block
  - Common in Europe
- Options available for many purposes
  - Analog and digital communication
  - Different models can support higher frequencies



BIX (Building Industry Cross-connect)

- Created in the 1970s by Northern Telecom
  - A common block type
- Updated through the years
  - GigaBIX performance is better than the Category 6 cable standard



1.3 - Ethernet Standards

Ethernet

- The most popular networking technology in the world
  - Standard, common, nearly universal
- Many different types of Ethernet
  - Speeds, cabling, connectors, equipment
- Modern Ethernet uses twisted pair copper or fiber
- BASE (baseband)
  - Single frequency using the entire medium
  - Broadband uses many frequencies, sharing the medium

10 and 100 megabit Ethernet

- 10BASE-T (twisted pair)
  - Two pair, Category 3 cable minimum
  - 100 meter maximum distance
- 100BASE-TX
  - "Fast Ethernet"
  - Category 5 or better twisted pair copper - two pair
  - 100 meters maximum length

1000BASE-T

- Gigabit Ethernet over Category 5
  - 4-pair balanced twisted-pair
- Category 5
  - Category 5 is deprecated, so we use Cat 5e today
  - A shift to using all four pair
  - 100 meter maximum distance

10GBASE-T

- 10 Gig Ethernet over copper
  - 4-pair balanced twisted-pair
- Frequency use of 500 MHz
  - Well above the 125 MHz for gigabit Ethernet
- Category 6
  - Unshielded: 55 meters, Shielded: 100 meters
- Category 6A (augmented)
  - Unshielded or shielded: 100 meters

40GBASE-T

- 40 gigabit per second Ethernet
  - 4-pair balanced twisted-pair
- Category 8 cable - Up to 30 meters

100 megabit Ethernet over fiber

- 100BASE-FX
  - Pair of multimode fiber - Same fiber as FDDI
  - Laser components
  - 400 meters (half-duplex), 2 kilometers (full-duplex)
- 100BASE-SX
  - A less-expensive version of 100 megabit Ethernet over fiber
  - LED optics, 300 meters maximum distance

1.3 - Ethernet Standards (continued)

Gigabit Ethernet over fiber

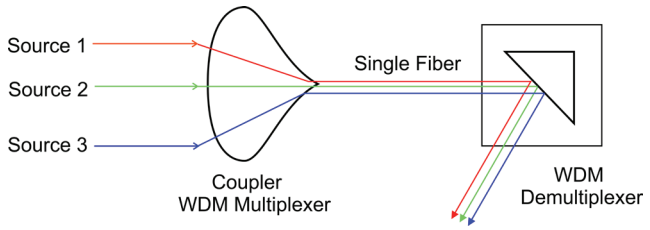
- 1000BASE-SX
  - Gigabit Ethernet using NIR (near infrared) light
  - Usually over multi-mode fiber
  - 220 meters to 500 meters, depending on fiber type
- 1000BASE-LX
  - Gigabit Ethernet using long wavelength laser
  - Multi-mode fiber to 550 meters
  - Single-mode fiber to 5 kilometers

10 Gigabit Ethernet over fiber

- 10GBASE-SR – Short Range
  - Multimode fiber
  - 26 to 400 meters, depending on the fiber
- 10GBASE-LR – Long range
  - Single-mode fiber
  - 10 kilometers maximum range

WDM

- Wavelength-Division Multiplexing
  - Bidirectional communication over a single strand of fiber
- Use different wavelengths for each carrier
  - Different "colors"
- CWDM (Coarse Wavelength-Division Multiplexing)
  - 10GBASE-LX4 uses four 3.125 Gbit/sec carriers at four different wavelengths
- DWDM (Dense Wavelength-Division Multiplexing)
  - Multiplex multiple OC carriers into a single fiber
  - Add 160 signals, increase to 1.6 Tbit/s



1.4 - Binary Math

2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
4,096	2,048	1,024	512	256	128	64	32	16	8	4	2	1

1.4 - IPv4 Addressing

Networking with IPv4

- IP Address, e.g., 192.168.1.165
  - Every device needs a unique IP address
- Subnet mask, e.g., 255.255.255.0
  - Used by the local device to determine what subnet it's on
  - The subnet mask isn't (usually) transmitted across the network
  - You'll ask for the subnet mask all the time
  - What's the subnet mask of this network?
- Default gateway, e.g., 192.168.1.1
  - The router that allows you to communicate outside of your local subnet
  - The default gateway must be an IP address on the local subnet

Special IPv4 addresses

- Loopback address
  - An address to yourself
  - Ranges from 127.0.0.1 through 127.255.255.254
  - An easy way to self-reference (ping 127.0.0.1)
- Reserved addresses
  - Set aside for future use or testing
  - 240.0.0.1 through 254.255.255.254
- Virtual IP addresses (VIP)
  - Not associated with a physical network adapter
  - Virtual machine, internal router address

DHCP

- IPv4 address configuration used to be manual
  - IP address, subnet mask, gateway, DNS servers, NTP servers, etc.
- Dynamic Host Configuration Protocol
  - Provides automatic addresses and IP configuration for almost all devices

APIPA - Automatic Private IP Addressing

- A link-local address - No forwarding by routers
- IETF has reserved 169.254.0.1 - through 169.254.255.254
  - First and last 256 addresses are reserved
  - Functional block of 169.254.1.0 through 169.254.254.255

IPv4 Address

192	168	1	131
11000000	10101000	00000001	10000011

8 bits = 1 byte = 1 octet

32 bits = 4 bytes

1.4 - Network Address Translation

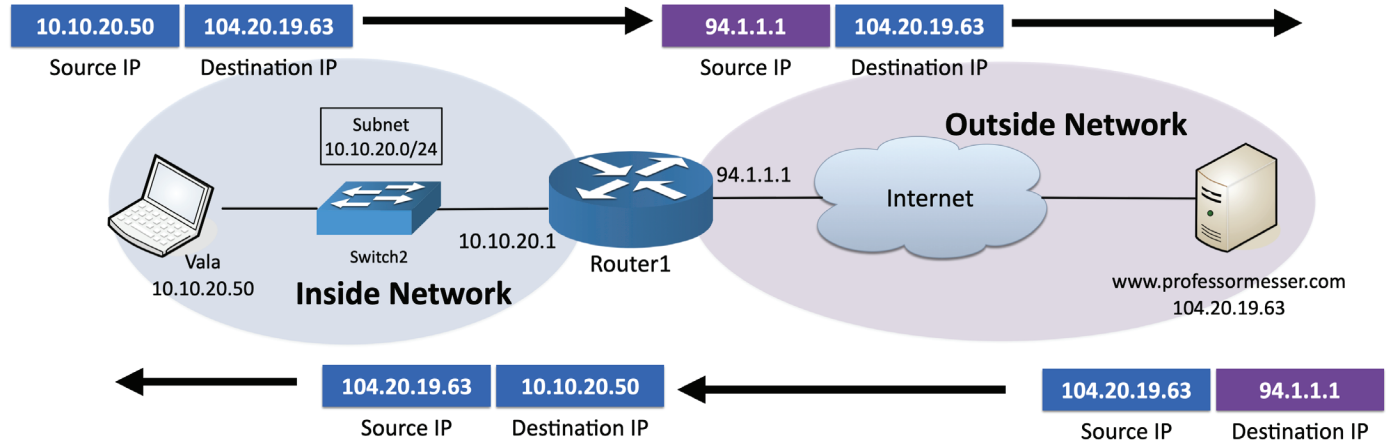
NAT (Network Address Translation)

- It is estimated that there are over 20 billion devices connected to the Internet (and growing)
  - IPv4 supports around 4.29 billion addresses
- The address space for IPv4 is exhausted
  - There are no available addresses to assign
- How does it all work?
  - Network Address Translation
- This isn't the only use of NAT
  - NAT is handy in many situations

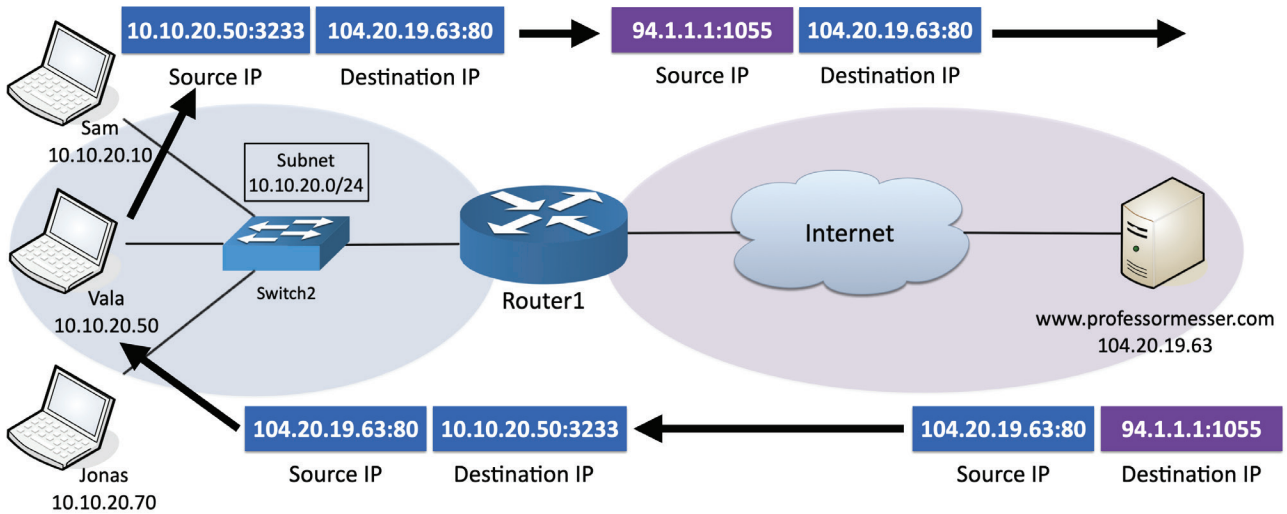
RFC 1918 Private IPv4 Addresses

IP address range	Number of addresses	Classful description	Largest CIDR block (subnet mask)	Host ID size
10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Static NAT



NAT Overload / Port Address Translation (PAT)



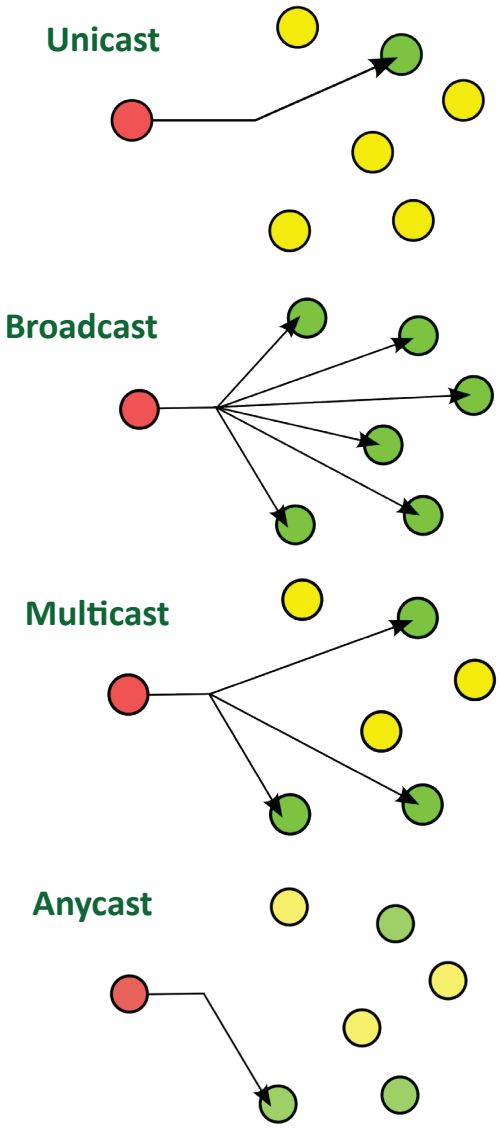
1.4 - Network Communication

Unicast
- One station sending information to another station
- Send information between two systems
- Web surfing, file transfers
- Does not scale optimally for streaming media

Broadcast
- Send information to everyone at once
- One packet, received by everyone
- Limited scope - the broadcast domain
- Routing updates, ARP requests
- Not used in IPv6 - focus on multicast

Multicast
- Delivery of information to interested systems
  - One to many
- Multimedia delivery, stock exchanges
- Very specialized
  - Difficult to scale across large networks
- Used in both IPv4 and IPv6
  - Extensive use in IPv6

Anycast
- Single destination IP address has multiple paths to two or more endpoints
  - One-to-one-of-many
  - Used in IPv4 and IPv6
- Configure the same anycast address on different devices
  - Looks like any other unicast address
- Packets sent to an anycast address are delivered to the closest interface
  - Announce the same route out of multiple data centers, clients use the data center closest to them
  - Anycast DNS



1.4 - Classful Subnetting and IPv4 Subnet Masks

Binary	Decimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts per Network	Default Subnet Mask
Class A	0xxx (1-127)	8	24	128	16,777,214	255.0.0.0
Class B	10xx (128-191)	16	16	16,384	65,534	255.255.0.0
Class C	110x (192-223)	24	8	2,097,152	254	255.255.255.0
Class D (multicast)	1110 (224-239)	Not defined	Not defined	Not defined	Not defined	Not defined
Class E (reserved)	1111 (240-254)	Not defined	Not defined	Not defined	Not defined	Not defined

1.4 - Classful Subnetting and IPv4 Subnet Masks (continued)

Classful Subnetting

- Very specific subnetting architecture
  - Not used since 1993
  - But still referenced in casual conversation
- Used as a starting point when subnetting
  - Standard values

The construction of a subnet

- Network address
  - The first IP address of a subnet - Set all host bits to 0 (0 decimal)
- First usable host address
  - One number higher than the network address
- Network broadcast address
  - The last IP address of a subnet - Set all host bits to 1 (255 decimal)
- Last usable host address
  - One number lower than the broadcast address

1.4 - Calculating IPv4 Subnets and Hosts

VLSM (Variable Length Subnet Masks)

- Class-based networks are inefficient
  - The subnet mask is based on the network class
- Allow network administrators to define their own masks
  - Customize the subnet mask to specific network requirements
- Use different subnet masks in the same classful network
  - 10.0.0.0/8 is the class A network - 10.0.1.0/24 and 10.0.8.0/26 would be VLSM

$$\text{Number of subnets} = 2^{\text{subnet bits}}$$

$$\text{Hosts per subnet} = 2^{\text{host bits}} - 2$$

2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1
256	128	64	32	16	8	4	2

2^{16}	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9
65,536	32,768	16,384	8,192	4,096	2,048	1,024	512

1.4 - Magic Number Subnetting

Four Important Addresses

- Network address / subnet ID
  - The first address in the subnet
- Broadcast address
  - The last address in the subnet
- First available host address
  - One more than the network address
- Last available host address
  - One less than the broadcast address

Magic number subnetting

- Very straightforward method
  - Can often perform the math in your head
- Subnet with minimal math
  - Still some counting involved
- Some charts might help
  - But may not be required
  - CIDR to Decimal
  - Host ranges

The magic number process

- Convert the subnet mask to decimal
- Identify the "interesting octet"
- Calculate the "magic number"
  - 256 minus the interesting octet
  - Calculate the host range
- Identify the network address
  - First address in the range
- Identify the broadcast address
  - Last address in the range

CIDR for interesting octet 2	/9	/10	/11	/12	/13	/14	/15	/16
CIDR for interesting octet 3	/17	/18	/19	/20	/21	/22	/23	/24
CIDR for interesting octet 4	/25	/26	/27	/28	/29	/30		
Magic number	128	64	32	16	8	4	2	1
Subnet mask for interesting octet	128	192	224	240	248	252	254	255

1.4 - Seven Second Subnetting

Seven second subnetting

- Convert IP address and subnet mask to decimal
  - Use chart to convert between CIDR-block notation and decimal
  - Same chart also shows the number of devices per subnet
- Determine network/subnet address
  - Second chart shows the starting subnet boundary
- Determine broadcast address
  - Chart below shows the ending subnet boundary
- Calculate first and last usable IP address
  - Add one from network address, subtract one from broadcast address

	Masks				Networks	Addresses
/1	/9	/17	/25	128	2	128
/2	/10	/18	/26	192	4	64
/3	/11	/19	/27	224	8	32
/4	/12	/20	/28	240	16	16
/5	/13	/21	/29	248	32	8
/6	/14	/22	/30	252	64	4
/7	/15	/23	/31	254	128	2
/8	/16	/24	/32	255	256	1

Addresses																																																															
128	0																															128																														
64	0																64																128																192														
32	0								32								64								96								128								160								192								224						
16	0				16				32				48				64				80				96				112				128				144				160				176				192				208				224				240		
8	0		8		16		24		32		40		48		56		64		72		80		88		96		104		112		120		128		136		144		152		160		168		176		184		192		200		208		216		224		232		240		248
4	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192	196	200	204	208	212	216	220	224	228	232	236	240	244	248

1.4 - IPv6 Addressing

IPv6 addresses

- Internet Protocol v6 - 128-bit address
  - 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (340 undecillion)
  - 6.8 billion people could have 5,000,000,000,000,000,000,000,000,000 addresses each

IPv6 address compression

- Your DNS will become very important!
- Groups of zeros can be abbreviated with a double colon ::
  - Only one of these abbreviations allowed per address
- Leading zeros are optional

fe80::5d18:652:cffd:8f52

fe80:0000:0000:0000:5d18:0652:cffd:8f52

fe80 : 0000 : 0000 : 0000 : 5d18 : 0652 : cffd : 8f52

1111111010000000:0000000000000000:0000000000000000:0000000000000000:0101110100011000:0000011001010010:1100111111111101:1000111101010010

16 bits = 2 bytes = 2 octets

128 bits = 16 bytes

Configuring IPv6 with a modified EUI-64

- Static addressing can be useful
  - The IP address never changes
- What other address never changes?
  - The MAC address
- Extended Unique Identifier (64-bit)
- Combined a 64-bit IPv6 prefix and the MAC address
  - Wait, the MAC address is only 48-bits long!
- You're going to need some extra bits
  - And a minor change to the MAC address

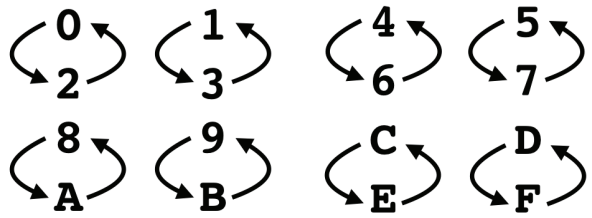
Converting EUI-48 to EUI-64

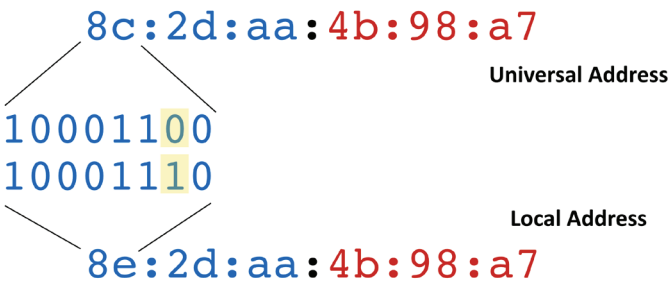
- Split the MAC
  - Two 3-byte (24 bit) halves
- Put `FFFE` in the middle
  - The missing 16 bits
- Invert the seventh bit
  - Changes the address from globally unique/universal
  - Turns the burned-in address (BIA) into a locally administered address
  - This is the U/L bit (universal/local)

1.4 - IPv6 Addressing (continued)

Shortcut for flipping the 7th bit

- Quickly convert the MAC address - create a chart
- Count from 0 to F in hex - two columns, groups of four
- Quickly convert the second character of the first hex byte
  - Change it to the other value

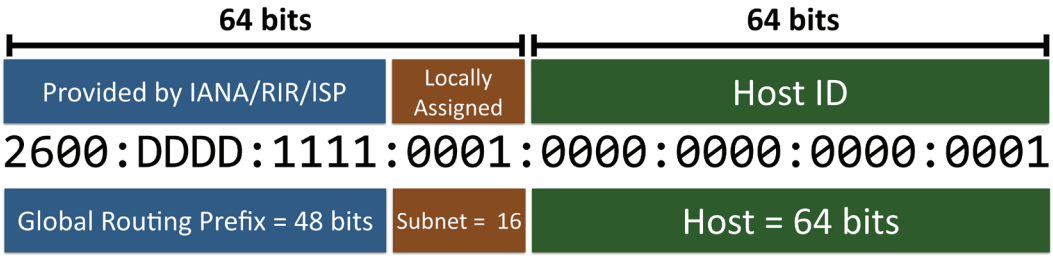




1.4 - IPv6 Subnet Masks

Assigning IPv6 Addresses

- Internet Assigned Numbers Authority (IANA) provides address blocks to RIRs (Regional Internet Registries)
- RIRs assigns smaller subnet blocks to ISPs (Internet Service Providers)
- ISP assigns a /48 subnet to the customer



1.4 - Configuring IPv6

Tunneling IPv6

- 6 to4 addressing
  - Send IPv6 over an existing IPv4 network
  - Creates an IPv6 based on the IPv4 address
  - Requires relay routers
  - No support for NAT
- 4in6 - Tunnel IPv4 traffic on an IPv6 network

Teredo/Miredo

- Tunnel IPv6 through NATed IPv4
  - End-to-end IPv6 through an IPv4 network
  - No special IPv6 router needed
  - Temporary use - We'll have IPv6 native networks soon (?)
- Miredo - Open-source Teredo for Linux,
- BSD Unix, and Mac OS X - Full functionality

Dual-stack routing

- Dual-stack IPv4 and IPv6 - Run both at the same time
  - Interfaces will be assigned multiple address types
- IPv4
  - Configured with IPv4 addresses
  - Maintains an IPv4 routing table
  - Uses IPv4 dynamic routing protocols
- IPv6 - Configured with IPv6 addresses
  - Maintains a separate IPv6 routing table
  - Uses IPv6 dynamic routing protocols

Howdy Neighbor

- There's no ARP in IPv6
  - So how do you find out the MAC address of a device?
- Neighbor Solicitation (NS) -Sent as a multicast
- Neighbor Advertisement (NA)

NDP (Neighbor Discovery Protocol)

- No broadcasts! - Operates using multicast over ICMPv6
- Neighbor MAC Discovery - Replaces the IPv4 ARP
- SLAAC (Stateless Address Autoconfiguration)
  - Automatically configure an IP address without a DHCP server
- DAD (Duplicate Address Detection) - No duplicate IPs!
- Discover routers
  - Router Solicitation (RS) and Router Advertisement (RA)

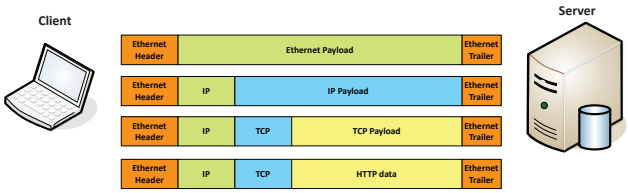
Finding Router

- ICMPv6 adds the Neighbor Discovery Protocol
- Routers also send unsolicited RA messages
  - From the multicast destination of ff02::1
- Transfers IPv6 address information, prefix value, and prefix length, etc. - Sent as a multicast
- Neighbor Advertisement (NA)

1.5 - Introduction to IP

A Series of Moving Vans

- Efficiently move large amounts of data
  - Use a shipping truck
- The network topology is the road
  - Ethernet, DSL, coax cable
- The truck is the Internet Protocol (IP)
  - We've designed the roads for this truck
- The boxes hold your data
  - Boxes of TCP and UDP
- Inside the boxes are more things
  - Application information



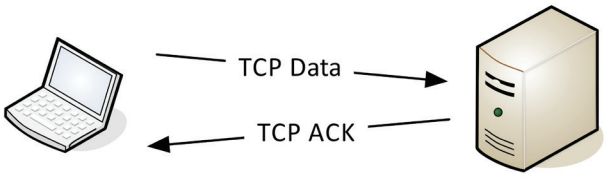
TCP and UDP

- Transported inside of IP
  - Encapsulated by the IP protocol
- Two ways to move data from place to place
  - Different features for different applications
- OSI Layer 4
  - The transport layer
- Multiplexing
  - Use many different applications at the same time
  - TCP and UDP

TCP - Transmission Control Protocol

- Connection-oriented
  - A formal connection setup and close
- "Reliable" delivery
  - Recovery from errors
  - Can manage out-of-order messages or retransmissions
- Flow control
  - The receiver can manage how much data is sent

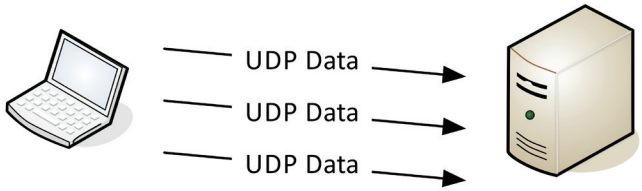
TCP - Transmission Control Protocol Communication



UDP - User Datagram Protocol

- Connectionless
  - No formal open or close to the connection
- "Unreliable" delivery
  - No error recovery
  - No reordering of data or retransmissions
- No flow control

UDP - User Datagram Protocol Communication



  - Sender determines the amount of data transmitted

Lots of Ports

- IPv4 sockets
  - Server IP address, protocol, server application port number
  - Client IP address, protocol, client port number
- Non-ephemeral ports –permanent port numbers
  - Ports 0 through 1,023
  - Usually on a server or service
- Ephemeral ports – temporary port numbers
  - Ports 1,024 through 65,535
  - Determined in real-time by the clients

Port Numbers

- TCP and UDP ports can be any number between 0 and 65,535
- Most servers (services) use non-ephemeral (not-temporary) port numbers
  - This isn't always the case - it's just a number.
- Port numbers are for communication, not security
- Service port numbers need to be "well known"
- TCP port numbers aren't the same as UDP port numbers

ICMP

- Internet Control Message Protocol
  - "Text messaging" for your network devices
- Another protocol carried by IP - Not used for data transfer
- Devices can request and reply to administrative requests
  - Hey, are you there? / Yes, I'm right here.
- Devices can send messages when things don't go well
  - That network you're trying to reach is not reachable from here
  - Your time-to-live expired, just letting you know

1.5 - Common Ports

Telnet
- Telnet – Telecommunication Network - tcp/23
- Login to devices remotely
- Console access
- In-the-clear communication
- Not the best choice for production systems

SSH - Secure Shell
- Encrypted communication link - tcp/22
- Looks and acts the same as Telnet

DNS - Domain Name System
- Converts names to IP addresses - udp/53
  - www.professormesser.com = 162.159.246.164
  - Large transfers may use tcp/53
- These are very critical resources
  - Usually multiple DNS servers are in production

SMTP - Simple Mail Transfer Protocol
- SMTP - Simple Mail Transfer Protocol
  - Server to server email transfer - tcp/25
- Also used to send mail from a device to a mail server
  - Commonly configured on mobile devices and email clients
- Other protocols are used for clients to receive email
  - IMAP, POP3

POP/IMAP
- Receive emails from an email server
  - Authenticate and transfer
- POP3 - Post office Protocol version 3 - tcp/110
  - Basic mail transfer functionality
- IMAP4 - Internet Message Access Protocol v4 - tcp/143
  - Manage email inbox from multiple clients

SFTP - Secure FTP
- Uses the SSH File Transfer Protocol - tcp/22
- Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal

File transfer application protocols
- FTP – File Transfer Protocol
  - tcp/20 (active mode data), tcp/21 (control)
  - Transfers files between systems
  - Authenticates with a username and password
  - Full-featured functionality (list, add, delete, etc.)
- TFTP – Trivial File Transfer Protocol
  - udp/69
  - Very simple file transfer application
    - Read files and write files
  - No authentication - Not used on production systems

DHCP - Dynamic Host Configuration Protocol
- Automated configuration of IP address, subnet mask and other options
  - udp/67, udp/68 - Requires a DHCP server
- Dynamic / pooled
  - IP addresses are assigned in real-time from a pool
  - Each system is given a lease
  - Must renew at set intervals
- Reserved
  - Addresses are assigned by MAC address
  - Quickly manage addresses from one location

HTTP and HTTPS
- Hypertext Transfer Protocol
  - Communication in the browser
  - And by other applications
- In the clear or encrypted
  - Supported by nearly all web servers and clients

SNMP - Simple Network Management Protocol
- Gather statistics from network devices
  - udp/161
- v1 – The original
  - Structured tables, in-the-clear
- v2 – A good step ahead
  - Data type enhancements, bulk transfers
  - Still in-the-clear
- v3 – The new standard
  - Message integrity, authentication, encryption

Syslog
- Standard for message logging
  - Diverse systems, consolidated log
  - udp/514
- Usually a central log collector
  - Integrated into the SIEM
- You're going to need a lot of disk space
  - Data storage from many devices over an extended timeframe

RDP - Remote Desktop Protocol
- Share a desktop from a remote location over tcp/3389
- Remote Desktop Services on many Windows versions
- Can connect to an entire desktop or just an application
- Clients for Windows, MacOS, Linux, iPhone, and others

NTP - Network Time Protocol
- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock - udp/123
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic updates
  - No flashing 12:00 lights
- Flexible - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond

1.5 - Common Ports (continued)

SIP - Session Initiation Protocol

- Voice over IP (VoIP) signaling
  - tcp/5060 and tcp/5061
- Setup and manage VoIP sessions
  - Call, ring, hang up
- Extend voice communication
  - Video conferencing, instant messaging, file transfer, etc.

SMB - Server Message Block

- Protocol used by Microsoft Windows
  - File sharing, printer sharing
  - Also called CIFS (Common Internet File System)
- Direct over tcp/445 (NetBIOS-less)
- Direct SMB communication over TCP

LDAP/LDAPS

- LDAP (Lightweight Directory Access Protocol) - tcp/389
  - Store and retrieve information in a network directory
- LDAPS (LDAP Secure) - tcp/636
  - A non-standard implementation of LDAP over SSL
  - Still in use today

Databases

- Microsoft SQL Server
  - MS-SQL (Microsoft Structured Query Language)
  - tcp/1433
- Oracle SQL *Net
  - Also called Oracle Net or Net8 - tcp/1521
- MySQL free and open-source database
  - Ultimately acquired by Oracle - tcp/3306

ARP	-	Address Resolution Protocol	Resolve IP address to MAC
TCP	-	Transmission Control Protocol	Connection-oriented network communication
UDP	-	User Datagram Protocol	Connectionless network communication

Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
SSH	tcp/22	Secure Shell	Encrypted console login
DNS	udp/53, tcp/53	Domain Name Services	Convert domain names to IP addresses
SMTP	tcp/25	Simple Mail Transfer Protocol	Transfer email between mail servers
POP3	tcp/110	Post Office Protocol version 3	Receive mail into a mail client
IMAP4	tcp/143	Internet Message Access Protocol v4	A newer mail client protocol
SFTP	tcp/22	Secure File Transfer Protocol	Encrypted file transfers using SSH
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
DHCP	udp/67, udp/68	Dynamic Host Configuration Protocol	Update to BOOTP
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
Syslog	udp/514	System Logging	A standard for message logging
RDP	tcp/3389	Remote Desktop Protocol	Graphical display of remote device
NTP	udp/123	Network Time Protocol	Automatically synchronize clocks
SIP	tcp/5060-5061	Session Initiation Protocol	Voice over IP signaling protocol
SMB	tcp/445	Server Message Block	File and printer sharing for Windows
LDAP	tcp/389	Lightweight Directory Access Protocol	Directory services
LDAPS	tcp/636	Lightweight Directory Access Protocol Secure	Directory services over SSL/TLS
MS-SQL	tcp/1433	Microsoft SQL Server	Microsoft's structured query language database
SQL *Net	tcp/1521	Oracle SQL *Net	Oracle SQL services
MySQL	tcp/3306	MySQL Server	Oracle's open-source SQL services

1.5 - Other Useful Protocols

ICMP

- Internet Control Message Protocol
  - "Text messaging" for your network devices
- Another protocol carried by IP
  - Not used for data transfer
- Devices can request and reply to administrative requests
  - Hey, are you there? / Yes, I'm right here.
- Devices can send messages when things don't go well
  - That network you're trying to reach is not reachable from here
  - Your time-to-live expired, just letting you know

GRE

- Generic Routing Encapsulation
  - The "tunnel" between two endpoints
- Encapsulate traffic inside of IP
  - Two endpoints appear to be directly connected to each other
  - No built-in encryption

AH (Authentication Header)

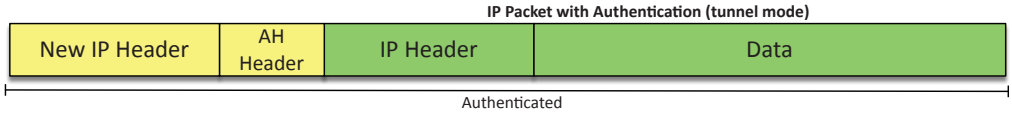
- Data integrity
- Origin authentication
- Replay attack protection
- Keyed-hash mechanism
- No confidentiality/encryption

VPNs

- Virtual Private Networks
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

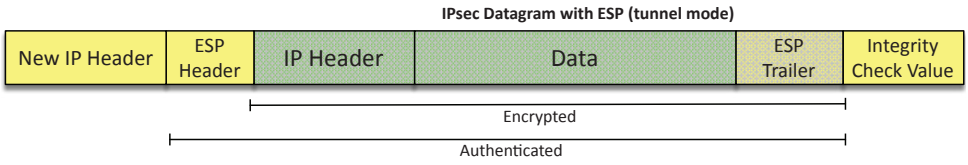
IPSec (Internet Protocol Security)

- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)



ESP (Encapsulating Security Payload)

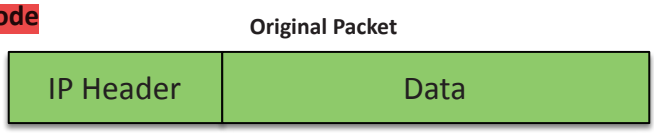
- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Anti-replay protection

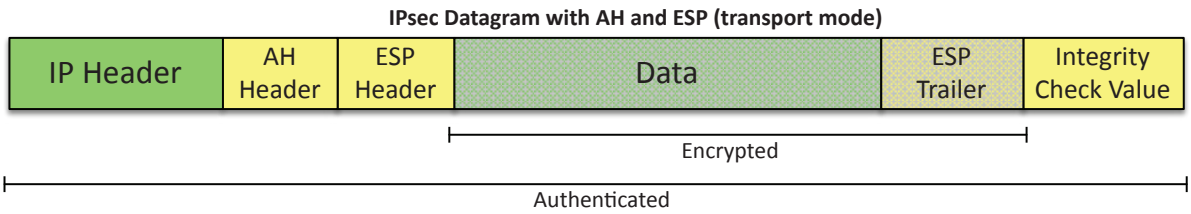


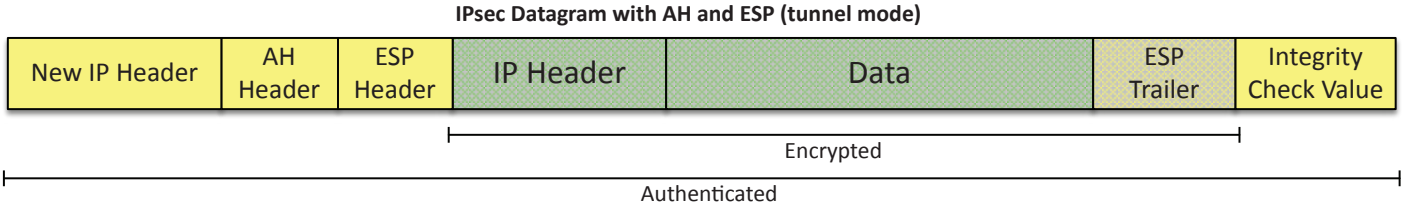
IPsec Transport mode and Tunnel mode

AH and ESP

- Combine the data integrity of AH with the confidentiality of ESP







1.6 - DHCP Overview

DHCP

- IPv4 address configuration used to be manual
  - IP address, subnet mask, gateway, DNS servers, NTP servers, etc.
- October 1993 - The bootstrap protocol - BOOTP
- BOOTP didn't automatically define everything
  - Some manual configurations were still required
  - BOOTP also didn't know when an IP address might be available again
- Dynamic Host Configuration Protocol
  - Initially released in 1997, updated through the years
  - Provides automatic address / IP configuration for almost all devices

The DHCP Process

- **Step 1: Discover** - Client to DHCP Server
  - Find all of the available DHCP Servers
- **Step 2: Offer** - DHCP Server to client
  - Send some IP address options to the client
- **Step 3: Request** - Client to DHCP Server
  - Client chooses an offer and makes a formal request
- **Step 4: Acknowledgement** - DHCP Server to client
  - DHCP server sends an acknowledgement to the client

Managing DHCP in the enterprise

- Limited Communication range
  - Uses the IPv4 broadcast domain
  - Stops at a router
- Multiple servers needed for redundancy
  - Across different locations
- Scalability is always an issue
  - May not want (or need) to manage
  - DHCP servers at every remote location
- You're going to need a little help(er)
  - Send DHCP request across broadcast domains

1.6 - Configuring DHCP

Scope properties

- IP address range (and excluded addresses)
- Subnet mask
- Lease durations
- Other scope options
  - DNS server, default gateway, WINS server

DHCP pools

- Grouping of IP addresses
  - Each subnet has its own scope
  - 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, etc.
- A scope is generally a single contiguous pool of IP addresses
  - DHCP exceptions can be made inside of the scope

DHCP address assignment

- Dynamic assignment
  - DHCP server has a big pool of addresses to give out
  - Addresses are reclaimed after a lease period
- Automatic allocation
  - Similar to dynamic allocation
  - DHCP server keeps a list of past assignments
  - You'll always get the same IP address
- Static assignment
  - Administratively configured table of MAC addresses
  - Each MAC address has a matching IP address
  - Other names - Static DHCP Assignment, Static DHCP, Address Reservation, IP Reservation

DHCP leases

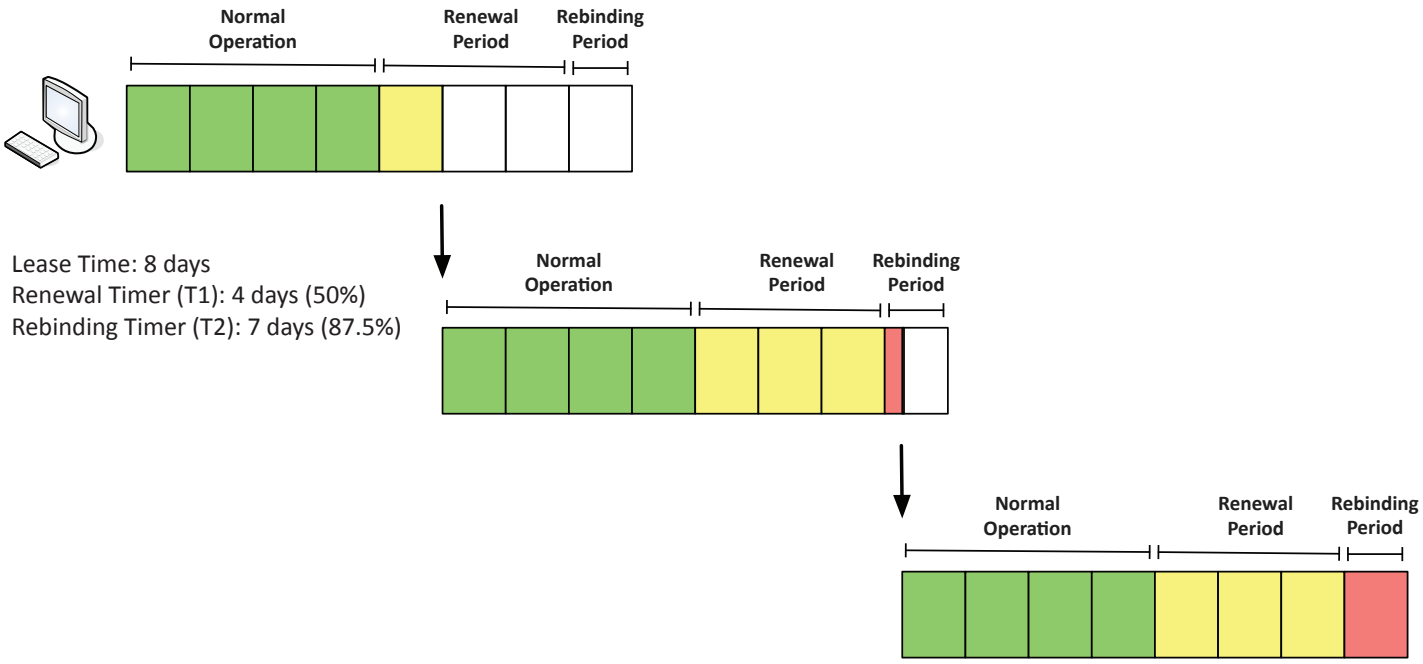
- Leasing your address
  - It's only temporary
  - But it can seem permanent
- Allocation
  - Assigned a lease time by the DHCP server
  - Administratively configured
- Reallocation
  - Reboot your computer
  - Confirms the lease
- Workstation can also manually release the IP address
  - Moving to another subnet

DHCP renewal

- T1 timer
  - Check in with the lending DHCP server to renew the IP address
  - 50% of the lease time (by default)
- T2 timer
  - If the original DHCP server is down, try rebinding with any DHCP server
  - 87.5% of the lease time (7/8ths)

1.6 - Configuring DHCP (continued)

DHCP Timers



1.6 - An Overview of DNS

Domain Name System

- Translates human-readable names into computer-readable IP addresses
  - You only need to remember www.ProfessorMesser.com
- Hierarchical
  - Follow the path
- Distributed database
  - Many DNS servers
  - 13 root server clusters (over 1,000 actual servers)
  - Hundreds of generic top-level domains (gTLDs) - .com, .org, .net, etc.
  - Over 275 country code top-level domains (ccTLDs) - .us, .ca, .uk, etc.

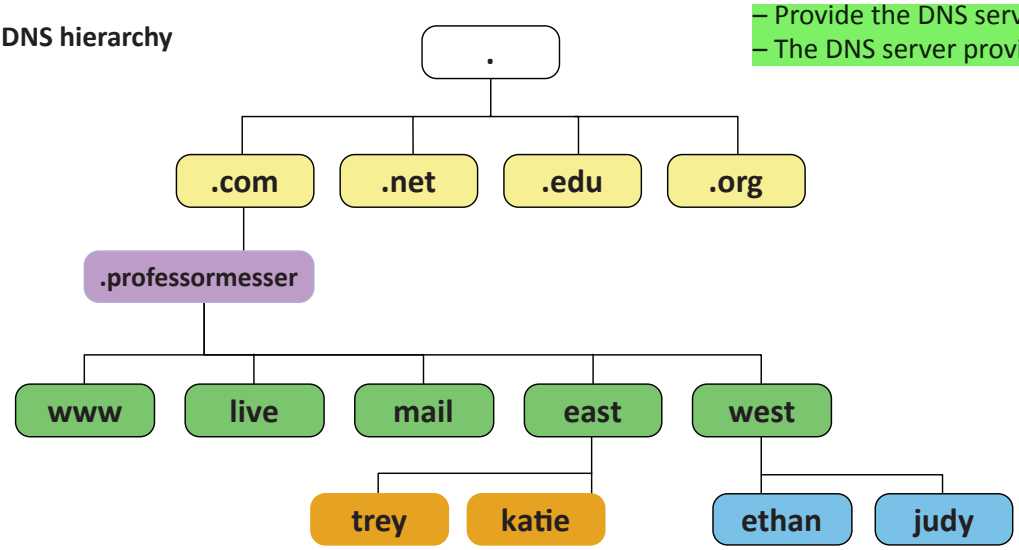
Internal vs. External DNS

- Internal DNS - managed on internal servers
  - Configured and maintained by the local team
  - Contains DNS information about internal devices
  - DNS service on Windows Server
- External DNS
  - Often Managed by a third-party
  - Does not have internal device information
  - Google DNS, Quad9

Lookups

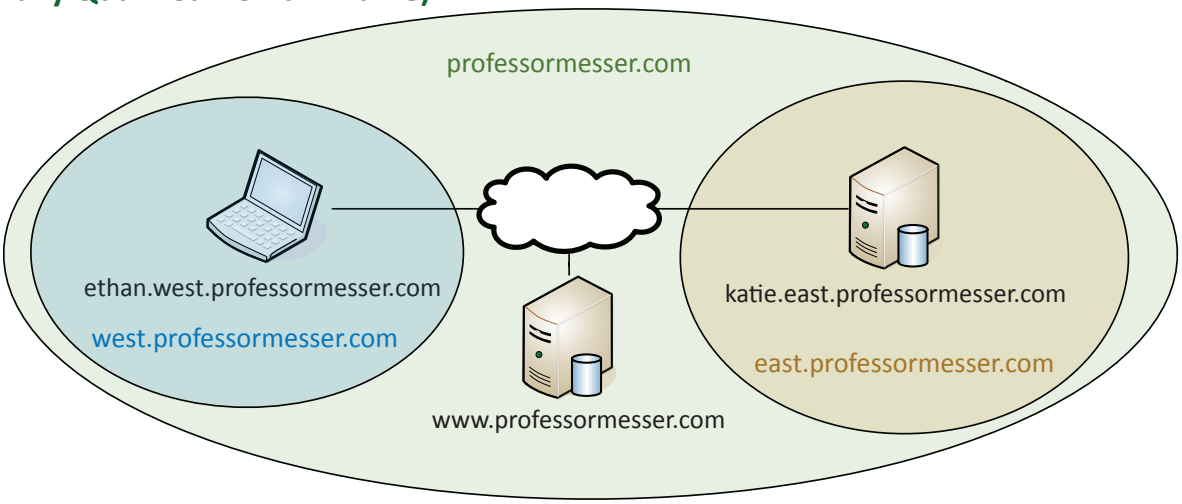
- Forward lookup
  - Provide the DNS server with an FQDN
  - DNS server provides an IP address
- Reverse DNS
  - Provide the DNS server with an IP address
  - The DNS server provides an FQDN

The DNS hierarchy



1.6 - An Overview of DNS (continued)

FQDN (Fully Qualified Domain Name)

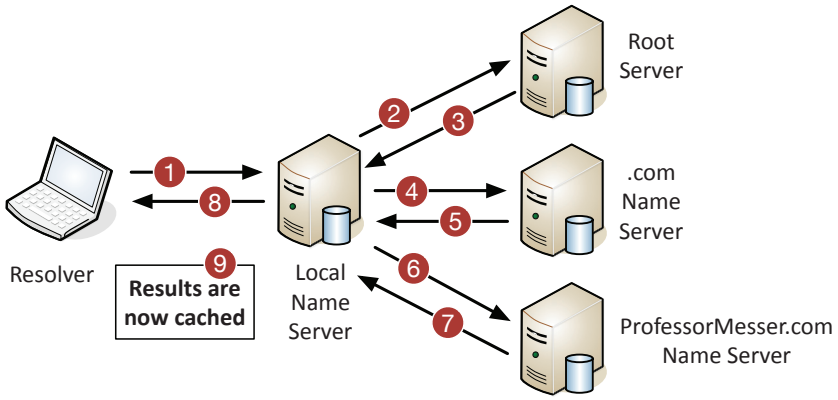


Recursive and iterative DNS queries

- Many ways to get what you need
- Recursive query
  - Delegate the lookup to a DNS server
  - The DNS server does the work and reports back
  - Large DNS cache provides a speed advantage
- Iterative query
  - Do all of the queries yourself
  - Your DNS cache is specific to you

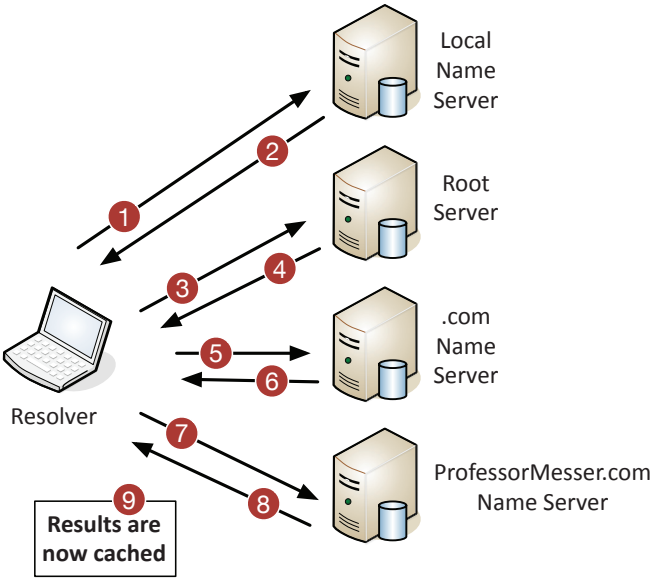
Recursive DNS query

1 - Request sent to local name server
2 - Name server queries root server
3 - Root response sent to local name server
4 - Name server queries .com name server
5 - .com Response sent to local name server
6 - Name server queries specific domain server
7 - Domain server responds to name server
8 - Name server provides result to local device
9 - Answer is cached locally



Iterative DNS query

1 - Request sent to local name server
2 - Response is the name of a more specific DNS server
3 - Request sent to a root server
4 - Response is the name of a more specific DNS server
5 - Request is sent to the .com server
6 - Response is the name of a more specific DNS server
7 - Request made to the authoritative server
8 - Authoritative server provides result
9 - Answer is cached locally



1.6 - DNS Record Types

Resource Records (RR)

- The database records of domain name services
- Over 30 record types - IP addresses, certificates, host alias names, etc.

Start of Authority (SOA)

- Describes the DNS zone details
- Structure
  - IN SOA (Internet zone, Start of Authority) with name of zone
  - Serial number
  - Refresh, retry, and expiry timeframes
  - Caching duration/TTL (Time To Live)

```
@ IN SOA mydomain.name.  postmaster.mydomain.name.
(
      19990811     ; Serial number
      3600         ; 1 hour refresh
      300          ; 5 minutes retry
      172800       ; 2 days expiry
      43200 )      ; 12 hours minimum
```

Address Records (A) (AAAA)

- Defines the IP address of a host
  - This is the most popular query
- A records are for IPv4 addresses
  - Modify the A record to change the host name to IP address resolution
- AAAA records are for IPv6 addresses
  - The same DNS server, different records

```
www.professormesser.com.    IN A    162.159.246.164  ; Professor Messer
```

Canonical name records (CNAME)

- A name is an alias of another, canonical name
  - One physical server, multiple services

```
; Alias (canonical) names
    gopher   IN CNAME    mail.mydomain.name.
    ftp      IN CNAME    mail.mydomain.name.
    www      IN CNAME    mail.mydomain.name.
```

Service records (SRV)

- Find a specific service
  - Where is the Windows Domain Controller? Where is the instant messaging server? Where is the VoIP controller?

```
;Service records
; _service._proto.name.  TTL   class SRV priority weight port target.
 _ldap._tcp.domain.com.  300   IN    SRV 10       60     389  s1.domain.com.
```

Mail exchanger record (MX)

- Determines the host name for the mail server - this isn't an IP address; it's a name

```
; This is the mail-exchanger.  You can list more than one (if
; applicable), with the integer field indicating priority (lowest
; being a higher priority)
      IN MX       mail.mydomain.name.

; Provides optional information on the machine type & operating system
; used for the server
      IN HINFO    Pentium/350 LINUX

; A list of machine names & addresses
    spock.mydomain.name.     IN A    123.12.41.40    ; OpenVMS Alpha
    mail.mydomain.name.      IN A    123.12.41.41    ; Linux (main server)
    kirk.mydomain.name.      IN A    123.12.41.42    ; Windows NT (blech!)
```

1.6 - DNS Record Types (continued)

Name server records (NS)

- List the name servers for a domain - NS records point to the name of the server

```
; main domain name servers
                IN      NS      ns1.example.com.
                IN      NS      ns2.example.com.
; mail domain mail servers
                IN      MX       mail.example.com.
; A records for name servers above
ns1             IN      A       192.168.0.3
ns2             IN      A       192.168.0.4
; A record for mail server above
mail            IN      A       192.168.0.5
```

Pointer record (PTR)

- The reverse of an A or AAAA record
  - Added to a reverse map zone file

```
2               IN      PTR     joe.example.com. ; FDQN
....
15              IN      PTR     www.example.com.
....
17              IN      PTR     bill.example.com.
```

Text records (TXT)

- Human-readable text information
  - Useful public information
- SPF protocol (Sender Policy Framework)
  - Prevent mail spoofing
  - Mail servers check that incoming mail really did come from an authorized host
- DKIM (Domain Keys Identified Mail)
  - Digitally sign your outgoing mail
  - Validated by the mail server, not usually seen by the end user
  - Put your public key in the DKIM TXT record

```
; SPF TXT records
; owner  class  ttl  TXT "attribute-name=attribute value"
  professormesser.com.  300   IN    TXT   "v=spf1 include:mailgun.org ~all"
```

```
; DKIM TXT records
; owner  class  ttl  TXT "attribute-name=attribute value"
1517680427.professormesser._domainkey.professormesser.com. IN 300 TXT
("v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqCUQ5dpKOtwQdE2k8HaCQqV+f"
        "3y30BCzNz75IffEXtk+sTBiDcGWIcapUzkgC4tN0boHBw57APzNInmjH9yZn15TB"
        "TfTavC44nXidUZ8LzsJGWVvYYxoFR5DuBoi/zIO0Hv6YDUpDxJa9knZABTOWLS2F"
        "YtK9dWAMaOZdtTBOhQIDAQAB")
```

Zone transfers

- Replicate a DNS database
  - The primary DNS server has the primary copy of the zone information
- Synchronize to a secondary server
  - Provide redundancy
- Triggered by referencing the serial number
  - If the serial number increases, there must have been a change
- Full zone transfers can be a security risk
  - Attackers can use the data as reconnaissance

1.6 - An Overview of NTP

NTP (Network Time Protocol)

- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic updates
  - No flashing 12:00 lights
- Flexible
  - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond on a local network

NTP clients and servers

- NTP server
  - Respond to time requests from NTP clients
  - Does not modify their own time
- NTP client
  - Requests time updates from NTP server
- NTP client/server
  - Requests time updates from an NTP server
  - Responds to time requests from other NTP clients
- Important to plan your NTP strategy
  - Which devices are clients, servers, and client/servers?

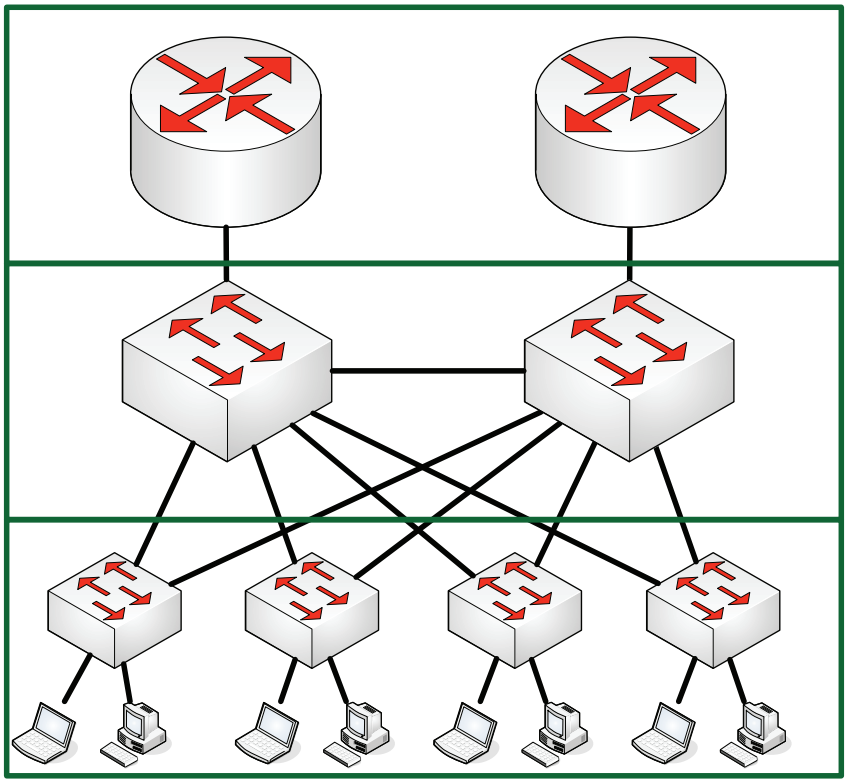
NTP stratum layers

- Some clocks are better than others
  - Your distance from the original reference clock is a stratum
- Stratum 0
  - Atomic clock, GPS clock
  - Very accurate
- Stratum 1
  - Synchronized to stratum 0 servers
  - Primary time servers
- Stratum 2
  - Sync'd to stratum 1 servers

Configuring NTP

- NTP client
  - Specify the NTP server address (IP or hostname)
  - Use multiple NTP servers (if available) for redundancy
- NTP server
  - You need at least one clock source
  - Specify the stratum level of the clock
  - If there's a choice, the lower stratum level wins

1.7 - Network Architectures



Three-Tier Architecture

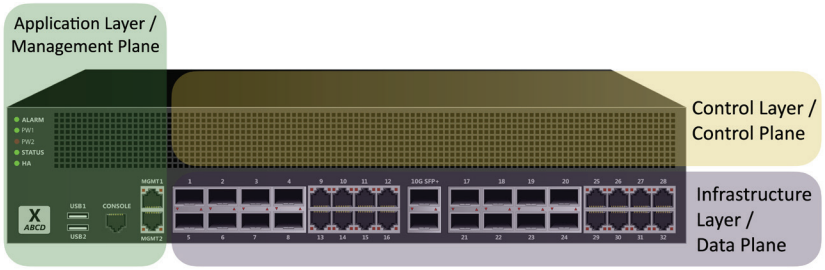
- Core
  - The "center" of the network
  - Web servers, databases, applications
  - Many people need access to this
- **Distribution**
  - A midpoint between the core and the users
  - Communication between access switches
  - Manage the path to the end users
- **Access**
  - Where the users connect
  - End stations, printers

1.7 - Network Architectures (continued)

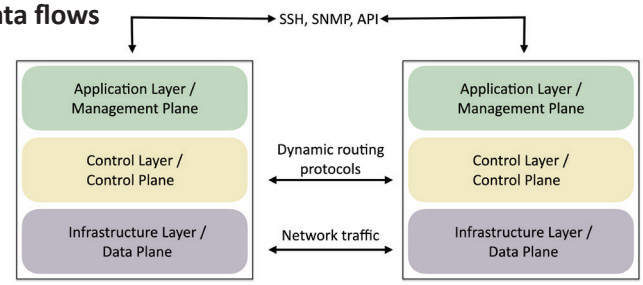
SDN (Software Defined Networking)

- Networking devices have different functional planes of operation
  - Data, control, and management planes
- Split the functions into separate logical units
  - Extend the functionality and management of a single device
  - Perfectly built for the cloud
- Infrastructure layer / Data plane
  - Process the network frames and packets
  - Forwarding, trunking, encrypting, NAT
- Control layer / Control plane
  - Manages the actions of the data plane
  - Routing tables, session tables, NAT tables
  - Dynamic routing protocol updates
- Application layer / Management plane
  - Configure and manage the device

Extend the physical architecture

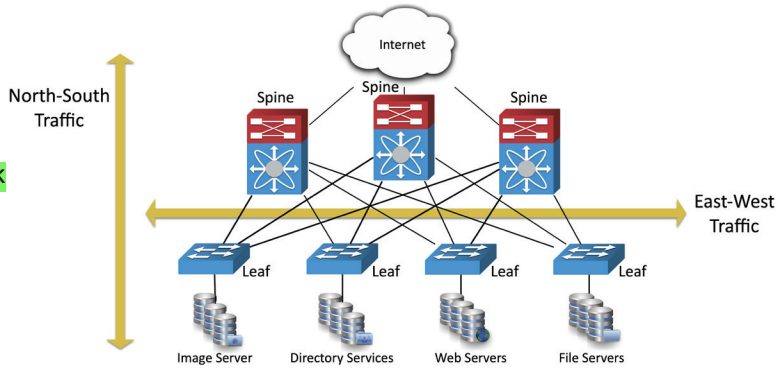


SDN data flows



Spine and leaf architecture

- Each leaf switch connects to each spine switch
  - Each spine switch connects to each leaf switch
- Leaf switches do not connect to each other
  - Same for spine switches
- Top-of-rack switching
  - Each leaf is on the "top" of a physical network rack
  - May include a group of physical racks
- Advantages
  - Simple cabling, redundant, fast
- Disadvantages
  - Additional switches may be costly



Traffic flows

- Traffic flows within a data center
  - Important to know where traffic starts and ends
- East-west
  - Traffic between devices in the same data center
  - Relatively fast response times
- North-south traffic
  - Ingress/egress to an outside device
  - A different security posture than east-west traffic

Network locations

- Branch office
  - A remote location
  - Client devices, printers, switch/router/firewall
- On-premises data center
  - Technology is located in-house
  - Requires power, cooling, and ongoing monitoring
- Colocation
  - Share a data center with others
  - Local oversight and monitoring

1.7 - Storage Area Networks

SAN

- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block-level access
  - Very efficient reading and writing
- Requires a lot of bandwidth
  - May use an isolated network and high-speed network technologies

Fibre Channel (FC)

- A specialized high-speed topology
  - Connect servers to storage
  - 2-, 4-, 8- and 16-gigabit per second rates
  - Supported over both fiber and copper
- Servers and storage connect to a Fibre Channel switch
  - Server (initiator) needs a FC interface
  - Storage (target) is commonly referenced by SCSI, SAS, or SATA commands

1.7 - Storage Area Networks (continued)

Fibre Channel over Ethernet

- Use Fibre Channel over an Ethernet network
  - No special networking hardware needed
  - Usually integrates with an existing Fibre Channel infrastructure
  - Not routable

iSCSI

- Internet Small Computer Systems Interface
  - Send SCSI commands over an IP network
  - Created by IBM and Cisco, now an RFC standard
- Makes a remote disk look and operate like a local disk
  - Like Fibre Channel
- Can be managed quite well in software
  - Drivers available for many operating systems
  - No proprietary topologies or hardware needed

1.8 - Cloud Models

Infrastructure as a service (IaaS)

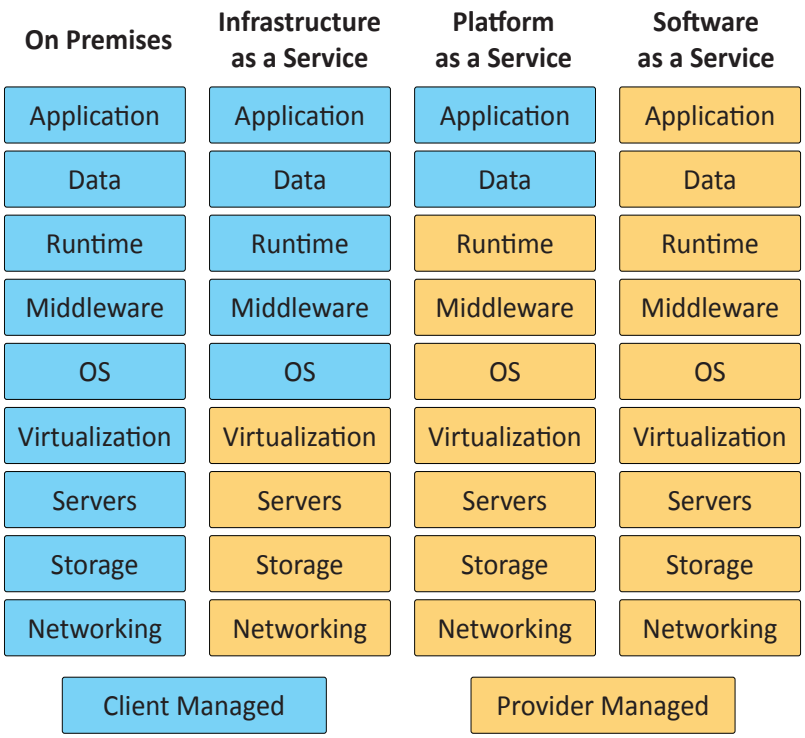
- Sometimes called Hardware as a Service (HaaS)
  - Outsource your equipment
- You're still responsible for the management
  - And for the security
- Your data is out there, but more within your control
- Web server providers

Software as a service (SaaS)

- On-demand software
  - No local installation
  - Why manage your own email distribution? Or payroll?
- Central management of data and applications
  - Your data is out there
- A complete application offering
  - No development work required
  - Google Mail

Platform as a service (PaaS)

- No servers, no software, no maintenance team, no HVAC
  - Someone else handles the platform, you handle the development
- You don't have direct control of the data, people, or infrastructure
  - Trained security professionals are watching your stuff
  - Choose carefully
- Put the building blocks together
  - Develop your app from what's available on the platform
  - SalesForce.com



Cloud deployment models

- Private - Your own virtualized local data center
- Public - Available to everyone over the Internet
- Hybrid - A mix of public and private
- Community - Several organizations share the same resources

Desktop as a Service

- Basic application usage
  - Applications actually run on a remote server
  - Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS)
  - Local device is a keyboard, mouse, and screen.
- Minimal operating system on the client
  - No huge memory or CPU needs
- Network connectivity
  - Big network requirement
  - Everything happens across the wire

1.8 - Designing the Cloud

Designing the cloud

- On-demand computing power
  - Click a button
- Elasticity
  - Scale up or down as needed
- Applications also scale
  - Scalability for large implementations
  - Access from anywhere
- Multitenancy
  - Many different clients are using the same cloud infrastructure

Infrastructure as code

- Describe an infrastructure
  - Define servers, network, and applications as code
- Modify the infrastructure and create versions
  - The same way you version application code
- Use the description (code) to build other application instances
  - Build it the same way every time based on the code
- An important concept for cloud computing
  - Build a perfect version every time

Orchestration

- Automation is the key to cloud computing
  - Services appear and disappear automatically, or at the push of a button
- Entire application instances can be instantly provisioned
  - All servers, networks, switches, firewalls, and policies
- Instances can move around the world as needed
  - Follow the sun
- The security policies should be part of the orchestration
  - As applications are provisioned, the proper security is automatically included

Connecting to the cloud

- VPN
  - Site-to-site virtual private network
  - Encrypt through the Internet
- Virtual Private Cloud Gateway
  - Connects users on the Internet
- VPC Endpoint
  - Direct connection between cloud provider networks

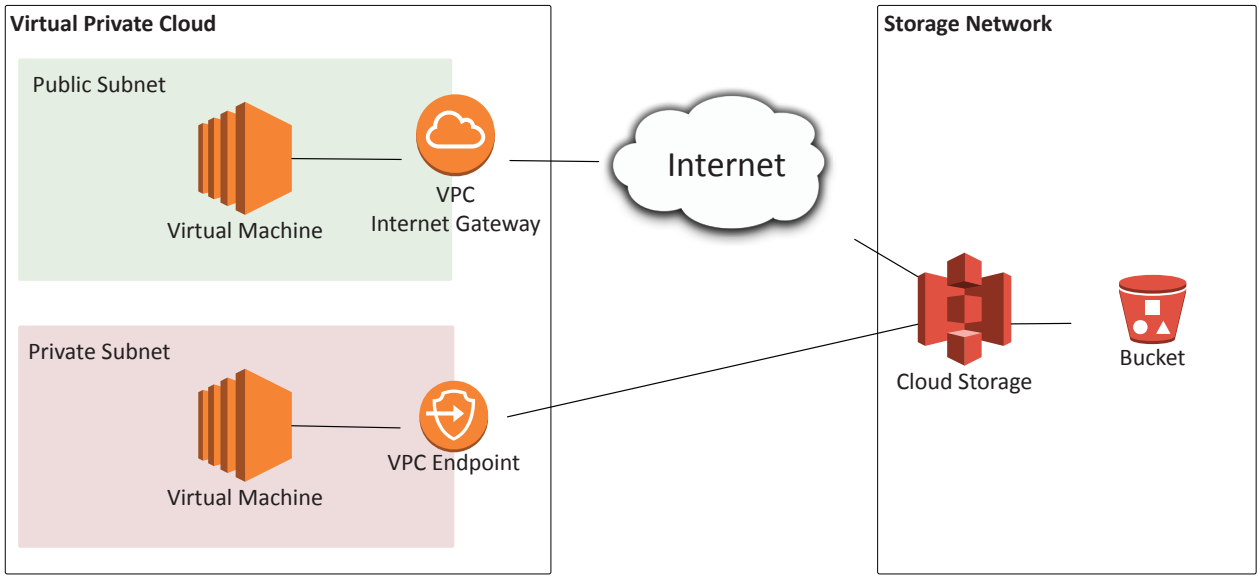
VM sprawl avoidance

- Click a button
  - You've built a server
  - Or multiple servers, networks, and firewalls
- It becomes almost too easy to build instances
  - This can get out of hand very quickly
- The virtual machines are sprawled everywhere
  - You aren't sure which VMs are related to which applications
  - It becomes extremely difficult to deprovision
- Formal process and detailed documentation
  - You should have information on every virtual object

VM escape protection

- The virtual machine is self-contained
  - There's no way out
  - Or is there?
- Virtual machine escape
  - Break out of the VM and interact with the host operating system or hardware
- Once you escape the VM, you have great control
  - Control the host and control other guest VMs
- This would be a huge exploit
  - Full control of the virtual world

Virtual private cloud endpoints



2.1 - Networking Devices

Hub
- "Multi-port repeater"
  - Traffic going in one port is repeated to every other port
  - OSI Layer 1
- Everything is half-duplex
- Becomes less efficient as network speeds increase
- 10 megabit / 100 megabit
- Difficult to find today

Bridge
- Imagine a switch with two to four ports
  - Makes forwarding decisions in software
- Connects different physical networks
  - Can connect different topologies
  - Gets around physical network size limitations / collisions
- OSI Layer 2 device
  - Distributes traffic based on MAC address
- Most bridges these days are wireless access points
  - Bridges wired Ethernet to wireless

Switch
- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- An OSI layer 2 device
  - Forwards traffic based on data link address
- Many ports and features
  - The core of an enterprise network
  - May provide Power over Ethernet (PoE)
- Multilayer switch
  - Includes Layer 3 (routing) functionality

Router
- Routes traffic between IP subnets
  - OSI layer 3 device
  - Routers inside of switches sometimes called "layer 3 switches"
  - Layer 2 = Switch
  - Layer 3 = Router
- Often connects diverse network types
  - LAN, WAN, copper, fiber

Access point
- Not a wireless router
  - A wireless router is a router and an access point in a single device
- An access point is a bridge
  - Extends the wired network onto the wireless network
  - OSI layer 2 device

Cable modem
- Broadband
  - Transmission across multiple frequencies
  - Different traffic types
- Data on the "cable" network
  - DOCSIS (Data Over Cable Service Interface Specification)
- High-speed networking
  - 4 Mbits/s through 250 Mbits/s are common
  - Gigabit speeds are possible
- Multiple services - Data, voice, video

DSL modem
- ADSL (Asymmetric Digital Subscriber Line)
  - Uses telephone lines
- Download speed is faster than the upload speed (asymmetric)
  - ~10,000 foot limitation from the central office (CO)
  - 52 Mbit/s downstream / 16 Mbit/s upstream are common
  - Faster speeds may be possible if closer to the CO

Repeater
- Receive signal, regenerate, resend
  - No forwarding decisions to make
- Common use
  - Boost copper or fiber connections
  - Convert one network media to another
  - Extend wireless network reach

Converting media
- OSI Layer 1 - Physical layer signal conversion
- Extend a copper wire over a long distance
  - Convert it to fiber, and back again
- You have fiber - The switch only has copper ports
- Almost always powered - Especially fiber to copper

2.1 - Advanced Networking Devices

Layer 3 capable switch
- A switch (Layer 2) and router (Layer 3) in the same physical device
  - Layer 3 switch
  - Layer 2 router?
- Switching still operates at OSI Layer 2, routing still operates at OSI Layer 3
  - There's nothing new or special happening here

Wireless networks everywhere
- Wireless networking is pervasive
  - And you probably don't just have a single access point
- Your access points may not even be in the same building
  - One (or more) at every remote site
- Configurations may change at any moment
  - Access policy, security policies, AP configs
- The network should be invisible to your users
  - Seamless network access, regardless of role

2.1 - Advanced Networking Devices (continued)

Wireless LAN controllers
- Centralized management of access points
  - A single "pane of glass"
- Deploy new access points
- Performance and security monitoring
- Configure and deploy changes to all sites
- Report on access point use
- Usually a proprietary system
  - Wireless controller is paired with the access points

Balancing the load
- Distribute the load
  - Multiple servers, invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Server outages have no effect, very fast convergence

Load balancer
- Configurable load - Manage across servers
- TCP offload - Protocol overhead
- SSL offload - Encryption/Decryption
- Caching - Fast response
- Prioritization - QoS
- Content switching - Application-centric balancing

IDS and IPS
- Intrusion Detection System / Intrusion Prevention System
  - Watch network traffic
- Intrusions
  - Exploits against operating systems, applications, etc.
  - Buffer overflows, cross-site scripting, other vulnerabilities
- Detection vs. Prevention
  - Detection – Alarm or alert
  - Prevention – Stop it before it gets into the network

Proxies
- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Useful for caching information, access control, URL filtering, content scanning
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

Application proxies
- Most proxies in use are application proxies
  - The proxy understands the way the application works
- A proxy may only know one application, i.e., HTTP
- Many proxies are multipurpose proxies
  - HTTP, HTTPS, FTP, etc.

VPN concentrator
- Virtual Private Network
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

VoIP technologies
- PBX (Private Branch Exchange)
  - The "phone switch"
  - Connects to phone provider network
  - Analog telephone lines to each desk
- VoIP PBX
  - Integrate VoIP devices with a corporate phone switch
- VoIP Gateway
  - Convert between VoIP protocols and traditional PSTN protocols
  - Often built-in to the VoIP PBX

Network-based Firewalls
- Filter traffic by port number or application
- Encrypt traffic - VPN between sites
- Most firewalls can be layer 3 devices (routers)
  - Often sits on the ingress/egress of the network
  - Network Address Translation (NAT), dynamic routing

2.1 - Networked Devices

VoIP phone
- A Voice over Internet Protocol
  - Instead of analog phone line or the
  - Plain Old Telephone Service (POTS)
- A relatively complex embedded system
  - Can be an important resource
- Each device is a computer
  - Separate boot process and network connection
  - Individual configurations
  - Different capabilities and functionalities

Printer
- Color and B&W output
  - Paper documents, photos
- All-in-one - AIO
  - Printer, scanner, copier, fax
- Connectivity
  - Ethernet
  - 802.11 Wireless
  - USB
  - Bluetooth / Infrared

2.1 - Networked Devices (continued)

Access control devices
- Card reader
  - Access with a smart card
- Biometric authentication
  - Fingerprint, retina, voiceprint
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Ethernet connected
  - IP address configured static or DHCP

Cameras
- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera properties are important
  - Focal length - Shorter is wider angle
  - Depth of field - How much is in focus
  - Illumination requirements - See in the dark
- Often many different cameras
  - Networked together and recorded over time

Surveillance systems
- Video/audio surveillance
  - Embedded systems in the cameras and the monitoring stations
- IP addressable
  - Multicast video
  - High definition

HVAC
- Heating, Ventilation, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- PC manages equipment
  - Makes cooling and heating decisions for workspaces and data centers
  - Network connectivity is critical

IoT (Internet of Things) devices
- Appliances - Refrigerators
- Smart devices
  - Smart speakers respond to voice commands
- Air control - Thermostats, temperature control
- Access - Smart doorbells
- May require a segmented network
  - Limit any security breaches

SCADA / ICS
- Supervisory Control and Data Acquisition System
  - Large-scale, multi-site Industrial Control Systems (ICS)
- PC manages equipment
  - Power generation, refining, manufacturing equipment
  - Facilities, industrial, energy, logistics
- Distributed control systems
  - Real-time information
  - System control
- Requires extensive segmentation
  - No access from the outside

2.2 - Dynamic Routing

Dynamic routing protocols
- Listen for subnet information from other routers
  - Sent from router to router
- Provide subnet information to other routers
  - Tell other routers what you know
- Determine the best path based on the gathered information
  - Every routing protocol has its own way of doing this
- When network changes occur, update the available routes
  - Different convergence process for every dynamic routing protocol

Which routing protocol to use?
- What exactly is a route?
  - Is it based on the state of the link?
  - Is it based on how far away it is?
- How does the protocol determine the best path?
  - Some formula is applied to the criteria to create a metric
  - Rank the routes from best to worst
- Recover after a change to the network
  - Convergence time can vary widely between routing protocols
- Standard or proprietary protocol?
  - OSPF and RIP are standards, some functions of EIGRP are Cisco proprietary

Distance-vector routing protocols
- Information passed between routers contains network details
  - How many "hops" away is another network?
  - The deciding "vector" is the "distance"
- Usually automatic
  - Very little configuration
- Good for smaller networks
  - Doesn't scale well to very large networks
- RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol)

2.2 - Dynamic Routing (continued)

Link-state routing protocols

- Information passed between routers is related to the current connectivity
  - If it's up, you can get there.
  - If it's down, you can't.
- Consider the speed of the link
  - Faster is always better, right?
- Very scalable
  - Used most often in large networks
- OSPF (Open Shortest Path First)
  - Large, scalable routing protocol

Hybrid routing protocols

- A little link-state, a little distance-vector
  - Not many examples of a hybrid routing protocol
- BGP (Border Gateway Protocol)
  - Determines route based on paths, network policies, or configured rule-sets

2.2 - Routing Technologies

Routing tables

- A list of directions for your packets
  - A table with many routes to your destination
  - Packets stop at every router and ask for directions
- Routing table in routers, workstations, and other devices
  - Every device needs directions

The hop

- A hop
  - A packet passes through a router
- The next hop
  - The destination address of the next gateway
- A router doesn't need to know how to get everywhere
  - It just needs to know how to get out of here
  - A default route handles everything not specifically listed
- "Time to live" in IPv4, "hop limit" in IPv6
  - Avoids a packet looping forever

Configuring the next hop

- Every router needs to know where traffic should be sent
  - Your packet is always asking for directions
- A router with the incorrect next hop will result in a routing problem
  - Data will go the wrong direction
  - A routing loop is easy to create
  - You'll know quickly if there's a loop

Default routes

- A route when no other route matches
  - The "gateway of last resort"
- A remote site may have only one route
  - Go that way -> rest of the world
  - Destination of 0.0.0.0/0
- Can dramatically simplify the routing process
  - Works in conjunction with all other routing methods

Routing metrics

- Each routing protocol has its own way of calculating the best route
  - i.e., RIPv2, OSPF, EIGRP
- Metric values are assigned by the routing protocol
  - RIPv2 metrics aren't useful to OSPF or EIGRP
- Use metrics to choose between redundant links
  - Choose the lowest metric,
  - i.e., 1 is better than 2

Administrative distances

- What if you have two routing protocols, and both know about a route to a subnet?
  - Two routing protocols, two completely different metric calculations
  - You can't compare metrics across routing protocols
  - Which one do you choose?
- Administrative distances
  - Used by the router to determine which routing protocol has priority

Managing network utilization

- Many different devices
  - Desktop, laptop, VoIP phone, mobile devices
- Many different applications
  - Mission critical applications, streaming video, streaming audio
- Different apps have different network requirements
  - Voice is real-time
  - Recorded streaming video has a buffer
  - Database application is interactive
- Some applications are "more important" than others
  - Voice traffic needs to have priority over YouTube

Traffic shaping

- Traffic shaping, packet shaping
- Control by bandwidth usage or data rates
- Set important applications to have higher priorities than other apps
- Manage the Quality of Service (QoS)
  - Routers, switches, firewalls, QoS devices

2.3 - Introduction to Ethernet

Field	Bytes	Description
Preamble	7	56 alternating ones and zeros used for synchronization (101010…)
SFD	1	Start Frame Delimiter - designates the end of the preamble (10101011)
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
EtherType	2	Describes the data contained the payload
Payload	46 - 1500	Layer 3 and higher data
FCS	4	Frame Check Sequence - CRC checksum of the frame

The MAC address
- Ethernet Media Access Control address
  - The "physical" address of a network adapter
  - Unique to a device
- 48 bits / 6 bytes long
  - Displayed in hexadecimal

8c:2d:aa:4b:98:a7

Organizationally Unique Identifier (OUI) (the manufacturer)

Network Interface Controller-Specific (the serial number)

Duplex
- Half-duplex
  - A device cannot send and receive simultaneously
  - All LAN hubs are half-duplex devices
  - Switch interfaces can be configured as half-duplex, but usually only when connecting to another half-duplex device
- Full-duplex
  - Data can be sent and received at the same time
  - A properly configured switch interface will be set to full-duplex

CSMA/CD
- CS - Carrier Sense
  - Is there a carrier? Is anyone communicating?
- MA - Multiple Access
  - More than one device on the network
- CD - Collision Detect
  - Collision - Two stations talking at once
  - Identify when data gets garbled
- Half-duplex Ethernet - not used any longer

CSMA/CD operation
- Listen for an opening
  - Don't transmit if the network is already busy
- Send a frame of data
  - You send data whenever you can
  - There's no queue or prioritization
- If a collision occurs
  - Transmit a jam signal to let everyone know a collision has occurred
  - Wait a random amount of time, then retry

2.3 - Network Switching Overview

The Switch
- Forward or drop frames
  - Based on the destination MAC address
- Gather a constantly updating list of MAC addresses
  - Builds the list based on the source MAC address of incoming traffic
- Maintain a loop-free environment
  - Using Spanning Tree Protocol (STP)

Learning the MACs
- Switches examine incoming traffic
  - Makes a note of the source MAC address
- Adds unknown MAC addresses to the MAC address table
  - Sets the output interface to the received interface

Flooding for unknown Macs
- The switch doesn't always have a MAC address in the table
- When in doubt, send the frame to everyone

Address Resolution Protocol
- Determine a MAC address based on an IP address
  - You need the hardware address to communicate
- `arp -a`
  - View local ARP table

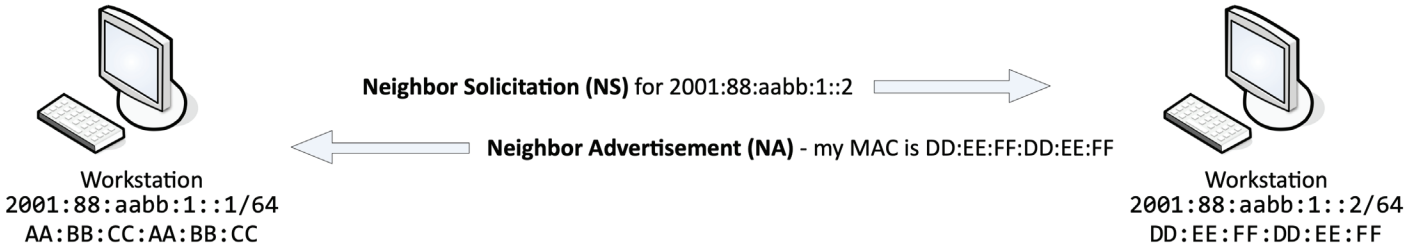
2.3 - Network Switching Overview (continued)

NDP (Neighbor Discovery Protocol)

- No broadcasts!
  - Operates using multicast with ICMPv6
- Neighbor MAC Discovery
  - Replaces the IPv4 ARP
- SLAAC (Stateless Address Autoconfiguration)
  - Automatically configure an IP address without a DHCP server
- DAD (Duplicate Address Detection)
  - No duplicate IPs!
- Discover routers
  - Router Solicitation (RS) and Router Advertisement (RA)

Howdy, neighbor

- There's no ARP in IPv6
  - So how do you find out the MAC address of a device?
- Neighbor Solicitation (NS)
  - Sent as a multicast
- Neighbor Advertisement (NA)



Power over Ethernet (PoE)

- Power provided on an Ethernet cable
  - One wire for both network and electricity
  - Phones, cameras, wireless access points
  - Useful in difficult-to-power areas
- Power provided at the switch
  - Built-in power - Endspans
  - In-line power injector - Midspans
- Power modes
  - Mode A - Power on the data pairs
  - Mode B - Power on the spare pairs

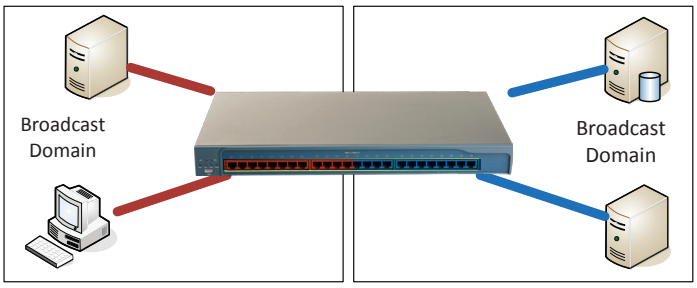
PoE and POE+

- PoE: IEEE 802.3af-2003
  - The original PoE specification
  - Now part of the 802.3 standard
  - 15.4 watts DC power
  - Maximum current of 350 mA
- POE+: IEEE 802.3at-2009
  - An updated PoE specification
  - Now also part of the 802.3 standard
  - 25.5 watts DC power
  - Maximum current of 600 mA

2.3 - VLANs and Trunking

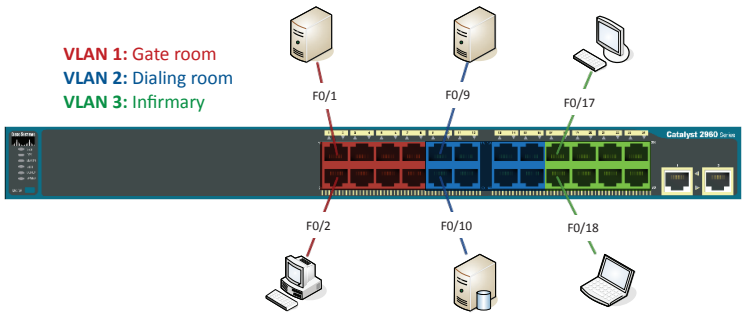
LANs

- Local Area Networks
  - A group of devices in the same broadcast domain



Virtual LANs

- Virtual Local Area Networks
  - A group of devices in the same broadcast domain
  - Separated logically instead of physically



2.3 - VLANs and Trunking (continued)

802.1Q trunking

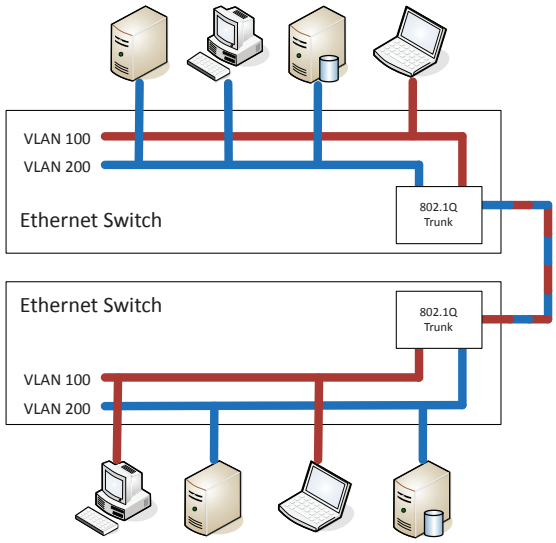
- Take a normal Ethernet frame

Preamble	SFD	Destination MAC	Source MAC	Type	Payload	FCS

- Add a VLAN header in the frame

Preamble	SFD	Destination MAC	Source MAC	VLAN	Type	Payload	FCS

- VLAN IDs - 12 bits long, 4,094 VLANs
  - "Normal range" - 1 through 1005,
    "Extended range" - 1006 through 4094
  - 0 and 4,095 are reserved VLAN numbers
- Before 802.1Q, there was ISL (Inter-Switch Link)
  - ISL is no longer used;
    everyone now uses the 802.1Q standard

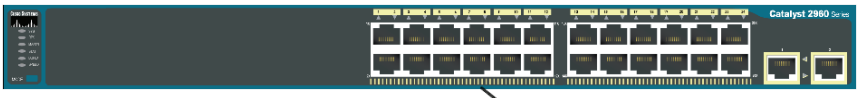


Working with data and voice

- Old school: Connect computer to switch,
  connect phone to PBX (Private Branch Exchange)
  - Two physical cables, two different technologies
- Now: Voice over IP (VoIP)
  - Connect all devices to the Ethernet switch
  - One network cable for both

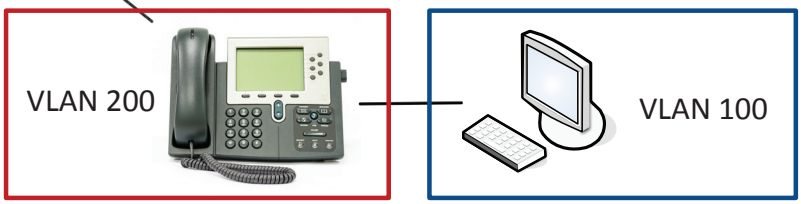
Just one problem...

- Voice and data don't like each other
  - Voice is very sensitive to congestion
  - Data loves to congest the network
- Put the computer on one VLAN and the phone on another
  - But the switch interface is not a trunk
  - How does that work?
- Each switch interface has a data VLAN and a voice VLAN
  - Configure each of them separately



Configuring voice and data VLANs

- Data passes as a normal untagged access VLAN
- Voice is tagged with an 802.1Q header



2.3 - Spanning Tree Protocol

Loop protection

- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
  - Relatively easy to resolve
- IEEE standard 802.1D to prevent loops
  in bridged (switched) networks (1990)

STP port states

- Blocking - Not forwarding to prevent a loop
- Listening - Not forwarding and cleaning the MAC table
- Learning - Not forwarding and adding to the MAC table
- Forwarding - Data passes through and is fully operational
- Disabled - Administrator has turned off the port

RSTP (802.1w)

- Rapid Spanning Tree Protocol (802.1w)
  - A much-needed updated of STP
  - This is the latest standard
- Faster convergence - From 30 to 50 seconds to 6 seconds
- Backwards-compatible with 802.1D STP
  - You can mix both in your network
- Very similar process - An update, not a wholesale change

2.3 - Interface Configurations

Basic Interface Configuration

- Speed and duplex
  - Speed: 10 / 100 / 1,000 / 10 Gig
  - Duplex: Half/Full
  - Automatic and manual
  - Needs to match on both sides
- IP address management
  - Layer 3 interfaces, VLAN interfaces
  - Management interfaces
  - IP address, subnet mask/CIDR block, default gateway, DNS (optional)

VLANs

- VLAN assignment
  - Each device port should be assigned a VLAN
- Trunking
  - Connecting switches together
  - Multiple VLANs in a single link
- Tagged and untagged VLANs
  - A non-tagged frame is on the default VLAN
    - Also called the native VLAN
  - Trunk ports will tag the outgoing frames
    - And remove the tag on incoming frames

LAG and mirroring

- Port bonding / Link aggregation (LAG)
  - Multiple interfaces acts like one big interface
  - LACP (Link Aggregation Control Protocol)
  - Adds additional automation and management
- Port mirroring
  - Copy traffic from one interface
  - Used for packet captures, IDS
  - Mirror traffic on the same switch
  - Mirror traffic from one switch to another
- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

Jumbo frames

- Ethernet frames with more than 1,500 bytes of payload
  - Up to 9,216 bytes (9,000 is the accepted norm)
- Increases transfer efficiency
  - Per-packet size
  - Fewer packets to switch/route
- Ethernet devices must support jumbo frames
  - Switches, interface cards
  - Not all devices are compatible with others

Ethernet flow control

- Ethernet is non-deterministic
  - You never know just how fast or slow traffic will flow
- If things get busy, tell the other device to slow down
  - Switches only have so much buffer
- One popular flow control method is IEEE 802.3x
  - The “pause” frame
- Enhancements have been made through the years
  - Incorporates CoS (Class of Service)

Port security

- Prevent unauthorized users from connecting to a switch interface - Alert or disable the port
- Based on the source MAC address
  - Even if forwarded from elsewhere
- Each port has its own config - Unique rules for every interface

Port security operation

- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Default is to disable the interface

2.3 - Straight-Through and Crossover Cables

Straight-through cables

- Patch cables - the most common Ethernet cable
- Connect workstations to network devices
  - Workstation to switch
  - Router to switch

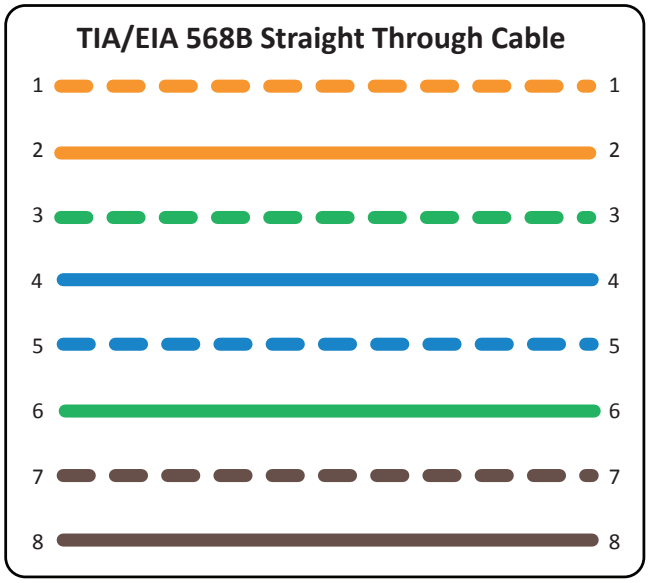
Ethernet crossover cables

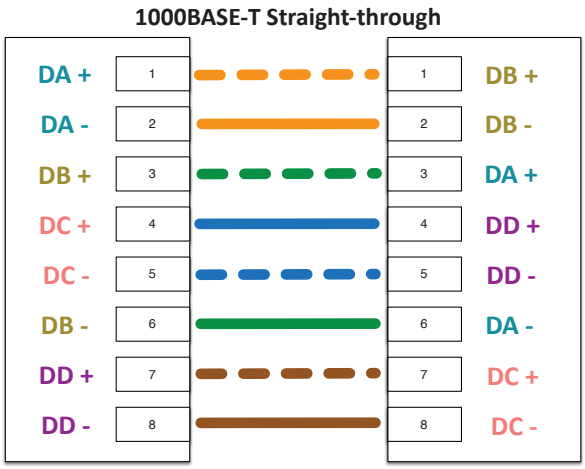
- Connect MDI to MDI
- Connect MDI-X to MDI-X
- Auto-MDI-X is on most modern Ethernet devices
  - Automatically decides to cross-over
- This is obviously not 568A on one side and 568B on the other
  - 568A and 568B are cabling standards
  - The TIA-568 standard does not define Ethernet (or other) crossover cables

Straight-through or crossover?

- Workstation to switch
  - Straight-through
- Router to switch
  - Straight-through
- Switch to switch
  - Crossover
- Router to router
  - Crossover
- Workstation to workstation
  - Crossover
- Workstation to router
  - Crossover

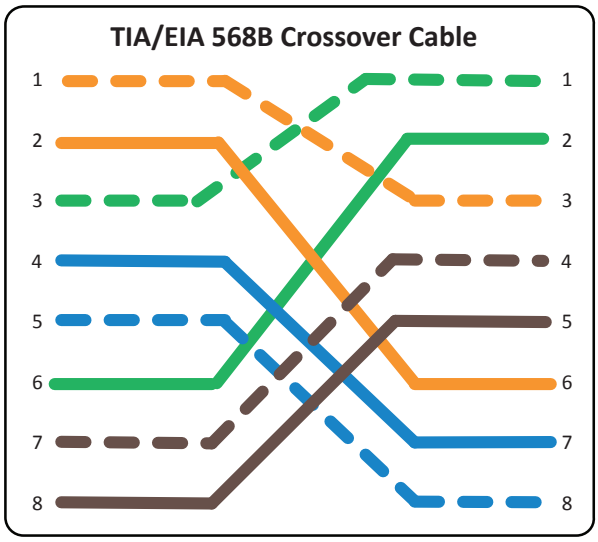
2.3 - Straight-Through and Crossover Cables (continued)

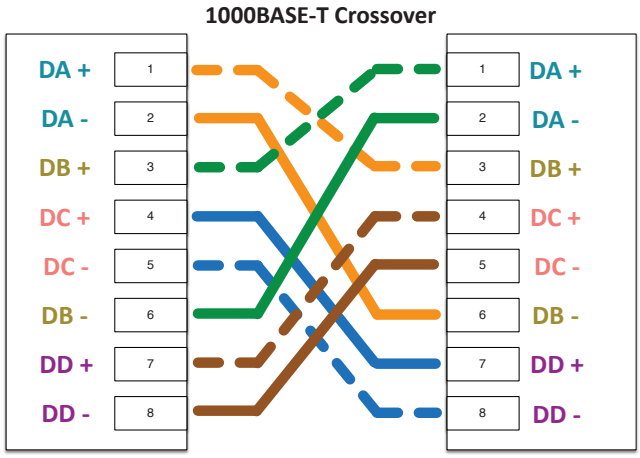




Media Dependent Interface (MDI)
Network Interface Card

Media Dependent Interface Crossover (MDI-X)
Network Switch





Media Dependent Interface (MDI)
Network Interface Card

Media Dependent Interface (MDI)
Network Interface Card

2.4 - Wireless Standards

Wireless Standards

- Wireless networking (802.11)
  - Managed by the IEEE LAN/MAN Standards Committee (IEEE 802)
- Many updates over time
- Wi-Fi Alliance handles interoperability testing

802.11a

- One of the original 802.11 wireless standards
  - October 1999
- Operates in the 5 GHz range
- 54 megabits per second (Mbit/s)
- Smaller range than 802.11b
  - Higher frequency is absorbed by objects in the way
  - Many rules-of-thumb calculate 1/3rd the range of 802.11b or 802.11g
- Not commonly seen today

802.11b

- Also an original 802.11 standard
  - October 1999
- Operates in the 2.4 GHz range
- 11 megabits per second (Mbit/s)
- Better range than 802.11a
  - Less absorption problems
- More frequency conflict
  - Baby monitors, cordless phones, microwave ovens, Bluetooth
- Not commonly seen today

2.4 - Wireless Standards (continued)

802.11g
- An "upgrade" to 802.11b - June 2003
- Operates in the 2.4 GHz range
- 54 megabits per second (Mbit/s)
  – Same as 802.11a
- Backwards-compatible with 802.11b
- Same 2.4 GHz frequency conflict problems as 802.11b

802.11n (Wi-Fi 4)
- The update to 802.11g, 802.11b, and 802.11a
  – October 2009
- Operates at 5 GHz and/or 2.4 GHz
  – 40 MHz channel widths
- 600 megabits per second (Mbit/s)
  – 40 MHz mode and 4 antennas
- 802.11n uses MIMO
  – Multiple-input multiple-output
  – Multiple transmit and receive antennas

802.11ac (Wi-Fi 5)
- Approved in January 2014
  – Significant improvements over 802.11n
- Operates in the 5 GHz band
  – Less crowded, more frequencies (up to 160 MHz channel bandwidth)
- Increased channel bonding - Larger bandwidth usage
- Denser signaling modulation - Faster data transfers
- Eight MU-MIMO streams
  – Twice as many streams as 802.11n
  – Nearly 7 gigabits per second

802.11ax (Wi-Fi 6)
- Approved in February 2021
  – The successor to 802.11ac/Wi-Fi 5
- Operates at 5 GHz and/or 2.4 GHz
  – 20, 40, 80, and 160 MHz channel widths
- 1,201 megabits per second per channel
  – A relatively small increase in throughput
  – Eight bi-directional MU-MIMO streams
- Orthogonal frequency-division multiple access (OFDMA)
  – Works similar to cellular communication
  – Improves high-density installations

	Frequencies	Maximum MIMO streams	Maximum theoretical throughput (per stream)	Maximum theoretical throughput (total)
802.11a	5 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	Not applicable	11 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11n	5 GHz / 2.4 GHz	4 x MIMO	150 Mbit/s	600 Mbit/s
802.11ac	5 GHz	8 x DL MU-MIMO	867 Mbit/s	6.9 Gbit/s
802.11ax	5 GHz / 2.4 GHz	8 x DL and UL MU-MIMO	1,201 Mbit/s	9.6 Gbit/s

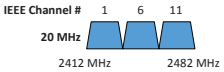
2.4 - Wireless Technologies

802.11 technologies
- Frequency
  – 2.4 GHz or 5 GHz
  – And sometimes both
- Channels
  – Groups of frequencies, numbered by the IEEE
  – Non-overlapping channels would be necessary
- Bandwidth
  – Amount of frequency in use
  – 20 MHz, 40 MHz, 80 MHz, 160 MHz

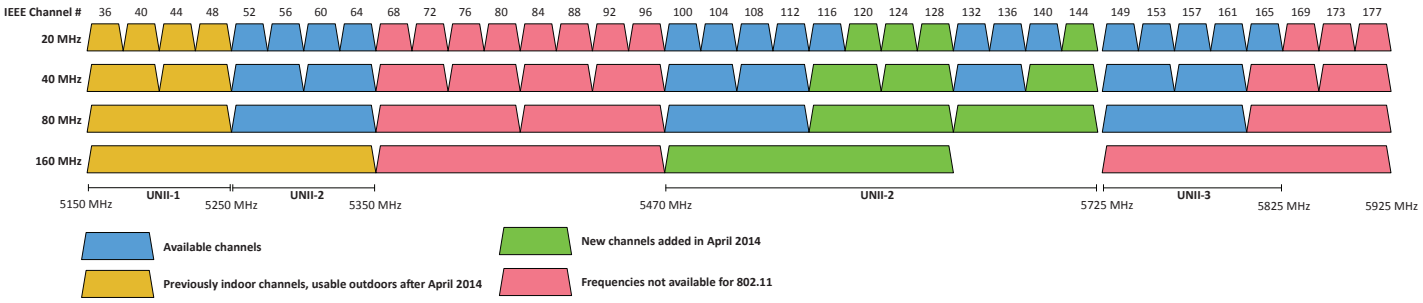
802.11 channel bandwidths
- 802.11a (20 MHz), 802.11b (22 MHz), 802.11g (20 MHz)
- 802.11n (20 MHz, 40 MHz, 80 MHz)
  – Increase bandwidth with bonded channels
  – In 2.4 GHz, a 40 MHz channel uses over 80% of the available bandwidth
- 802.11ac (20 MHz, 40 MHz, 80 MHz, 80+80 MHz, 160 MHz)
  – 40 MHz for 802.11n stations, 80 MHz required for 802.11ac stations
  – 160 MHz optional (contiguous channels or non-contiguous bonded channels)
- 802.11ax (20 MHz, 40 MHz, 80 MHz, 80+80 MHz, 160 MHz)
  – Similar bandwidths to 802.11ac

2.4 - Wireless Technologies (continued)

2.4 GHz Spectrum for 802.11 - North America



5 GHz Spectrum for 802.11 - North America



Independent basic service set (IBSS)

- Two devices communicate directly to each other using 802.11
  - No access point required
- Ad hoc
  - Created for a particular purpose without any previous planning
  - Without an AP
- Temporary or long-term communication
  - Connect to a device with an ad hoc connection
  - Configure it with the access point settings and credentials

SSID and BSSID

- Every wireless network needs a name
  - SSID (Service Set Identifier)
- There might be multiple access points supporting an SSID
  - How does your computer tell them apart?
  - The hardware address of an access point is a BSSID (Basic Service Set Identifier)
  - The MAC (Media Access Control) address

Extending the network

- Most organizations have more than one access point
  - Tens or hundreds
- Wireless network names can be used across access points
  - Makes it easier to roam from one part of the network to another
- The network name shared across access points is an ESSID (Extended Service Set Identifier)
- Your device automatically roams when moving between access points
  - You don't have to manually reconnect

Counting antennas

- New technologies were added to
  - 802.11n, 802.11ac, and 802.11ax
  - Send multiple streams of information over the same frequency at the same time
  - 802.11n - MIMO (Multiple-Input and Multiple-Output)
  - 802.11ac - Downstream MU-MIMO (Multi-user MIMO)
  - 802.11ax - Downstream and upstream MU-MIMO
- Number of antennas (802.11n, 802.11ac, 802.11ax)
  - Used to determine the number of available streams
  - (Antennas on the access point) x (antennas on the client): number of streams
  - 2x2:2, 3x3:2, 4x4:4

Omnidirectional antennas

- One of the most common
  - Included on most access points
- Signal is evenly distributed on all sides
  - Omni=all
- Good choice for most environments
  - You need coverage in all directions
- No ability to focus the signal
  - A different antenna will be required

Directional antennas

- Focus the signal
  - Increased distances
- Send and receive in a single direction
  - Focused transmission and listening
- Antenna performance is measured in dB
  - Double power every 3dB of gain
- Yagi antenna
  - Very directional and high gain
- Parabolic antenna
  - Focus the signal to a single point

2.4 - Wireless Encryption

Securing a wireless network

- An organization's wireless network can contain confidential information
  - Not everyone is allowed access
- Authenticate the users before granting access
  - Who gets access to the wireless network?
  - Username, password, multi-factor authentication
- Ensure that all communication is confidential
  - Encrypt the wireless data
- Verify the integrity of all communication
  - The received data should be identical to the original sent data
  - A message integrity check (MIC)

WPA (Wi-Fi Protected Access)

- 2002: WPA was the replacement for serious cryptographic weaknesses in WEP
  - (Wired Equivalent Privacy)
  - Don't use WEP
- Needed a short-term bridge between WEP and whatever would be the successor
  - Run on existing hardware
- WPA: RC4 with TKIP (Temporal Key Integrity Protocol)
  - Initialization Vector (IV) is larger and an encrypted hash
  - Every packet gets a unique 128-bit encryption key

Wireless encryption

- All wireless computers are radio transmitters and receivers - Anyone can listen in
- Solution: Encrypt the data
  - Everyone has an encryption key
- Only people with the right key can transmit and listen
  - WPA2 and WPA3

WPA2 and CCMP

- Wi-Fi Protected Access II (WPA2)
  - WPA2 certification began in 2004
- CCMP block cipher mode
  - Counter Mode with Cipher Block Chaining
  - Message Authentication Code Protocol, or
  - Counter/CBC-MAC Protocol
- CCMP security services
  - Data confidentiality with AES encryption
  - Message Integrity Check (MIC) with CBC-MAC

WPA3 and GCMP

- Wi-Fi Protected Access 3 (WPA3)
  - Introduced in 2018
- GCMP block cipher mode
  - Galois/Counter Mode Protocol
  - A stronger encryption than WPA2
- GCMP security services - Data confidentiality with AES
  - Message Integrity Check (MIC) with Galois Message Authentication Code (GMAC)

The WPA2 PSK problem

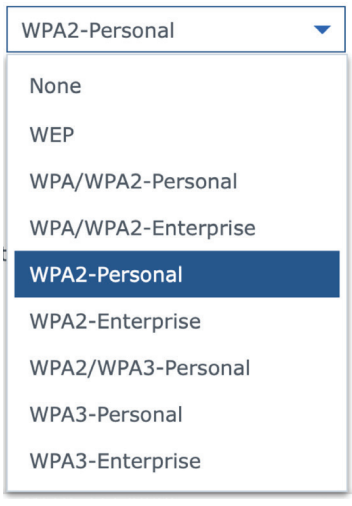
- WPA2 has a PSK brute-force problem
  - Listen to the four-way handshake
  - Some methods can derive the PSK hash without the handshake
  - Capture the hash
- With the hash, attackers can brute force the pre-shared key (PSK)
- This has become easier as technology improves
  - A weak PSK is easier to brute force
  - GPU processing speeds
  - Cloud-based password cracking
- Once you have the PSK, you have everyone's wireless key
  - There's no forward secrecy

SAE

- WPA3 changes the PSK authentication process
  - Includes mutual authentication
  - Creates a shared session key without sending that key across the network
  - No more four-way handshakes, no hashes, no brute force attacks
  - Adds perfect forward secrecy
- Simultaneous Authentication of Equals (SAE)
  - A Diffie-Hellman derived key exchange with an authentication component
  - Everyone uses a different session key, even with the same PSK
  - An IEEE standard - the dragonfly handshake

Wireless security modes

- Configure the authentication on your wireless access point / wireless router
- Open System - No authentication password is required
- WPA2/3-Personal / WPA2/3-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA2/3-Enterprise / WPA2/3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS)



2.4 - Cellular Standards

Cellular networks

- Mobile devices - "Cell" phones
- Separate land into "cells"
  - Antenna coverages a cell with certain frequencies
- 2G networks
  - GSM - Global System for Mobile Communications
  - CDMA - Code Division Multiple Access
- Poor data support
  - Originally used circuit-switching
  - Minor upgrades for some packet-switching

GSM

- Global System for Mobile Communications
  - Mobile networking standard
- 90% of the market
  - Originally an EU standard - Worldwide coverage
- Used by AT&T and T-Mobile in the United States
  - Move your SIM card (Subscriber Identity Module) from phone to phone
- Original GSM standard used multiplexing
  - Everyone gets a little slice of time

CDMA

- Code Division Multiple Access
  - Everyone communicates at the same time
  - Each call uses a different code
  - The codes are used to filter each call on the receiving side
- Used by Verizon and Sprint
  - Handsets are controlled by the network provider
  - Not much adoption elsewhere

3G technology

- 3rd Generation
  - Introduced in 1998
- Upgraded data connectivity over 2G
  - Incremental 3G updates improved speeds
  - Usually several megabits per second
- Bandwidth improvement allowed new functionality
  - GPS, mobile television, video on demand, video conferencing

4G and LTE

- Long Term Evolution (LTE) - A "4G" technology
  - Converged standard (GSM and CDMA providers)
  - Based on GSM and EDGE (Enhanced Data Rates for GSM Evolution
  - Standard supports download rates of 150 Mbit/s
- LTE Advanced (LTE-A)
  - Standard supports download rates of 300 Mbit/s

5G

- Fifth generation cellular networking
  - Launched worldwide in 2020
- Significant performance improvements
  - At higher frequencies
  - Eventually 10 gigabits per second
  - Slower speeds from 100-900 Mbit/s
- Significant IoT impact
  - Bandwidth becomes less of a constraint
  - Larger data transfers
  - Faster monitoring and notification
  - Additional cloud processing

3.1 - Performance Metrics

Device performance

- Temperature
  - Internal sensors, sometimes many
  - Can be an early warning of excessive utilization or hardware issues
- CPU usage
  - Measures performance of the processor(s)
  - Overall performance is usually based on these values
- Memory
  - The operational resource
  - Running out of memory is usually a fatal event

Bandwidth monitors

- The fundamental network statistic
  - Amount of network use over time
- Many different ways to gather this metric
  - SNMP, NetFlow, sFlow, IPFIX protocol analysis, software agent
- Identify fundamental issues
  - Nothing works properly if bandwidth is highly utilized

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

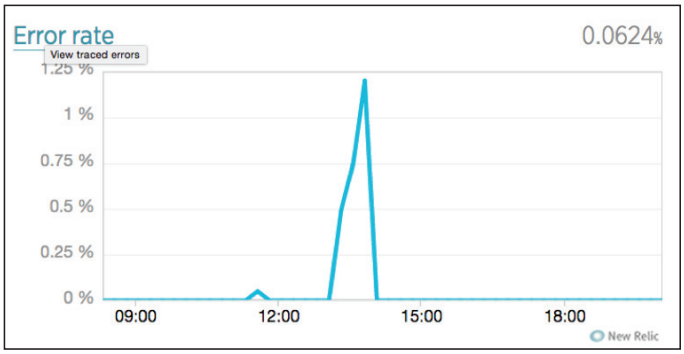
Jitter

- 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

3.1 - Performance Metrics (continued)

Monitoring the interface

- Often your first sign of trouble
  - The local problems are easy to attack
- Can sometimes indicate a bigger issue
  - Problem with a switch or congestion in the network
- View in the operating system
  - Interface details
- Monitor with SNMP
  - Remote monitoring of all devices
  - Most metrics are in MIB-II
  - Proprietary MIB may be available



Interface monitoring

- Link status - link up, or link down?
  - May be a problem on the other end of the cable
- Error rate
  - Problems with the signal - CRC error, runt, giant
- Utilization
  - Per-interface network usage
  - Run bandwidth tests to view throughput
- Discards, packet drops
  - No errors in the packet, but system could not process
- Interface resets
  - Packets are queued, but aren't sent
  - Connection is good, but line protocols aren't talking
  - Reset and hope for the best
- Speed and duplex
  - These should match on both sides
  - Auto speed and auto duplex isn't always the best option
  - Check for expected throughput

3.1 - SNMP

SNMP

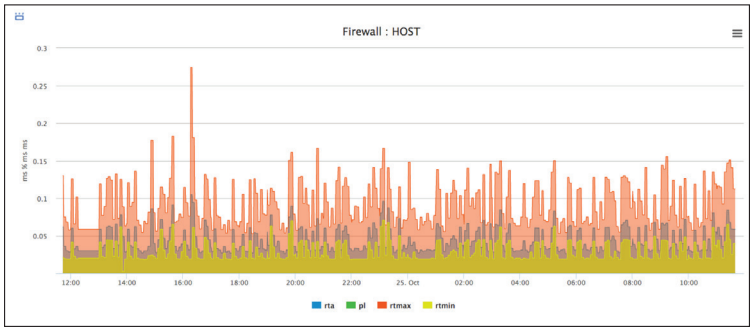
- Simple Network Management Protocol
  - A database of data (MIB) - Management Information Base
  - The database contains OIDs - Object Identifiers
  - Poll devices over udp/161
- SNMP v1 - The original
  - Structured tables, in-the-clear
- SNMP v2 – A good step ahead
  - Data type enhancements, bulk transfers, still in-the-clear
- SNMP v3 - The new standard
  - Message integrity, authentication, encryption

SNMP OIDs

- An object identifier can be referenced by name or number
  - .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).snmp(11).snmpOutTraps(29).0
  - .1.3.6.1.2.1.11.29.0
- Every variable in the MIB has a corresponding OID
  - Some are common across devices
  - Some manufacturers define their own object identifiers
- The SNMP manager requests information based on OID
  - A consistent reference across devices

SNMP Traps

- Most SNMP operations expect a poll
  - Devices then respond to the SNMP request
  - This requires constant polling
- SNMP traps can be configured on the monitored device
  - Communicates over udp/162
- Set a threshold for alerts
  - If the number of CRC errors increases by 5, send a trap
  - Monitoring station can react immediately



3.1 - Logs and Monitoring

Traffic logs
- View traffic information from routers, switches, firewalls, etc.
  - Identify traffic flows
  - View traffic summaries
- Can be very detailed
  - Every flow from every device
- Important historical information
  - Monitoring, post-event analysis

Audit logs
- What did they do, and when did they do it?
  - Often more specific than general traffic logs

Syslog
- Standard for message logging
  - Diverse systems create a consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM (Security Information and Event Manager)
- Each log entry is labeled
  - Facility code (program that created the log) and severity level

Severity levels
- Not all alerts have the same priority
  - Low level debug and information
  - High level critical and alert
- Alerts can be used as a filter
  - Only show Warning level and higher
- You decide the importance of each alert level
  - Informational may or may not be useful

Interface errors
- Runts
  - Frames that are less than 64 bytes
  - May be a result of a collision
- Giants - Frames that are more than 1518 bytes
- CRC error
  - Failed the Frame Check Sequence
  - May indicate a bad cable or interface
- Encapsulation error
  - Inconsistent configurations between switches - ISL or 802.1Q

Environmental sensors
- Temperature - Devices need constant cooling (So do humans)
- Humidity level
  - High humidity promotes condensation
  - Low humidity promotes static discharges
- Electrical - Device and circuit load
- Flooding - Water and electrical devices don't get along

NetFlow
- Gather traffic statistics from all traffic flows
  - Shared communication between devices
- NetFlow
  - Standard collection method - Many products and options
- Probe and collector
  - Probe watches network communication
  - Summary records are sent to the collector
- Usually a separate reporting app
  - Closely tied to the collector

Uptime and downtime
- Is it up or down?
  - It can often be difficult to tell
- Uptime and downtime status page
  - A summary of availability
  - You know they know

3.2 - Plans and Procedures

Change management
- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
  - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

Security incidents
- User clicks an email attachment and executes malware
  - Malware then communicates with external servers
- DDoS
  - Botnet attack
- Confidential information is stolen
  - Thief wants money or it goes public
- User installs peer-to-peer software and allows external access to internal servers

3.2 - Plans and Procedures (continued)

NIST SP800-61

- National Institute of Standards and Technology
  - NIST Special Publication 800-61 Revision 2
  - Computer Security Incident
  - Handling Guide
- The incident response lifecycle:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-incident Activity

Disaster recovery plan

- If a disaster happens, IT should be ready
  - Part of business continuity planning
  - Keep the organization up and running
- Disasters are many and varied
  - Natural disasters
  - Technology or system failures
  - Human-created disasters
- A comprehensive plan
  - Recovery location
  - Data recovery method
  - Application restoration
  - IT team and employee availability

Continuity of operations planning (COOP)

- Not everything goes according to plan
  - Disasters can cause a disruption to the norm
- We rely on our computer systems
  - Technology is pervasive
- There needs to be an alternative
  - Manual transactions
  - Paper receipts
  - Phone calls for transaction approvals
- These must be documented and tested before a problem occurs

System life cycle

- Managing asset disposal
  - Desktops, laptops, tablets, mobile devices
- Disposal becomes a legal issue
  - Some information must not be destroyed
  - Consider offsite storage
- You don't want critical information in the trash
  - People really do dumpster dive
  - Recycling can be a security concern

Standard operating procedures

- Organizations have different business objectives
  - Processes and procedures
- Operational procedures
  - Downtime notifications, facilities issues
- Software upgrades - Testing, change control
- Documentation is the key
  - Everyone can review and understand the policies

Common agreements

- Service Level Agreement (SLA)
  - Minimum terms for services provided
  - Uptime, response time agreement, etc.
  - Commonly used between customers and service providers
- Memorandum of Understanding (MOU)
  - Both sides agree on the contents of the memorandum
  - Usually includes statements of confidentiality
  - Informal letter of intent; not a signed contract

Non-disclosure agreement (NDA)

- Confidentiality agreement between parties
  - Information in the agreement should not be disclosed
- Protects confidential information
  - Trade secrets, business activities
  - Anything else listed in the NDA
- Unilateral or bilateral (or multilateral)
  - One-way NDA or mutual NDA
- Formal contract - Signatures are usually required

3.2 - Security Policies

Password policy

- Make your password strong
  - Resist guessing or brute-force attack
- Increase password entropy
  - No single words, no obvious passwords (What's the name of your dog?)
  - Mix upper and lower case and use special characters (Don't replace a o with a 0, t with a 7)
- Stronger passwords are at least 8 characters
  - Consider a phrase or set of words
- Prevent password reuse
  - System remembers password history, requires unique passwords

Acceptable use policies (AUP)

- What is acceptable use of company assets?
  - Detailed documentation
  - May be documented in the Rules of Behavior
- Covers many topics
  - Internet use, telephones, computers, mobile devices, etc.
- Used by an organization to limit legal liability
  - If someone is dismissed, these are the well-documented reasons why

3.2 - Security Policies (continued)

BYOD
- Bring Your Own Device or Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?

Remote access policies
- Easy to control internal communication
  - More difficult when people leave the building
- Policy for everyone
  - Including third-party access
- Specific technical requirements
  - Encrypted connection, confidential credentials, use of network, hardware and software requirements

On-boarding
- Bring a new person into the organization
  - New hires or transfers
- IT agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with the proper groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc.
  - Preconfigured and ready to go

Off-boarding
- All good things…
  - But you knew this day would come
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- What happens to the hardware?
- What happens to the data?
- Account information is usually deactivated
  - But not always deleted

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Detailed policies needed to define what is allowed
  - How is sensitive data transferred?
  - Is the data encrypted? How?
- DLP solutions can watch and alert on policy violations
  - Often requires multiple solutions in different places

Security policy
- Documentation of the organization's processes and procedures regarding IT security
  - Every organization has a different focus
- Almost everything in this module would be included
  - Remote access, building security, incident response, etc.
- This is not a static document
  - Change is constant

3.2 - Network Documentation

Floor plans
- Overlay the wired and wireless network with the existing architectural layout
  - Wires in the ceiling
  - Access point locations
- Can be useful for patch panel labels
  - Associate a desk with a number
- Used for planning
  - Avoid heavy machinery
  - Identify closet locations

Physical network maps
- Follows the physical wire and device
  - Can include physical rack locations

Distribution frames
- Passive cable termination
  - Punch down blocks
  - Patch panels
- Usually mounted on the wall or flat surface
  - Uses a bit of real-estate
- All transport media
  - Copper, fiber, voice and data
- Often used as a room or location name
  - It's a significant part of the network

Main Distribution Frame (MDF)
- Central point of the network
  - Usually in a data center
- Termination point for WAN links
  - Connects the inside to the outside
- Good test point
  - Test in both directions
- This is often the data center
  - The central point for data

3.2 - Network Documentation (continued)

Intermediate Distribution Frame (IDF)
- Extension of the MDF
  - A strategic distribution point
- Connects the users to the network
  - Uplinks from the MDF
  - Workgroup switches
  - Other local resources
- Common in medium to large organizations
  - Users are geographically diverse

Logical network maps
- Specialized software
  - Visio, OmniGraffle, Gliffy.com
- High level views
  - WAN layout, application flows
- Useful for planning and collaboration

Managing your cables
- ANSI/TIA/EIA 606
  - Administration Standard for the Telecommunications
  - Infrastructure of Commercial Buildings
- Presentation of information
  - Reports, drawings, work orders
- Pathway, space, grounding
  - Identifiers, Labeling
- Cables
  - Identifiers, labels, color coding, bar coding

Labeling
- Everything is tagged and labeled
  - A standard format
- Port labeling
  - CB01-01A-D088
  - CB01 - Main facility
  - 01A - Floor 1, space A
  - D088 - Data port 88
- All cables are documented
  - Central database

Site surveys
- Determine existing wireless landscape
  - Sample the existing wireless spectrum
- Identify existing access points
  - You may not control all of them
- Work around existing frequencies
  - Layout and plan for interference
- Plan for ongoing site surveys
  - Things will certainly change
- Heat maps
  - Identify wireless signal strengths

Audit and assessment report
- Validate existing security policies
  - Are we following our own rules?
- Internal audits
  - Self-imposed checks
  - Validate permissions, check access logs, verify user account status
- External audits
  - Third-party performs the checks
  - May be required for compliance regulations

Baselines
- Broadly defined
  - What does it mean to you?
  - Application response time, network throughput, etc.
- Point of reference
  - Accumulated knowledge
  - Examine the past to predict the future
  - Useful for planning

3.2 - High Availability

Fault tolerance
- Maintain uptime in the case of a failure
  - If a problem occurs, what happens?
  - Can degrade performance
- Fault tolerance adds complexity
  - The cost of managing the environment increases
- Single device fault tolerance
  - RAID, redundant power supplies, redundant NICs
- Multiple device fault tolerance
  - Server farms with load balancing
  - Multiple network paths

Redundancy and fault tolerance
- Redundant hardware components
  - Multiple devices, load balancing power supplies
- RAID
  - Redundant Array of Independent Disks
- Uninterruptible power supplies (UPS)
  - Prepare for the disconnections
- Clustering
  - A logical collective of servers
- Load balancing
  - Shared service load across components

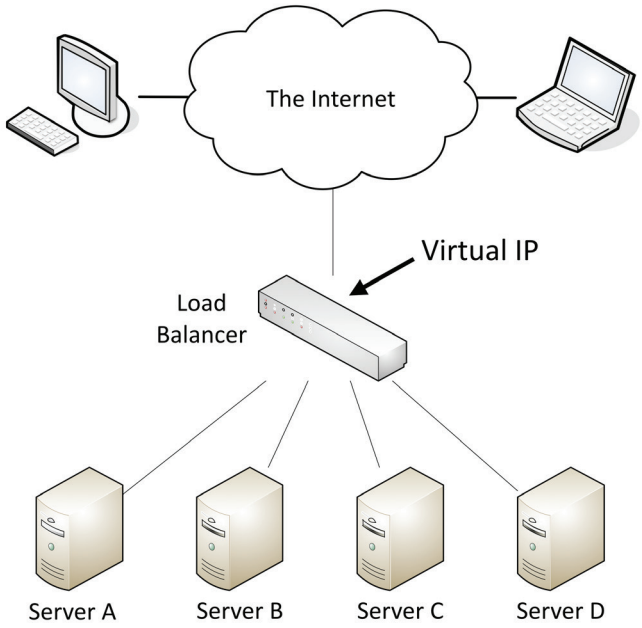
3.2 - High Availability (continued)

High availability
- Redundancy doesn't always mean always available
  - May need to be enabled manually
- HA (high availability)
  - Always on, always available
- May include many different components working together
  - Watch for single points of failure
- Higher availability almost always means higher costs
  - There's always another contingency you could add
  - Upgraded power, high-quality server components, etc.

Load balancing
- Some servers are active, others are on standby
  - If an active server fails, the passive server takes its place

NIC teaming
- Load Balancing / Fail Over (LBFO)
  - Aggregate bandwidth, redundant paths
  - Becomes more important in the virtual world
- Multiple network adapters
  - Looks like a single adapter
  - Integrate with switches
- NICs talk to each other
  - Usually multicast instead of broadcast
  - Fails over when a NIC doesn't respond

Load balancing



3.3 - Infrastructure Support

UPS
- Uninterruptible Power Supply
  - Short-term backup power
  - Blackouts, brownouts, surges
- UPS types
  - Standby UPS, line-interactive UPS, and on-line UPS
- Features
  - Auto shutdown, battery capacity, outlets, phone line suppression

Power distribution units (PDUs)
- Provide multiple power outlets
  - Usually in a rack
- Often include monitoring and control
  - Manage power capacity
  - Enable or disable individual outlets

Generators
- Long-term power backup
  - Fuel storage required
- Power an entire building
  - Some power outlets may be marked as generator-powered
- It may take a few minutes to get the generator up to speed
  - Use a battery UPS while the generator is starting

HVAC
- Heating, Ventilation, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- PC manages equipment
  - Makes cooling and heating decisions for workspaces and data centers
- A critical component
  - Keep the equipment and people comfortable

Fire suppression
- Data center fire safety
  - Large area, lots of electronics
  - Water isn't the best fire suppression option
- Common to use inert gases and chemical agents
  - Stored in tanks and dispersed during a fire
  - Many warning signs
- Integrated into HVAC system
  - Monitor for carbon monoxide
  - Enable/disable air handlers

3.3 - Recovery Sites

Site resiliency

- Recovery site is prepped
  - Data is synchronized
- A disaster is called
  - Business processes failover to the alternate processing site
- Problem is addressed
  - This can take hours, weeks, or longer
- Revert back to the primary location
  - The process must be documented for both directions

Cold site

- No hardware - empty building
- No data - bring it with you
- No people - bus in your team

Warm site

- Somewhere between cold and hot
  - Just enough to get going
- Big room with rack space
  - You bring the hardware
- Hardware is ready and waiting
  - You bring the software and data

Hot site

- An exact replica
  - Duplicate everything
- Stocked with hardware
  - Constantly updated
  - You buy two of everything
- Applications and software are constantly updated
  - Automated replication
- Flip a switch and everything moves
  - This may be quite a few switches

Cloud site

- Use an established cloud provider
  - Can provide enough resources for the recovery process
- No separate facility to manage
  - Online configuration
- Costs can be flat fee or based on use
  - More data, more cost
- The data and applications still need to be moved
  - Large data storage requirements may create a challenge

3.3 - Network Redundancy

Active-passive

- Two devices are installed and configured
  - Only one operates at a time
- If one device fails, the other takes over
  - Constant communication between the pair
- Configuration and real-time session information is constantly synchronized
  - The failover might occur at any time

Active-active

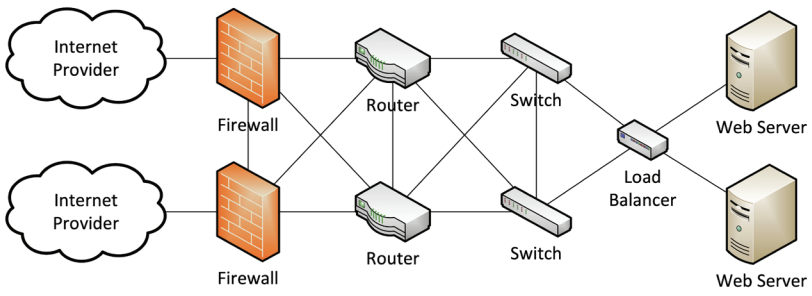
- You bought two devices
  - Use both at the same time
- More complex to design and operate
  - Data can flow in many different directions
  - A challenge to manage the flows
  - Monitoring and controlling data requires a very good understanding of the underlying infrastructure

Diverse paths

- Create multiple paths
  - More than one internet service provider (ISP)
- May require additional hardware and engineering
  - Advanced dynamic routing protocols
  - Failover processes
  - Local device configurations
- Great for redundancy - No reliance on a single provider

High availability protocols

- FHRP (First Hop Redundancy Protocol)
  - Your computer is configured with a single default gateway
  - We need a way to provide availability if the default gateway fails
- VRRP (Virtual Router Redundancy Protocol)
  - The default router isn't real
  - Devices use a virtual IP for the default gateway
  - If a router disappears, another one takes its place
  - Data continues to flow



3.3 - Availability Concepts

Recovery

- Recovery time objective (RTO)
  - Get up and running quickly
  - Get back to a particular service level
- Recovery point objective (RPO)
  - How much data loss is acceptable?
  - Bring the system back online; how far back does data go?
- Mean time to repair (MTTR)
  - Time required to fix the issue
- Mean time between failures (MTBF)
  - Predict the time between outages

Network device backup and restore

- Every device has a configuration
  - IP addresses, security settings, port configurations
  - Most devices allow the configuration to be downloaded and uploaded
  - Configurations may be specific to a version of operating code or firmware
- Revert to a previous state
  - Use backups to return to a previous configuration date and time
  - May require a firmware or version downgrade

4.1 - CIA Triad

The CIA Triad

- Combination of principles
  - The fundamentals of security
- Confidentiality
  - Prevent disclosure of information to unauthorized individuals or systems
- Integrity
  - Messages can't be modified without detection
- Availability
  - Systems and networks must be up and running

Confidentiality

- Certain information should only be known to certain people
- Encryption
  - Encode messages so only certain people can read it
- Access controls
  - Selectively restrict access to a resource
- Steganography
  - Conceal information within another piece of information
  - Commonly associated with hiding information in an image

Integrity

- Data is stored and transferred as intended
  - Any modification to the data would be identified
- Hashing
  - Map data of an arbitrary length to data of a fixed length
- Digital signatures
  - Mathematical scheme to verify the integrity of data
- Certificates
  - Combine with a digital signature to verify an individual
- Non-repudiation
  - Provides proof of integrity, can be asserted to be genuine

Availability

- Information is accessible to authorized users
  - Always at your fingertips
- Redundancy
  - Build services that will always be available
- Fault tolerance
  - System will continue to run, even when a failure occurs
- Patching
  - Stability
  - Close security holes

4.1 - Security Concepts

Vulnerabilities

- A weakness in a system
  - Allows the bad guys to gain access or cause a security breach
- Some vulnerabilities are never discovered
  - Or discovered after years of use
- Many different vulnerability types
  - Data injection
  - Broken authentication process
  - Sensitive data exposure
  - Security misconfiguration

Zero-day attacks

- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with the developer
- Attackers keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - https://cve.mitre.org/

4.1 - Security Concepts (continued)

Threat
- A vulnerability can be exploited by a threat
  - May be intentional (attacker) or accidental (fire, flood, etc.)
  - Many of these threats are external to the organization
- A resource can have a vulnerability
  - The vulnerability can be exploited by a threat agent
  - The threat agent takes a threat action to exploit the vulnerability
- The result is a loss of security
  - Data breach, system failure, data theft

Insider threats
- We give people tons of access
  - Least privilege, anyone?
- You have more access than others just by entering the building
  - Lock away your documents
  - Some organizations have very specific procedures
- Significant security issues
  - Harms reputation
  - Critical system disruption
  - Loss of confidential or proprietary information

Vulnerability databases
- Researchers find vulnerabilities
  - Everyone needs to know about them
- Common Vulnerabilities and Exposures (CVE)
  - A community managed list of vulnerabilities
  - Sponsored by the U.S. Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. National Vulnerability Database (NVD)
  - A summary of CVEs
  - Also sponsored by DHS and CISA - https://nvd.nist.gov/
- NVD provides additional details over the CVE list
  - Patch availability and severity scoring

Exploits
- Take advantage of a vulnerability
  - Gain control of a system, modify data, disable a service
- Many exploit methods
  - Built to take advantage of a vulnerability
  - May be complex

Least privilege
- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- All user accounts must be limited
  - Applications should run with minimal privileges
- Don't allow users to run with administrative privileges
  - Limits the scope of malicious behavior

Role-based access control (RBAC)
- You have a role in your organization
  - Manager, director, team lead, project manager
- Administrators provide access based on the role of the user
  - Rights are gained implicitly instead of explicitly
- In Windows, use Groups to provide role-based access control
  - You are in shipping and receiving, so you can use the shipping software
  - You are the manager, so you can review shipping logs

Zero trust
- Many networks are relatively open on the inside
  - Once you're through the firewall, there are few security controls
- Zero trust is a holistic approach to network security
  - Covers every device, every process, every person
- Everything must be verified
  - Nothing is trusted
  - Multifactor authentication, encryption, system permissions, additional firewalls, monitoring and analytics, etc.

4.1 - Defense in Depth

Layering the defense
- Physical controls
  - Keep people away from the technology
  - Door locks, fences, rack locks, cameras
- Technical controls
  - Hardware and software to keep things secure
  - Firewalls, active directory authentication, disk encryption
- Administrative controls
  - Policies and procedures
  - Onboarding and offboarding
  - Backup media handling

Defense in depth
- Firewall
- Screened subnet
- Hashing and salting passwords
- Authentication
- Intrusion prevention system
- VPN access
- Card/badge access
- Anti-virus and anti-malware software
- Security guard

4.1 - Defense in Depth (continued)

Physical segmentation
- Separate devices
  - Multiple units, separate infrastructure

Logical segmentation with VLANs
- Virtual Local Area Networks (VLANs)
  - Separated logically instead of physically
  - Cannot communicate between VLANs without a Layer 3 device / router

Screened subnet
- Previously known as the demilitarized zone (DMZ)
  - An additional layer of security between the Internet and you
  - Public access to public resources

Separation of duties
- Split knowledge
  - No one person has all of the details
  - Half of a safe combination
- Dual control
  - Two people must be present to perform the business function
  - Two keys open a safe (or launch a missile)

Network Access Control (NAC)
- IEEE 802.1X - Port-based Network Access Control (NAC)
  - You don't get access until you authenticate
- We're talking about physical interfaces
  - Not TCP or UDP ports
- Makes extensive use of EAP and RADIUS
  - Extensible Authentication Protocol / Remote Authentication Dial In User Service
- Administrative enable/disable
  - Disable your unused ports
- Duplicate MAC address checking
  - Stop the spoofers

Honeypots
- Attract the bad guys - And trap them there
- The "attacker" is probably a machine
  - Makes for interesting recon
- Honeypots - Create a virtual world to explore
- Many different options
  - Kippo, Google Hack Honeypot, Wordpot, etc.
- Constant battle to discern the real from the fake

4.1 - Authentication Methods

Local authentication
- Authentication credentials are stored on the local device
  - Must be individually administered
- Very manual process
  - A password change must be done manually on all devices
- Doesn't rely on a third-party authentication server
  - A network outage won't impact the login process

Multi-factor authentication
- More than one factor
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Can be expensive
  - Separate hardware tokens
  - Specialized scanning equipment
- Can be inexpensive - Free smartphone applications

RADIUS (Remote Authentication Dial-in User Service)
- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access, 802.1X network access
- RADIUS services available on almost any server operating system

TACACS
- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP (tcp/389 and udp/389)
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.
- Hierarchical structure - Builds a tree
- Container objects
  - Country, organization, organizational units
- Leaf objects
  - Users, computers, printers, files

4.1 - Authentication Methods (continued)

Kerberos
- Network authentication protocol
  - Authenticate once, trusted by the system
- No need to re-authenticate to everything
  - Mutual authentication - the client and the server
  - Protect against man-in-the-middle or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT) - RFC 4120
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

SSO with Kerberos
- Authenticate one time
  - Lots of backend ticketing, uses cryptographic tickets
- No constant username and password input! - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly
- There are many other SSO methods
  - Smart-cards, SAML, etc.

Which method to use?
- Many different ways to communicate to an authentication server
  - More than a simple login process
- Often determined by what is at hand
  - VPN concentrator can talk to a RADIUS server
  - We have a RADIUS server
- TACACS+ - Probably a Cisco device
- Kerberos or LDAP - Probably a Microsoft network

IEEE 802.1X
- IEEE 802.1X
  - Port-based Network Access Control (NAC)
  - You don't get access to the network until you authenticate
- EAP integrates with 802.1X
  - Extensible Authentication Protocol
  - 802.1X prevents access to the network until the authentication succeeds
- Used in conjunction with an access database
  - RADIUS, LDAP, TACACS+

EAP
- Extensible Authentication Protocol (EAP)
  - An authentication framework
- Many different ways to authenticate based on RFC standards
  - Manufacturers can build their own EAP methods
- EAP integrates with 802.1X
  - Prevents access to the network until the authentication succeeds

4.1 - Risk Management

Threat assessment
- Research the threats
  - And the threat actors
- Data is everywhere
  - Hacker group profiles, tools used by the attackers, and much more
- Make decisions based on this intelligence
  - Invest in the best prevention
- Used by researchers, security operations teams, and others

Vulnerability assessment
- Usually minimally invasive
  - Unlike a penetration test
- Run a vulnerability scanner
  - Poke around and see what's open
- Identify systems
  - And security devices
- Test from the outside and inside
  - Don't dismiss insider threats
- Gather as much information as possible
  - We'll separate wheat from chaff later

Vulnerability scan results
- Lack of security controls
  - No firewall
  - No anti-virus
  - No anti-spyware
- Misconfigurations
  - Open shares
  - Guest access
- Real vulnerabilities
  - Especially newer ones
  - Occasionally the old ones

Penetration testing
- Pentest - Simulate an attack
- Similar to vulnerability scanning
  - Except we actually try to exploit the vulnerabilities
- Often a compliance mandate
  - Regular penetration testing by a 3rd-party
- National Institute of Standards and Technology
- Technical Guide to Information Security
- Testing and Assessment
  - https://professormesser.link/800115 (PDF download)

4.1 - Risk Management (continued)

Posture assessment

- You can't trust everyone's computer
  - BYOD (Bring Your Own Device)
  - Malware infections / missing anti-malware
  - Unauthorized applications
- Before connecting to the network, perform a health check
  - Is it a trusted device?
  - Is it running anti-virus? Which one? Is it updated?
  - Are the corporate applications installed?
  - Is it a mobile device? Is the disk encrypted?
  - The type of device doesn't matter - Windows, Mac, Linux, iOS, Android

Failing your assessment

- What happens when a posture assessment fails?
  - Too dangerous to allow access
- Quarantine network, notify administrators
  - Just enough network access to fix the issue
- Once resolved, try again - May require additional fixes

Risk assessment

- Identify assets that could be affected by an attack
  - Define the risk associated with each asset
  - Hardware, customer data, intellectual property
- Identify threats - Loss of data, disruption of services, etc.
- Determine the risk - High, medium, or low risk
- Process assessment - Make future security plans

Vendors

- Every organization works with vendors
  - Payroll, customer relationship management, email marketing, travel, raw materials
- Important company data is often shared
  - May be required for cloud-based services
- Perform a risk assessment
  - Categorize risk by vendor and manage the risk
- Use contracts for clear understanding
  - Make sure everyone understands the expectations
  - Use the contract to enforce a secure environment

SIEM

- Security Information and Event Management
  - Logging of security events and information
- Security alerts
  - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation
  - Link diverse data types
- Forensic analysis
  - Gather details after an event

Getting the data

- Sensors and logs
  - Operating systems
  - Infrastructure devices
  - NetFlow sensors
- Sensitivity settings
  - Easy to be overwhelmed with data
  - Some information is unnecessary
  - Informational, Warning, Urgent

Viewing the data

- Trends
  - Identify changes over time
  - Easily view constant attack metrics
- Alerts
  - Identify a security event
  - View raw data
  - Visualize the log information
- Correlation
  - Combine and compare
  - View data in different ways

4.2 - Denial of Service

Denial of service

- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
- Doesn't have to be complicated
  - Turn off the power

A "friendly" DoS

- Unintentional DoSing
  - It's not always a ne'er-do-well
- Network DoS
  - Layer 2 loop without STP
- Bandwidth DoS
  - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks
  - Get a good shop vacuum

4.2 - Denial of Service (continued)

Bots

- Robots
  - That's you
- Once your machine is infected, it becomes a bot
  - You may not even know
- How does it get on your computer?
  - Trojan Horse
    (I just saw a funny video of you! Click here.)
  - You run a program or click an ad you THOUGHT was legit, but...
  - OS or application vulnerability
- A day in the life of a bot
  - Sit around.
  - Check in with the Command and Control (C&C) server.
  - Wait for instructions.

Botnets

- A group of bots working together
  - Nothing good can come from this
- Distributed Denial of service (DDoS)
  - The power of many
- Relay spam, proxy network traffic, distributed computing tasks
- Botnets are for sale
  - Rent time from the botnet owner
  - Not a long-term business proposition

Stopping the bot

- Prevent the initial infection
  - OS and application patches
  - Anti-virus/anti-malware and updated signatures
- Identify an existing infection
  - On-demand scans
  - Network monitoring
- Prevent command and control (C&C)
  - Block at the firewall
  - Identify at the workstation with a host-based firewall or host-based IPS

4.2 - On-path Attacks

On-path network attack

- How can an attacker watch without you knowing?
  - Formerly known as man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security
  - On-path attack on the local IP subnet

DNS poisoning

- Modify the DNS server
  - Requires some crafty hacking
- Modify the client host file
  - The host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires a redirection of the original request or the resulting response
  - Real-time redirection
  - This is an on-path attack

Other on-path attacks

- Get in the middle of the conversation and view or change information
  - Session hijacking
  - HTTPS spoofing
  - Wi-Fi eavesdropping
- Encryption fixes most of these situations
  - You can't change what you can't see

4.2 - VLAN Hopping

VLAN hopping

- Define different VLANs
- You only have access to your VLAN
  - Good security best practice
- "Hop" to another VLAN - this shouldn't happen
- Two primary methods
  - Switch spoofing and double tagging

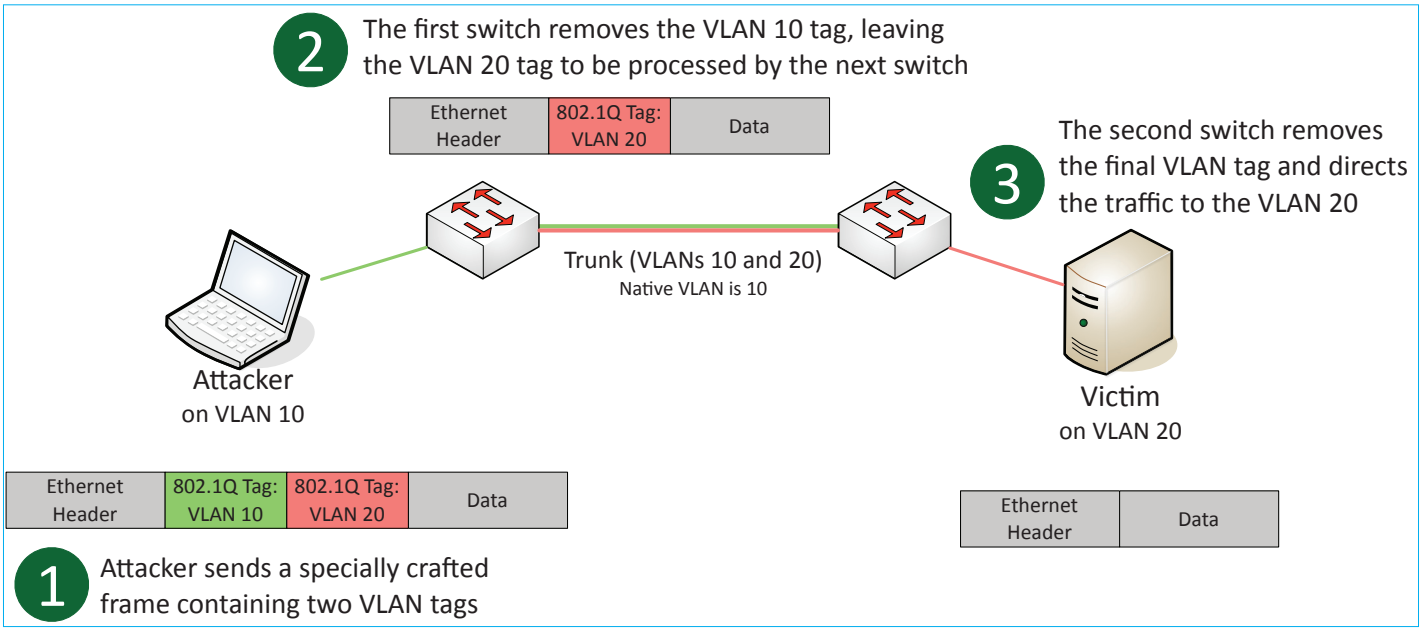
Switch spoofing

- Some switches support automatic configuration
  - Is the switch port for a device, or is it a trunk?
- There's no authentication required
  - Pretend to be a switch
  - Send trunk negotiation
- Now you've got a trunk link to a switch
  - Send and receive from any configured VLAN
- Switch administrators should disable trunk negotiation
  - Administratively configure trunk interfaces and device/access interfaces

4.2 - VLAN Hopping (continued)

Double tagging

- Craft a packet that includes two VLAN tags
  - Takes advantage of the "native" VLAN configuration
- The first native VLAN tag is removed by the first switch
  - The second "fake" tag is now visible to the second switch
  - Packet is forwarded to the target
- This is a one-way trip
  - Responses don't have a way back to the source host
- Don't put any devices on the native VLAN
  - Change the native VLAN ID
  - Force tagging of the native VLAN



4.2 - Spoofing

Spoofing

- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Caller ID spoofing
  - The incoming call information is completely fake
- On-path attacks
  - The person in the middle of the conversation pretends to be both endpoints

MAC spoofing

- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate
  - Circumvent MAC-based ACLs
  - Fake-out a wireless address filter
- Very difficult to detect
  - How do you know it's not the original device?

IP address spoofing

- Take someone else's IP address
  - Actual device
  - Pretend to be somewhere you are not
- Can be legitimate
  - Load balancing
  - Load testing
- May not be legitimate
  - ARP poisoning
  - DNS amplification / DDoS
- Easier to identify than MAC address spoofing
  - Apply rules to prevent invalid traffic, enable switch security

4.2 - Rogue Services

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

Rogue access points

- An unauthorized wireless access point
  - May be added by an employee or an attacker
  - Not necessarily malicious
  - A significant potential backdoor
- Very easy to plug in a wireless AP
  - Or enable wireless sharing in your OS
- Schedule a periodic survey
  - Walk around your building/campus
  - Use third-party tools / WiFi Pineapple
- Consider using 802.1X (Network Access Control)
  - You must authenticate, regardless of the connection type

Wireless evil twins

- Looks legitimate, but actually malicious
  - The wireless version of phishing
- Configure an access point to look like an existing network
  - Same (or similar) SSID and security settings/captive portal
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots (and users) are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPNPublic access to public resources

4.2 - Malware and Ransomware

Malware

- Malicious software
  - These can be very bad
- Gather information
  - Keystrokes
- Participate in a group
  - Controlled over the 'net
- Show you advertising
  - Big money
- Viruses and worms
  - Encrypt your data
  - Ruin your day

Malware Types and Methods

- Viruses
- Crypto-malware
- Ransomware
- Worms
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Botnet

How you get malware

- These all work together
  - A worm takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is vulnerable
  - Operating system - Keep your OS updated!
  - Applications - Check with the publisher

Ransomware

- A particularly nasty malware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

4.2 - Password Attacks

Plaintext / unencrypted passwords

- Some applications store passwords "in the clear"
  - No encryption. You can read the stored password.
  - This is rare, thankfully
- Do not store passwords as plaintext
  - Anyone with access to the password file or database has every credential
- What to do if your application saves passwords as plaintext:
  - Get a better application

Hashing a password

- Hashes represent data as a fixed-length string of text
  - A message digest, or "fingerprint"
- Will not have a collision (hopefully)
  - Different inputs will not have the same hash
- One-way trip
  - Impossible to recover the original message from the digest
  - A common way to store passwords

The password file

- Different across operating systems and applications
  - Different hash algorithms

Linux Account Hashes

```
Jumper Bay:1001::42e2f19c31c9ff73cb97eb1b26c10f54:::
Carter:1007::cf4eb977a6859c76efd21f5094ecf77d:::
Jackson:1008::e1f757d9cdc06690509e04b5446317d2:::
O'Neill:1009::78a8c423faedd2f002c6aef69a0ac1af:::
Teal'c:1010::bf84666c81974686e50d300bc36aea01:::
```

Brute force

- Try every possible password combination until the hash is matched
- This might take some time
  - A strong hashing algorithm slows things down
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

Dictionary attacks

- Use a dictionary to find common words
  - Passwords are created by humans
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- The password crackers can substitute letters
  - p&ssw0rd
- This takes time
  - Distributed cracking and GPU cracking is common
- Discover passwords for common words
  - This won't discover random character passwords

4.2 - Deauthentication

It started as a normal day

- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless disassociation
  - A significant wireless denial of service (DoS) attack

802.11 management frames

- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/disassociate with an access point, etc.
- Original wireless standards did not add protection for management frames
  - Sent in the clear
  - No authentication or validation

Protecting against disassociation

- IEEE has already addressed the problem
  - 802.11w - July 2014
- Some of the important management frames are encrypted
  - Disassociate, deauthenticate, channel switch announcements, etc.
- Not everything is encrypted
  - Beacons, probes, authentication, association
- 802.11w is required for 802.11ac compliance
  - This will roll out going forward

4.2 - Social Engineering

Phishing
- Social engineering with a touch of spoofing
  - Often delivered by email, text, etc.
  - Very remarkable when well done
- Don't be fooled
  - Check the URL, and don't click links in email or text
- Usually there's something not quite right
  - Spelling, fonts, graphics

Tricks and misdirection
- How are they so successful?
  - Digital slight of hand - it fools the best of us
- Typosquatting
  - A type of URL hijacking - https://professormessor.com
  - Prepending: https://pprofessormesser.com
- Pretexting
  - Lying to get information
  - Attacker is a character in a situation they create
  - Hi, we're calling from Visa regarding an automated payment to your utility service…

Tailgating and piggybacking
- Tailgating uses an authorized person to gain unauthorized access to a building
  - The attacker does not have consent
  - Sneaks through when nobody is looking
- Piggybacking follows the same process, but the authorized person is giving consent
  - Hold the door, my hands are full of donut boxes
  - Sometimes you shouldn't be polite
- Once inside, there's little to stop you
  - Most security stops at the border

Watching for tailgating
- Policy for visitors
  - You should be able to identify anyone
- One scan, one person
  - A matter of policy or mechanically required
- Access Control Vestibule / Airlock
  - You don't have a choice
- Don't be afraid to ask
  - Who are you and why are you here?

Shoulder surfing
- You have access to important information
  - Many people want to see
  - Curiosity, industrial espionage, competitive advantage
- This is surprisingly easy
  - Airports / Flights
  - Hallway-facing monitors
  - Coffee shops
- Surf from afar
  - Binoculars / Telescopes
  - Easy in the big city
  - Webcam monitoring

Preventing shoulder surfing
- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

4.3 - Network Hardening

Secure SNMP
- Simple Network Management Protocol
  - Monitor and control servers, switches, routers, firewalls, and other devices
- Different versions through the years
  - SNMPv1 and SNMPv2 do not encrypt network traffic
- SNMPv3
  - Version 3 added encrypted communication
  - Not all devices support SNMPv3
  - Use it everywhere you can

Router Advertisement (RA) guard
- IPv6 includes periodic router announcements
  - Automatic configuration for network devices
- A rogue device could pretend to be a router
  - Could be part of an on-path attack, denial of service, etc.
- Switches can validate the RA messages
  - Administrators define policies to check the RA messages

Port security
- Prevent unauthorized users from connecting to a switch interface
  - Alert or disable the port
- Based on the source MAC address
  - Even if forwarded from elsewhere
- Each port has its own config
  - Unique rules for every interface

Port security operation
- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Default is to disable the interface

4.3 - Network Hardening (continued)

DHCP snooping
- IP tracking on a layer 2 device (switch)
  - The switch is a DHCP firewall
  - Trusted: Routers, switches, DHCP servers
  - Untrusted: Other computers, unofficial DHCP servers
- Switch watches for DHCP conversations
  - Adds a list of untrusted devices to a table
- Filters invalid IP and DHCP information
  - Static IP addresses
  - Devices acting as DHCP servers
- Other invalid traffic patterns

Dynamic ARP inspection (DAI)
- ARP is powerful
  - And has no built-in security
- Prevent those nasty on-path attacks
  - Stops ARP poisoning at the switch level
- Relies on DHCP snooping for intel
  - Knowing every device's IP can be valuable information
- Intercept all ARP requests and responses
  - Invalid IP-to-MAC address bindings are dropped
  - Only valid requests make it through

Control plane policing
- Control plane manages the device
  - Data plane performs the operational processes
- Protect against DoS or reconnaissance
  - Defines a QoS filter to protect the control plane
  - Control packets should have the priority
- Manage traffic
  - Prioritize management traffic
  - Block unnecessary control plane traffic types (i.e., non-SSH)
  - Rate limit the control plane traffic flows

Private VLANs
- Port isolation
  - Restrict access between interfaces
  - Even when they're in the same VLAN
- You might already be using private VLANs
  - Your home Internet can't directly connect to another home
  - Hotel room access is limited to Internet connectivity

Disabling unused interfaces
- Enabled physical ports
  - Conference rooms
  - Break rooms
- Administratively disable unused ports
  - More to maintain, but more secure
- Network Access Control (NAC)
  - 802.1X controls
  - You can't communicate unless you are authenticated

Disable unnecessary ports and services
- Every open port is a possible entry point
  - Close everything except required ports
- Control access with a firewall
  - NGFW would be ideal
- Unused or unknown services
  - Installed with the OS or from other applications
- Applications with broad port ranges
  - Open port 0 through 65,535
- Use Nmap or similar port scanner to verify
  - Ongoing monitoring is important

Changing default credentials
- Most devices have default usernames and passwords
  - Change yours!
- The right credentials provide full control
  - Administrator access
- Very easy to find the defaults for your AP or router
  - http://www.routerpasswords.com

Password complexity and length
- Make your password strong
  - Resist guessing or brute-force attack
- Increase password entropy
  - No single words, no obvious passwords
  - What's the name of your dog?
  - Mix upper and lower case and use special characters
  - Don't replace a o with a 0, t with a 7
- Stronger passwords are at least 8 characters
  - Consider a phrase or set of words
  -

Change default VLAN
- All access ports (non-trunk ports) are assigned to a VLAN
  - Without any additional security (i.e., 802.1X), anyone connecting will be part of the default VLAN
- The default VLAN might also be used by default for control plane access/management
  - Don't put users on the management VLAN
  - Change the management VLAN to something exclusive
- Assign unused interfaces to a specific non-routable, non-forwarding VLAN
  - A "dead-end" or "impasse" VLAN

Upgrading firmware
- Many network devices do not use a traditional operating system
  - All updates are made to firmware
- The potential exists for security vulnerabilities
  - Upgrade the firmware to a non-vulnerable version
- Plan for the unexpected
  - Always have a rollback plan
  - Save those firmware binaries

4.3 - Network Hardening (continued)

Patch management
- Incredibly important
  - System stability
  - Security fixes
- Service packs
  - All at once
- Monthly updates
  - Incremental (and important)
- Emergency out-of-band updates
  - Zero-day and important security discoveries

Role-based access
- Not everyone connecting to a switch or router needs the same level of access
  - Administrators, help desk, management, API access
- Many devices allow the configuration of specific roles
  - Rights and permissions are based on the role
  - Administrators can configure and reboot the device
  - Help desk can view statistics
  - API access can't interactively login/SSH

Access control lists (ACLs)
- Allow or disallow traffic based on tuples
  - Groupings of categories
  - Source IP, Destination IP, port number, time of day, application, etc.
- Restrict access to network devices
  - Limit by IP address or other identifier
  - Prevent regular user / non-admin access
- Be careful when configuring these
  - You can accidentally lock yourself out

Firewall rules
- Manage access from the firewall
  - Additional security options - Username, VPN, MFA
- Most firewall rules include an implicit deny
  - If there's no explicit rule, then traffic is blocked
  - These implicit deny rules aren't usually logged
- Some firewall administrators will add explicit deny rules
  - Anything denied by a rule is logged by default
  - Can be useful for identifying reconnaissance or access attempts

4.3 - Wireless Security

MAC filtering
- Media Access Control -
  - The "hardware" address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity
  - If you know the method, you can easily defeat it

Antenna placement
- Focus coverage to the necessary work areas
  - Limit access from outside the building
- Adjust power levels
  - Control coverage based on signal strength
- May require some additional site surveys
  - Walk around and optimize the coverage

Wireless isolation
- Wireless client isolation
  - Wireless devices on an access point can't communicate with each other
  - Useful in a hotel or public area
  - May not be useful at work with peer-to-peer applications
- Guest network isolation
  - The guest network does not have access to the internal private network
  - This is almost always the right configuration

Wireless security modes
- Configure the authentication on your access point / wireless router
- Open System - No authentication password is required
- WPA2/3-Personal / WPA-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA2/3-Enterprise / WPA2/3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS, LDAP)

EAP
- EAP (Extensible Authentication Protocol)
  - An authentication framework
- Many different ways to authenticate based on RFC standards
  - WPA2 and WPA3 use five EAP types as authentication mechanisms
- Some version of EAP is used when authenticating to the network
  - Common to integrate on wireless networks using 802.1X

Geofencing
- Some MDMs allow for geofencing
  - Restrict or allow features when the device is in a particular area
- Cameras
  - The camera might only work when outside the office
- Authentication
  - Only allow logins when the device is located in a particular area

4.3 - Wireless Security (continued)

Captive portal

- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
- Username / password
  - And additional authentication factors
- Once proper authentication is provided, the web session continues
  - Until the captive portal removes your access

IoT security

- Internet of Things devices
  - Smart devices, appliances, garage doors, door locks, lights, etc.
- Security is probably not the primary focus
  - In some cases, it's not a consideration at all
- IoT devices should be segmented from the private network
  - Keep your personal devices and storage systems away from IoT devices
  - If an IoT device is breached, your personal data is not accessible
- Use a separate VLAN
  - Many home access points provide a "guest" network
  - This is different than the DMZ or screened-subnet

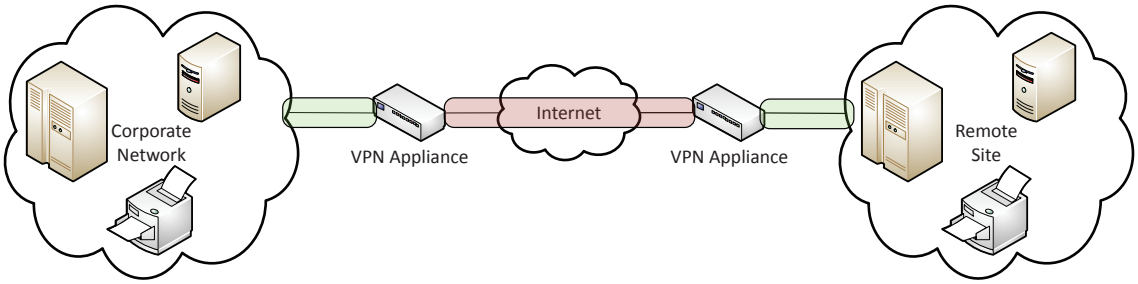
4.4 - Remote Access

VPNs

- Virtual Private Networks
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

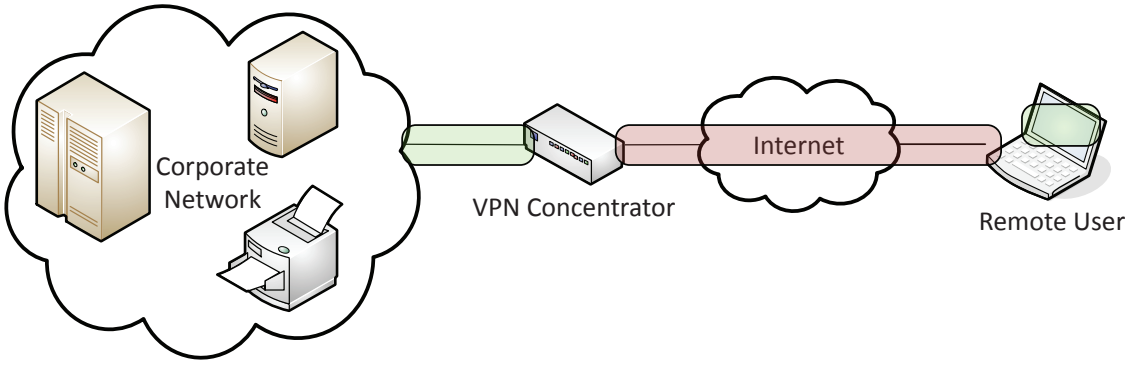
Site-to-Site VPNs

- Encrypt traffic between sites
  - Through the public Internet
- Use existing Internet connection
  - No additional circuits or costs



Host-to-Site VPNs

- Also called "remote access VPN"
- Requires software on the user device
  - May be built-in to existing operating system



Clientless VPNs

- Hypertext Markup Language version 5
  - The language commonly used in web browsers
- Includes comprehensive API support
  - Application Programming Interface
  - Web cryptography API
- Create a VPN tunnel without a separate VPN application
  - Nothing to install
- Use an HTML5 compliant browser
  - Communicate directly to the VPN concentrator

4.4 - Remote Access (continued)

Remote desktop connection

- Share a desktop from a remote location
  - It's like you're right there
- RDP (Microsoft Remote Desktop Protocol)
  - Clients for Mac OS, Linux, and others as well
- VNC (Virtual Network Computing)
  - Remote Frame Buffer (RFB) protocol
  - Clients for many operating systems
  - Many are open source
- Commonly used for technical support
  - And for scammers

Remote desktop gateway

- Combine a VPN with Microsoft Remote Desktop
  - Securely access RDP servers from the outside
- Client connects to the Remote Desktop Gateway
  - Secure SSL tunnel
  - Many authentication options
- Remote Desktop Gateway connects internally to RDP servers over tcp/3389
  - No special configurations required
  - Gateway is the proxy between the
  - SSL tunnel and the Remote Desktop protocol

SSH (Secure Shell)

- Encrypted console communication - tcp/22
- Looks and acts the same as Telnet - tcp/23

Cloud-hosted virtual desktops

- A virtual desktop infrastructure (VDI) in the cloud
  - Users connect to a pre-built desktop
- Access from almost any OS
  - Windows, Mac OS, Linux, iOS, Chromebook, web browser
- Virtual NIC
  - All communication in the desktop are local to the virtual desktop
  - No sensitive information sent from the local device

Authentication and authorization

- 2008 until May 2011 - Subway Sandwiches
  - 200 locations were breached
  - Point of sale systems were equipped with remote desktop software
  - 80,000 credit cards, millions of dollars of unauthorized purchases
- Significant security issues
  - Default credentials and brute force attacks
  - Remote access requires MORE security, not less
- Once connected, authorization is key
  - Access rights should be limited

Out-of-band management

- The network isn't available
  - Or the device isn't accessible from the network
- Most devices have a separate management interface
  - Usually a serial connection / USB
- Connect a modem
  - Dial-in to manage the device
- Console router / comm server
  - Out-of-band access for multiple devices
  - Connect to the console router, then choose where you want to go

4.5 - Physical Security

Video surveillance

- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera properties are important
  - Focal length - Shorter is wider angle
  - Depth of field - How much is in focus
  - Illumination requirements - See in the dark
- Often many different cameras
  - Networked together and recorded over time
- Motion detection
  - Radio reflection or passive infrared
  - Useful in areas not often in use

Asset tracking tags

- A record of every asset
  - Routers, switches, cables, fiber modules, CSU/DSUs, etc.
- Financial records, audits, depreciation
  - Make/model, configuration, purchase date, location, etc.
- Tag the asset
  - Barcode, RFID, visible tracking number

Tamper detection

- You can't watch all of your equipment all of the time
  - Have your systems monitor themselves
- Hardware tampering
  - Case sensors, identify case removal
  - Alarm sent from BIOS
  - Firewalls, routers, etc.
- Foil asset tags
  - Tamper notification

4.5 - Physical Security (continued)

Employee training
- One on one - Personal training
- Posters and signs - High visibility
- Login message - These become invisible
- Intranet page - Always available
- Ongoing updates - Keep everyone on their toes

Access control hardware
- Security hardware
  - Purpose-built technology
- Gates, locks, cameras, etc.
  - Specialized hardware to handle specific security requirements
- Often networked
  - Real-time monitoring and control
  - Required for cameras and sensors

Badge readers
- Electronic - Keyless, PIN
- No keys to lose - No locks to re-key
- Centrally managed - Immediate control

Biometrics
- Biometric authentication
  - Fingerprint, iris, voiceprint
- Usually stores a mathematical representation of your biometrics
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations - Not foolproof

Access control vestibules
- All doors normally unlocked
  - Opening one door causes others to lock
- All doors normally locked
  - Unlocking one door prevents others from being unlocked
- One door open / other locked
  - When one is open, the other cannot be unlocked
- One at a time, controlled groups
  - Managed control through an area

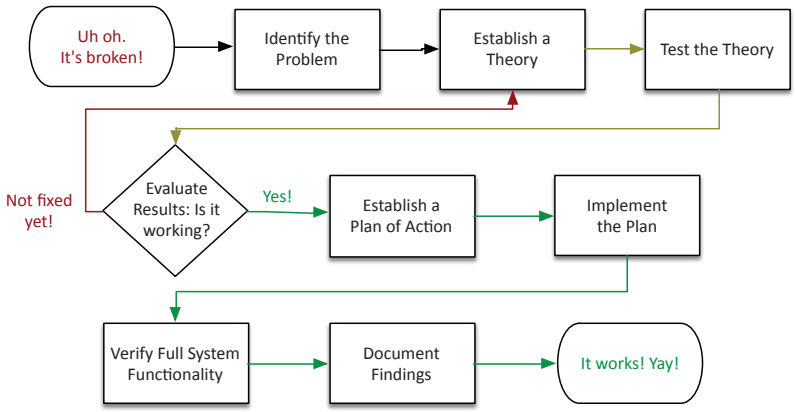
Locking cabinets
- Data center hardware is usually managed by different groups
  - Responsibility lies with the owner
- Racks can be installed together - Side-to-sides
- Enclosed cabinets with locks
  - Ventilation on front, back, top, and bottom

Smart lockers
- Safe and automated delivery and pickup
  - Save time and prevent theft
- Packages are delivered to a smart locker
  - Recipient is sent an email/text with instructions
  - Use a PIN or mobile app to unlock
- Fast, convenient, and secure
  - No missing packages, easy to track, and stress-free

Data destruction and media sanitization
- Disposal becomes a legal issue
  - Some information must not be destroyed
  - Consider offsite storage
- You don't want critical information in the trash
  - People really do dumpster dive
  - Recycling can be a security concern
  - Physically destroy the media
- Reuse the storage media
  - Sanitize the media for reuse
  - Ensure nothing is left behind

Sanitizing media
- Factory reset
  - Delete data and return configuration to the default
  - The next user gets a fresh configuration
- Wipe data
  - Unrecoverable removal of data on a storage device
  - Usually overwrites the data storage locations
  - Useful when you need to reuse or continue using the media

5.1 - 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

5.2 - Cable Connectivity

Using the right cable
- Speed/bandwidth
  - Theoretical maximum data rate
  - Usually measured in bits per second
  - The size of the pipe
- Throughput
  - Amount of data transferred in a given timeframe
  - Usually measured in bits per second
  - How much water is flowing through the pipe
- Distance
  - Know the maximum distance
  - Varies based on copper, fiber, repeaters, etc.

Unshielded and shielded cable
- Abbreviations
  - U = Unshielded, S = Braided shielding, F = Foil shielding
- (Overall cable) / (individual pairs)TP
  - Braided shielding around the entire cable and foil around the pairs is S/FTP
  - Foil around the cable and no shielding around the pairs is F/UTP

Plenum
- Plenum space
  - Building air circulation
  - Heating and air conditioning system
- Concerns in the case of a fire
  - Smoke and toxic fumes
- Worst-case planning
  - Important concerns for any structure

Plenum-rated cable
- Traditional cable jacket
  - Polyvinyl chloride (PVC)
- Fire-rated cable jacket
  - Fluorinated ethylene polymer (FEP) or low-smoke polyvinyl chloride (PVC)
- Plenum-rated cable may not be as flexible
  - May not have the same bend radius

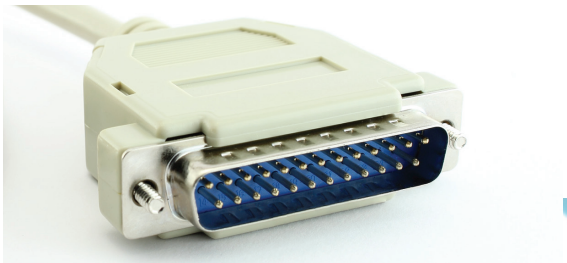
Serial console cables
- D-subminiature or D-sub
  - The letter refers to the connector size
- Commonly used for RS-232
  - Recommended Standard 232
  - An industry standard since 1969
- Serial communications standard
  - Built for modem communication
  - Used for modems, printers, mice, networking
- Now used as a configuration port

"Rollover" cable
- Rolled cable, Cisco console cable,
  - Yost cable
  - Serial cable "standard" proposed by Dave Yost
- A standard for RJ-45 to serial communications
- Used in conjunction with serial port connectors

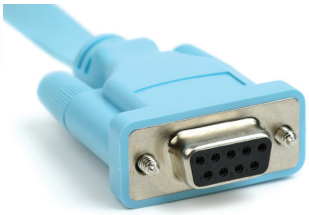
Ethernet cross-over cables
- Connect to Ethernet devices without using a switch
  - Use your crossover cable
- Can be a good alternative to a console connection
  - You may not always have the right serial cable or connector
- Always carry a crossover cable
  - Or an adapter with the crossover

Power over Ethernet (PoE)
- Power provided on an Ethernet cable
  - One wire for both network and electricity
  - Phones, cameras, wireless access points
  - Useful in difficult-to-power areas
- Power provided at the switch
  - Built-in power - Endspans
  - In-line power injector - Midspans
- Power modes
  - Mode A - Common-mode data pair power
  - Mode B - Power on the spare pair
  - 4-pair - Power on all four data pair

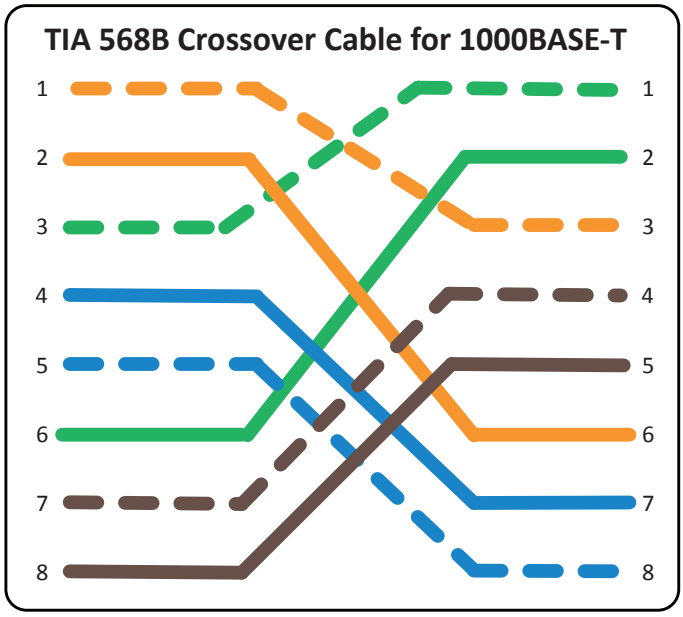
PoE, PoE+, PoE++
- PoE: IEEE 802.3af-2003
  - The original PoE specification
  - Now part of the 802.3 standard
  - 15.4 watts DC power, 350 mA max current
- PoE+: IEEE 802.3at-2009
  - Now also part of the 802.3 standard
  - 25.5 watts DC power, 600 mA max current
- PoE++: IEEE 802.3bt-2018
  - 51 W (Type 3), 600 mA max current
  - 71.3 W (Type 4), 960 mA max current
  - PoE with 10GBASE-T

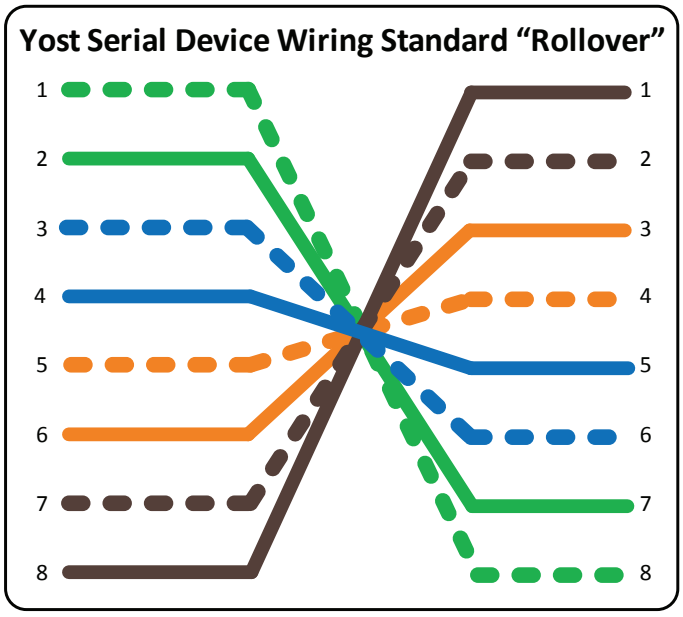


DB-25 connector



DB-9 connector





5.2 - Wired Network Troubleshooting

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

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

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

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

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

Incorrect pin-out
- Near and far pins in cables aren't where they are supposed to be
  - Pin 1 goes to pin 1, pin 2 to pin 2, etc.
- Performance or connectivity issues
  - May drop from 1 gbit/sec to 100 mbit/sec
  - May not connect at all

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

5.2 - Wired Network Troubleshooting (continued)

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

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
  - Increase in late collisions

Duplex/speed mismatch
- Speed and duplex
  - Speed: 10 / 100 /1,000 / Auto
  - Duplex: Half / Full / Auto
- Incorrect speed
  - Many switch configurations will auto-negotiate speed
  - Less than expected throughput
- Incorrect duplex
  - Again, the switch may auto-negotiate
  - Needs to match on both sides
  - A mismatch will cause significant slowdowns
  - Increase in Late Collisions may indicate a duplex mismatch

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

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

Incorrect transceivers
- 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

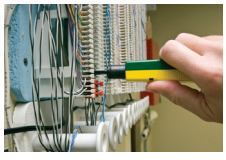
Reversing transmit and receive
- Wiring mistake
  - Cable ends
  - Punchdowns
- Easy to find with a wire map
  - 1-3, 2-6, 3-1, 6-2
  - Simple to identify
- Some network interfaces will automatically correct (Auto-MDIX)

TX/RX reversal troubleshooting
- No connectivity
  - Auto-MDIX might connect
  - Try turning it on
- Locate reversal location
  - Often at a punchdown
  - Check your patch panel

Dirty optical cables
- Light needs to be seen
  - Fiber connectors must be clean
  - Always use your dust caps
- Dirty connectors will inhibit or prevent communication
  - Attenuation can prevent data transfer
- Clean thoroughly before using
  - Just before installation

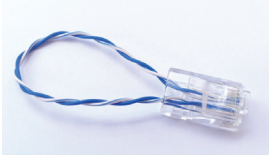
5.2 - Hardware Tools

Cable crimper
- "Pinch" the connector onto the wire
- The final step of a cable installation
- Metal prongs push through insulation



Punch-down Tool
- Forces wire into a wiring block
- Trims the wires and breaks the insulation

Tone generator
- Puts an analog sound on the wire
- Inductive probe doesn't need to touch the copper



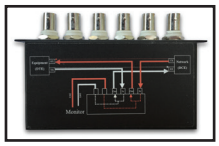
Loopback plug
- Useful for testing physical ports
- Serial, Ethernet, T1, fiber
- These are not crossover cables

5.2 - Hardware Tools (continued)

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

Multimeter
- AC/DC voltages
- Continuity, wire mapping

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



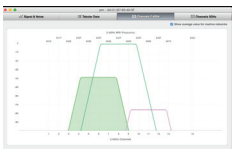
Taps and port mirrors
- Intercept network traffic
- Physical active or passive taps
- Port mirror from a switch

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

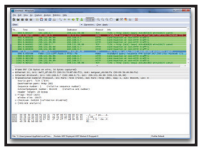
Spectrum analyzer
- View the frequency spectrum
- Identify frequency conflicts

Fusion splicer
- Join two fiber ends together
- Add connectors
- Repair fiber using heat

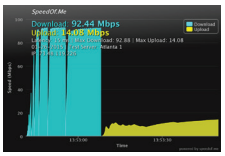
5.3 - Software Tools



Wireless packet analysis
- View wireless information
- Signal-to-noise ratio, channel information, etc.

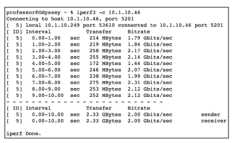


Protocol analyzer
- Capture and display network traffic
- Use a physical tap or redirect on the switch



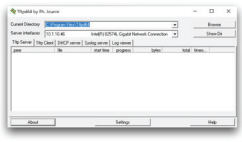
Speed test sites
- Bandwidth testing
- Pre- and post-change analysis
- Not all sites are the same

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



iPerf
- Performance monitoring
- Speed testing
- Run tests across different OSes

NetFlow
- Gather traffic statistics
- Standard collection method
- Probes and collectors



TFTP server
- Trivial File Transfer Protocol
- File transfers, firmware upgrades
- Your device is the TFTP server

Terminal emulator
- SSH (Secure Shell)
- Encrypted communication
- Support across many OSes

5.3 - 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

ipconfig, ifconfig, ip - 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
- `ip address` - The latest Linux utility

nslookup and dig - Lookup information from DNS servers

- `nslookup <ip address>`
- `dig <ip address>`

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>`

arp - Address resolution protocol information

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

netstat - Display network statistics

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

hostname

- View the FQDN and IP address of the device
- Windows, Linux, macOS, and others
- `hostname`

route

- View the device's routing table
  - Find out which way the packets will go
- Windows: `route print`
- Linux and macOS: `netstat -r`

Telnet

- Login to devices remotely
- In-the-clear communication
- Useful for checking a port or application
- `telnet <ip address> <port number>`

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

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
- Additional scripts
  - Nmap Scripting Engine (NSE)

Basic platform commands

- `show interface`
  - View the interfaces on a device
  - View detailed interface information
- `show config`
  - View the device configuration
- `show route`
  - View the routing table

5.4 - Wireless Troubleshooting

Wireless performance

- Performance can vary
  - The wireless spectrum is unforgiving
  - Many more variables in play
- Throughput
  - The amount of data successfully transferred through the wireless network
- Speed
  - The maximum bandwidth available
  - Is generally faster as you get closer to the antennas
- Distance
  - The user needs to be relatively close to the access points

Wireless signals

- RSSI (Received signal strength indication)
  - The strength of a received radio signal
- Measured in decibel-milliwatts (dBm)
  - The number of decibels (dB) with reference to one milliwatt (mW)
- Shown as a negative number on a log scale
  - Closer to zero is better
  - -50 dBm is excellent
  - -70 dBm is good
  - -80 dBm and smaller is low

5.4 - Wireless Troubleshooting (continued)

Wireless survey tools
- Signal coverage
- Potential interference
- Built-in tools
- 3rd-party tools
- Spectrum analyzer

Wireless signals
- EIRP (Effective isotropic radiated power)
  - The radiated signal strength
  - Transmit strength + antenna gain - cable loss
- In the United States, transmission power is regulated by the FCC (Federal Communications Commission)
  - For 2.4 GHz, maximum EIRP is +36 dBm or 4W
  - Varies based on connections and frequencies used
- Sometimes configurable on the access point
  - Equipment owner is responsible for managing EIRP

Omnidirectional antennas
- One of the most common
  - Included on most access points
- Signal is evenly distributed on all sides
  - Place the antennas in the middle
- Good choice for most environments
  - You need coverage in all directions
- No ability to focus the signal
  - A different antenna will be required

Directional antennas
- Focus the signal
  - Increased distances
- Send and receive in a single direction
  - Focused transmission and listening
- Antenna performance is measured in dB
  - Double power every 3dB of gain
- Yagi antenna
  - Very directional and high gain
- Parabolic antenna
  - Focus the signal to a single point
- Often used to bridge a gap
  - Point to point
  - Antennas are placed at both ends

Antenna configuration
- Polarization
  - The orientation of an antenna
  - Relative to the surface of the Earth
- Transmitting and receiving polarization should be the same
  - If polarization is offset, only part of the signal will be received

AP association time
- Devices must associate with an access point
  - This can occur multiple times as a device roams
- Signal strength
  - Association is delayed or blocked due to low signal
- Wired network controller issue
  - Latency and firmware issues can affect association time
- Track association metrics
  - Gather from the management console or via SNMP

Channel utilization
- There's a limited amount of frequency
  - Everyone can't talk at one time
  - Similar to a wired network
- An increasing number of wireless devices
  - They all want to talk
- Most access points can monitor utilization
  - A percentage of available air-time
  - When you hit 100%, you've used up all of your available wireless space

Managing channel utilization
- Disable legacy, low speed support
  - Use the fastest possible speeds and configurations
- Check your channels
  - Avoid overlap between access points
- Adjust the output power
  - Avoid conflicts with other access points
  - Interference can steal valuable network time
- Split the network
  - You might need additional frequencies and access points

Site surveys
- Determine existing wireless landscape
  - Sample the existing wireless spectrum
- Identify existing access points
  - You may not control all of them
- Work around existing frequencies
  - Layout and plan for interference
- Plan for ongoing site surveys
  - Things will certainly change
- Heat maps - Identify wireless signal strengths

5.4 - Common Wireless Issues

Overlapping channels
- Avoid interference from other access points
  - Use a wireless analyzer

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
- Some power is lost in the antenna cable coax
  - Most applicable at higher frequencies
  - Also check for damaged cables, especially outside

Wrong SSID
- Every access point has at least one
  - Service Set Identifier (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
- Confirm the correct SSID settings
  - Should be listed in the current connection status

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

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 WPA2/3
- 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 WPA2/3

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

Captive portal
- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
  - Use a username/password to authenticate
- Authentication timeout
  - May require re-authentication after an interval
- Portal is probably authenticating to an external database
  - Check the back-end RADIUS/LDAP/TACACS process

Client disassociation
- A denial of service attack
  - Takes advantage of older 802.11 management frame transmission
- Device keeps dropping from the wireless network
  - Or never connects
- Frames can be clearly seen in a packet capture
  - Grab the 802.11 frame information with Wireshark
- Remove the device performing the disassociation
  - Or upgrade to a new 802.11 standard

5.5 - General Network Troubleshooting

Device configuration review
- Don't start blindly troubleshooting
  - Know what you're getting into
- View the configuration
  - Native desktop or web-based console
  - SSH/terminal console
- Try getting the configuration ahead of time - Prepare early

Routing tables
- The digital version of asking for directions
  - Know how to get from point A to point B
- This can answer a lot of questions
  - Default gateway, manually configured static routes
- Know which way data will flow
  - A network map might help
- Refer to every router
  - Routing loops and missing routes are common

Interface status
- Know the details of the important interfaces
  - Easy to view on the console
  - You'll rarely be physically next to the device
- Check the easy stuff first
  - Verify the physical connectivity
  - Nothing works properly if the interface is misconfigured
- You will often solve the problem here
  - Check for errors and mismatches
  - It's a quick and easy fix

5.5 - General Network Troubleshooting (continued)

VLAN assignment

- Network link is active and
  - IP address is assigned
  - No access to resources or limited functionality
- Every switch interface is configured as an access port or a trunk port
  - Each access port is assigned to a VLAN
- Confirm the specific switch interface
  - Check the VLAN assignment
- This is also a common issue
  - Another quick fix

Network performance baseline

- Troubleshooting starts with a blank slate
  - A baseline can add context
- Intermittent or all-day issues
  - Check utilization, individual device performance, etc.
- Some organizations already collect this data
  - Check the SIEM or management console
- Look for patterns and correlation
  - The baseline might also tell you what's NOT happening

5.5 - Common Network Issues

Half-duplex Ethernet

- If two devices communicate simultaneously, you have a collision

Collisions

- On a half-duplex link, collisions are normal
  - Heavy utilization can cause excessive collisions
- Most Ethernet connections are full-duplex
  - Where are the collisions coming from?
- Interface configuration issues
  - Duplex mismatch
- Hardware issue
  - Could indicate a bad NIC or bad driver

Broadcast storms

- Some processes use broadcasts to communicate
  - Send a message to every device
- Broadcast domain
  - A single VLAN
  - Broadcast domains are separated by routers
- Large numbers of broadcasts can impact performance
  - Each device must process every broadcast

Troubleshooting broadcast storms

- Packet capture
  - Identify the source
- Research the process that's broadcasting
  - There may be another option
- Separate the network into smaller broadcast domains
  - Change one large subnet to many smaller routed subnets

Duplicate MAC addresses

- Not a common occurrence
  - MAC addresses are designed to be unique
  - May be an on-path attack
- 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

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

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?

Multicast flooding

- Multicast
  - Used for one-to-many traffic flows
  - For example, live video feeds
- Switches forward multicast traffic
  - There's no multicast destination address in the switch forwarding table
  - All multicast traffic is sent to every switch port
  - Multicast flooding
- Every device receives the multicast traffic
  - Consumes resources on the remote device
  - Uses bandwidth and switch processing time

5.5 - Common Network Issues (continued)

IGMP snooping
- IGMP (Internet Group Management Protocol)
  - Hosts and routers use IGMP to direct multicast transmissions
- Switches can watch for these IGMP messages
  - The switch then intelligently forwards multicasts to those specific devices
  - Enable IGMP Snooping

Asymmetric routes
- Traffic follows one path on egress
  - And a different path on ingress, or vice versa
  - This is often by design
- This can be difficult to troubleshoot
  - It may be challenging to understand the path
- Firewalls may drop sessions
  - An unexpected traffic flow is dropped by default
- Traceroute can help
  - Identify potential asymmetric routes

Switching loops
- A fear of every network administrator
  - Spanning Tree Protocol is often configured
- Switches communicate by MAC address
  - Every device has it's own address
  - Every packet is directed
- Broadcasts and multicasts are sent to all
  - Broadcast repeated to all switch ports
- Nothing at the MAC address level to identify loops
  - IP has TTL (Time to Live)

Routing loops
- Router A thinks the next hop is to Router B
  - Router B thinks the next hop is to router A
  - And repeat (until TTL=0)
- Easy to misconfigure
  - Especially with static routing
- A traceroute will tell the story
  - Check the routing tables in each L3 device
  - Modify routing tables as needed

Missing route
- A route to the destination network does not exist
  - The packet will be dropped
- ICMP host unreachable message will be sent to the source address
  - Source device will be informed of the error
- Check your routes
  - In both directions

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

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

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

Troubleshooting IP configurations
- Check your documentation
  - IP address, subnet mask, gateway, DNS
- 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

Low optical link budget
- Fiber networks rely on the transmission of light
  - Block the light, block the network
- Attenuation
  - A challenge over long distances
  - Or with dirty connectors
- Always check with a light meter
  - Equipment documentation will specify the required amount light

Certificate issues
- Security alerts and invalid certificates
  - Something isn't quite right
  - Should raise your interest
- Look at the certificate details
  - Click the lock icon
  - May be expired or the wrong domain name
  - The certificate may not be properly signed (untrusted certificate authority)
  - Correct time and date is important

5.5 - Common Network Issues (continued)

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?

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

Incorrect VLAN configurations
- Check VLAN assignments on the switch
  - This is one of the most common issues you'll find
- Confirm the data and voice VLAN assignments
  - Useful when using VoIP phones
- Validate the physical interface with the VLAN number
  - Also important for trunks

DNS issues
- Web browsing doesn't work
  - The Internet is broken!
- Ping works, browser doesn't
  - There isn't a communication problem
- Applications aren't communicating
  - They often use names and not IP addresses

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
  - Quad9 is 9.9.9.9

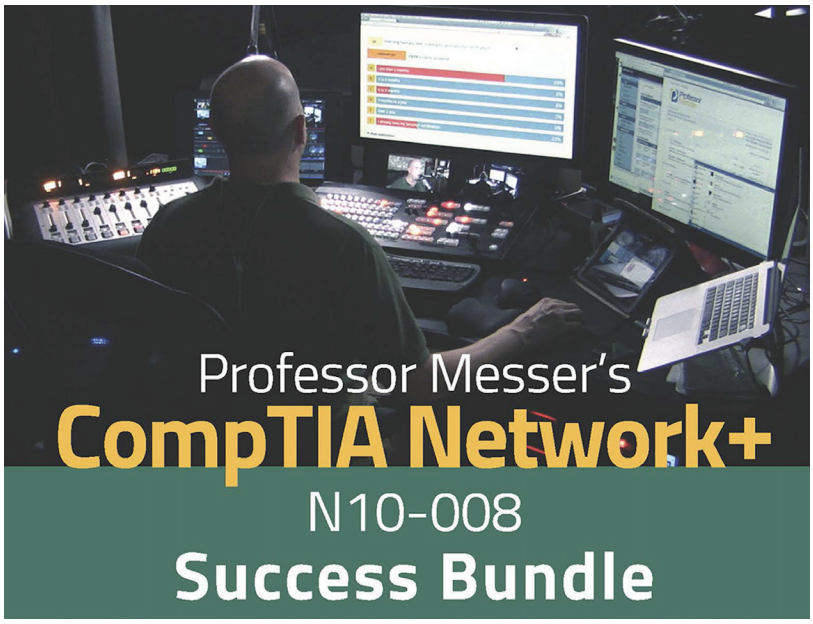
NTP issues
- Some cryptography is very time sensitive
  - Active Directory requires clocks set within five minutes of each other
- Kerberos communication uses a time stamp
  - If the ticket shown during authentication is too old, it's invalid
- Client can't login
  - Check the timestamp of the client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

BYOD
- Bring Your Own Device
  - Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?
- Use an MDM (Mobile Device Manager)

Licensed feature issues
- Features are often individually licensed
  - Requires payment or some type of license agreement
- Some features may not be available
  - A license key unlocks functionality
- This can cause problems during an upgrade or configuration update
  - Test your changes in the lab

Network performance issues
- 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

Continue your journey on
ProfessorMesser.com:



Professor Messer's Free
CompTIA Network+ Training Course

Monthly Network+ Study Group Live Streams

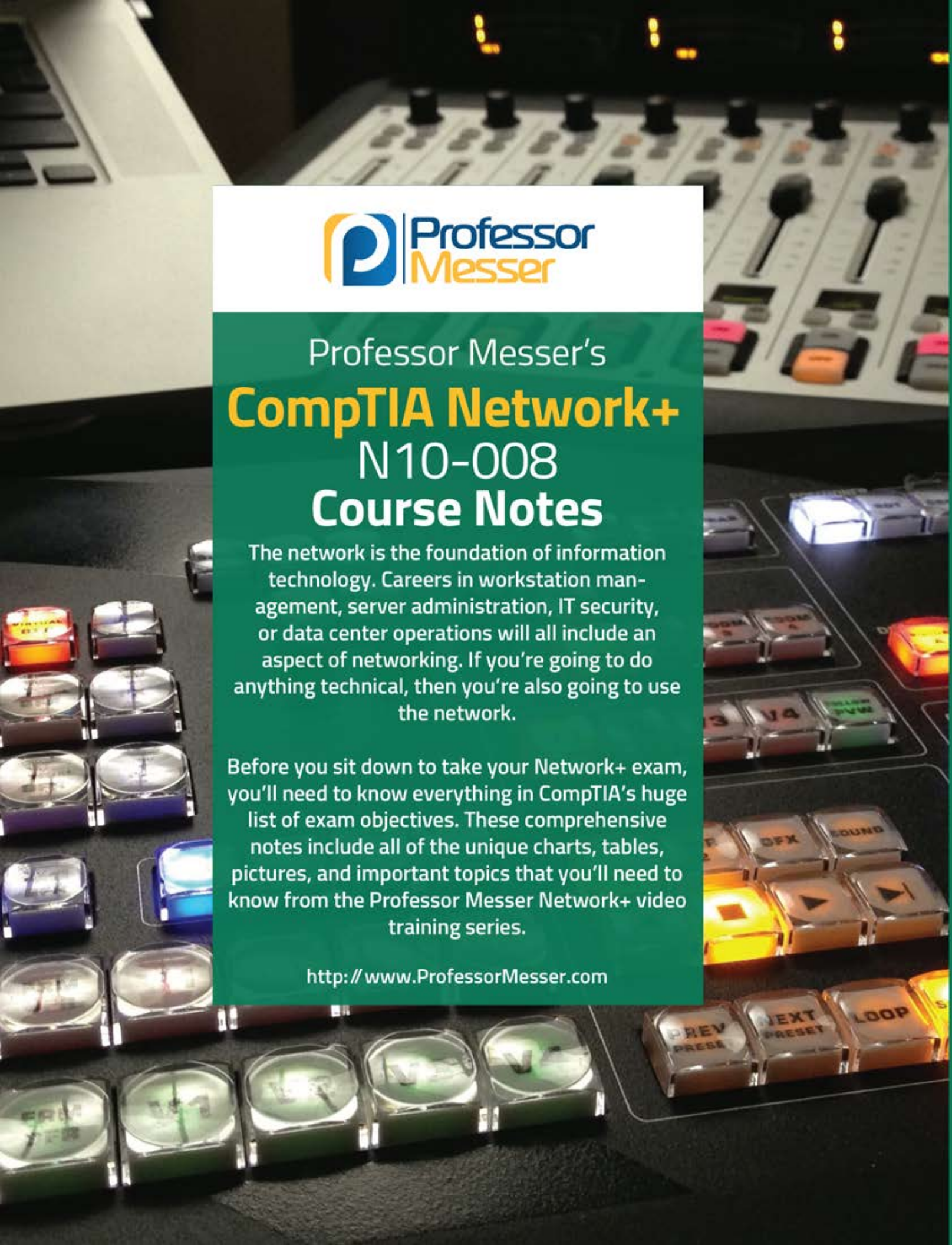
24 x 7 Live Discord Chat

Professor Messer's
CompTIA Network+ Success Bundle

Voucher Discounts

Professor Messer

https://www.ProfessorMesser.com



Professor Messer

Professor Messer's

CompTIA Network+

N10-008

Course Notes

The network is the foundation of information technology. Careers in workstation management, server administration, IT security, or data center operations will all include an aspect of networking. If you're going to do anything technical, then you're also going to use the network.

Before you sit down to take your Network+ exam, you'll need to know everything in CompTIA's huge list of exam objectives. These comprehensive notes include all of the unique charts, tables, pictures, and important topics that you'll need to know from the Professor Messer Network+ video training series.

http://www.ProfessorMesser.com