Professor Messer

Professor Messer's

CompTIA Network+

N10-009

Course Notes

James "Professor" Messer

Professor Messer's CompTIA N10-009 Network+ Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's CompTIA N10-009 Network+ Course Notes
Written by James "Professor" Messer

https://www.ProfessorMesser.com

First Edition: June 2024
This is version 1.4

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA 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 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 Concepts - 23%
Section 2.0 - Network Implementation - 20%
Section 3.0 - Network Operations - 19%
Section 4.0 - Network Security - 14%
Section 5.0 - Network Troubleshooting - 24%

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 N10-009 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+

N10-009 Course Notes

http://www.ProfessorMesser.com

1.1 - Understanding the OSI Model

The OSI Model

- What is 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
  - Often
- All People Seem To Need Data Processing

Layer 1 – 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 – Network Layer

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

Layer 4 – Transport Layer

- The "post office" layer
  - Parcels and letters
- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)

Layer 5 – Session Layer

- Communication management between devices
  - Start, stop, restart
- 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

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

1.1 - Networking Devices

Networking devices

- Many different ways to forward traffic
  - A data center full of equipment
- Every device have a purpose
  - The implementation may change over time
  - Once installed, It can often be difficult to remove
- There are new technologies all the time
  - Always something to learn

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

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

Firewalls
- Filter traffic by port number or application
  - Traditional vs. NGFW
- 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

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

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

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)

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 technologies

Access point (AP)
- 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

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

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
  - The wireless controller is paired with the access points

1.2 - Networking Functions

Networking functions
- There's a lot happening behind the scenes
  - Many networking functions are part of the infrastructure
- Access to important data
  - From anywhere in the world
- Remote access - Secure network communication
- Traffic management
  - Prioritize the important applications
- Protocol support
  - Maintain uptime and availability

Content Delivery Network (CDN)
- It takes time to get data from one place to another
  - Speed up the process
- Geographically distributed caching servers
  - Duplicate the data
  - Users get the data from a local server
- You're using a CDN right now
  - Used on many websites
  - Invisible to the end user

Virtual Private Network (VPN)
- Secure private data traversing a public network
  - Encrypted communication on an insecure medium
- Concentrator / head-end Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Often used with client software
  - Sometimes built into the OS

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

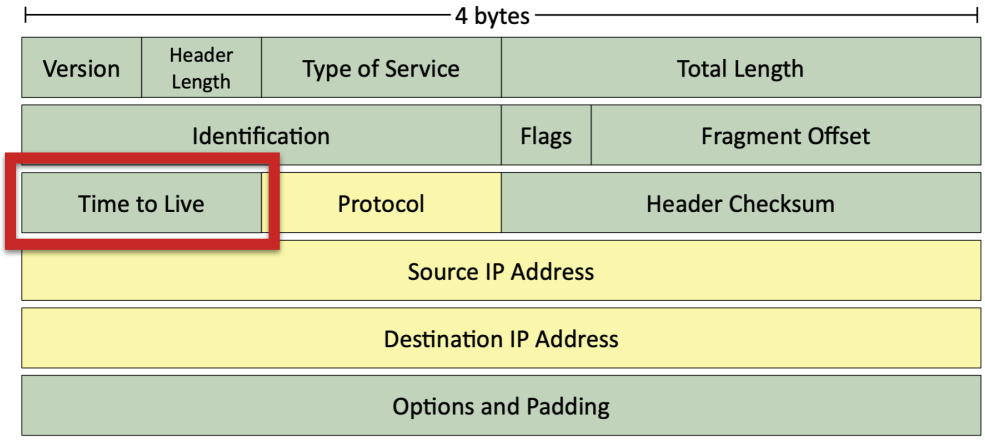
Time to live (TTL)
- How long should data be available?
  - Not all systems or protocols are self-regulating
  - We sometimes need to tell a system when to stop
- Create a timer
  - Wait until traversing a number of hops, or wait until a certain amount of time elapses
  - Then stop (or drop)
- Many different uses
  - Drop a packet caught in a loop
  - Clear a cache

Routing loops
- Router A thinks the next hop is to Router B
  - Router B thinks the next hop is to router A
  - And repeat
- Easy to misconfigure
  - Especially with static routing
- This can't go on forever
  - TTL is used to stop the loop

IP (Internet Protocol)
- Loops could cause a packet to live forever
  - Drop the packet after a certain number of hops
- Each pass through a router is a hop
  - Default TTL for macOS/Linux is 64 hops
  - Default TTL for Windows is 128 hops
- The router decreases TTL by 1
  - A TTL of zero is dropped by the router

DNS (Domain Name System)
- DNS lookups
  - Resolve an IP address from a fully-qualified domain name www.professormesser.com = 172.67.41.114
- A device caches the lookup for a certain amount of time
  - How long? TTL seconds long.

Ethernet frame and the TTL field



1.3 - Designing the Cloud

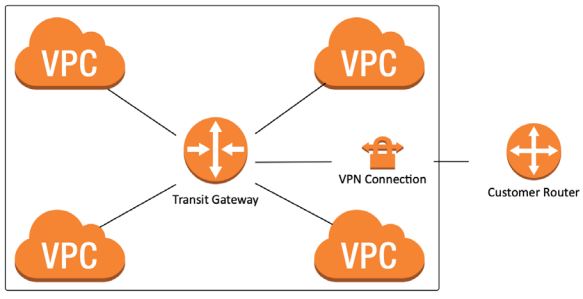
Designing the cloud
- On-demand computing power
  – Click a button
- Elasticity
  – Scale up or down as needed
- Applications also scale
  – Scalability for large implementations
  – Access from anywhere
- Multitenancy
  – Many different clients are using the same cloud infrastructure

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.

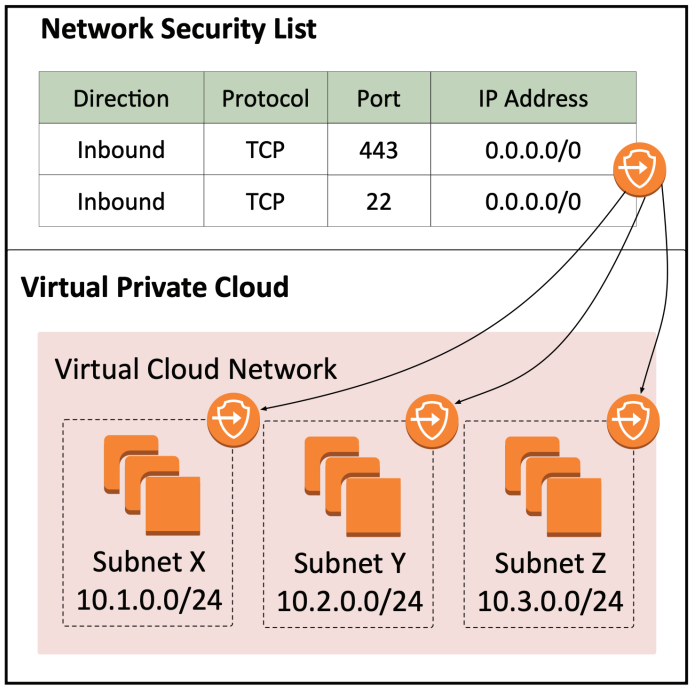
Connecting to the cloud
- Virtual Private Cloud (VPC)
  – A pool of resources created in a public cloud
- Common to create many VPCs
  – Many different application clouds
- Connect VPCs with a transit gateway
  – And users to VPCs
  – A "cloud router"
- Now make it secure
  – VPCs are commonly on different IP subnets



- VPN (Virtual Private Network)
  – Site-to-site VPN through the Internet
- Virtual Private Cloud Gateway / Internet gateway
  – Connects users on the Internet
- VPC NAT gateway
  – Network address translation
  – Private cloud subnets connect to external resources
  – External resources cannot access the private cloud
- VPC Endpoint
  – Direct connection between cloud provider networks
  Connecting to the cloud is often through a VPN

Security groups and lists
- A firewall for the cloud
  – Control inbound and outbound traffic flows
- Layer 4 port number
  – TCP or UDP port
- Layer 3 address
  – Individual addresses
  – CIDR block notation
  – IPv4 or IPv6

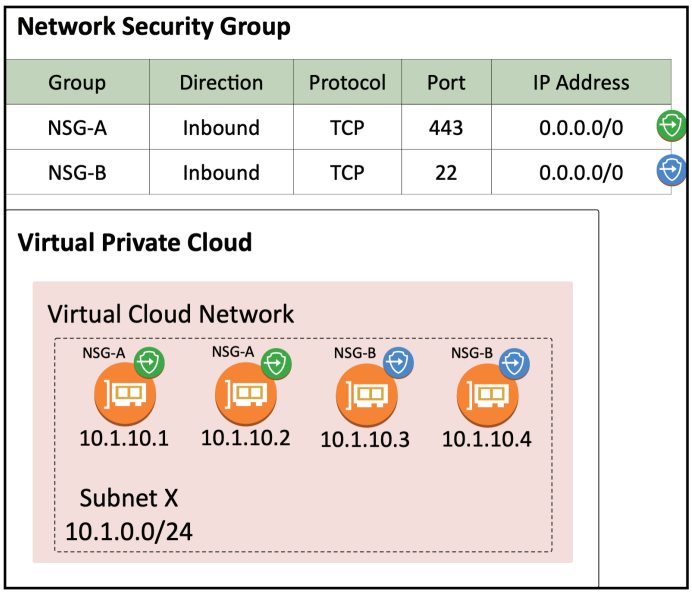
Network security list
- Assign a security rule to an entire IP subnet
  – Applies to all devices in the subnet
- Very broad
  – Can become difficult to manage
  – Not all devices in a subnet have the same security posture
- More granularity may be needed
  – Broad rules may not provide the right level of security



1.3 - Designing the Cloud (continued)

Network security group

- Assign a security rule to a specific virtual NIC (VNIC)
  - Applies to specific devices and network connections
- More granular than network security lists
  - Different rules for devices in the same IP subnet
- Better control and granularity
  - The best practice for cloud security rules



1.3 - Cloud Models

Cloud deployment models

- Public
  - Available to everyone over the Internet
- Private
  - Your own virtualized local data center
- Hybrid
  - A mix of public and private

Software as a service (SaaS)

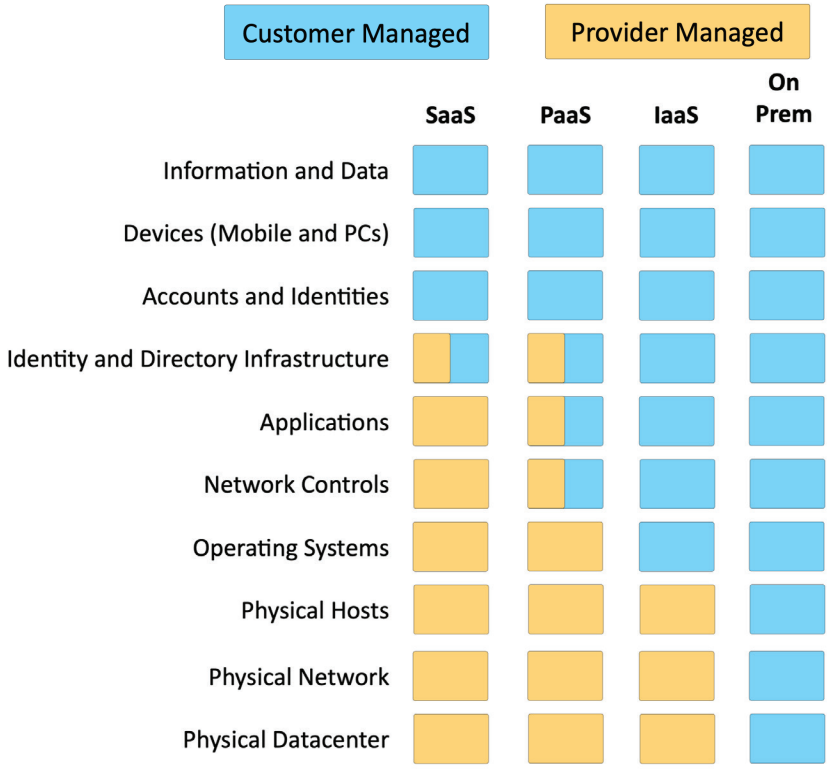
- On-demand software
  - No local installation
  - Why manage your own email distribution?
  - Or payroll?
- Central management of data and applications
  - Your data is out there
- A complete application offering
  - No development work required
  - Google Mail, Office 365

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

Platform as a service (PaaS)

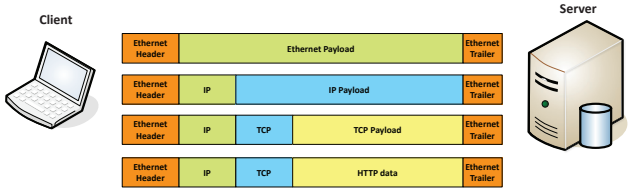
- No servers, no software, no maintenance team, no HVAC
  - Someone else handles the platform, you handle the development
- You don't have direct control of the data, people, or infrastructure
  - Trained security professionals are watching your stuff
  - Choose carefully
- Put the building blocks together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



1.4 - 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, cable system
- 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



IP - Internet Protocol

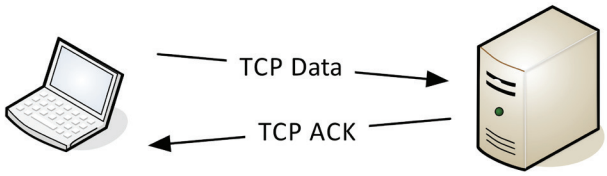
TCP and UDP

- 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

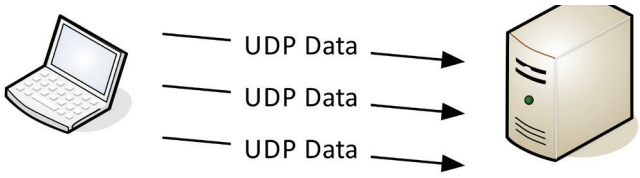
TCP - Transmission Control Protocol Communication



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
  - Sender determines the amount of data transmitted

UDP - User Datagram Protocol Communication



Speedy delivery

- The IP delivery truck delivers from one (IP) address to another (IP) address
  - Every house has an address, every computer has an IP address
- Boxes arrive at the house / IP address
  - Where do the boxes go?
  - Each box has a room name
- Port is written on the outside of the box
  - Drop the box into the right room

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 client

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

1.4 - Common Ports

FTP - File Transfer Protocol
- Transfers files between systems
  - Generic file transfer method
  - Not specific to an operating system
- tcp/20 (active mode data), tcp/21 (control)
  - Authenticates with a username and password
- Full-featured functionality
  - List, add, delete, etc.

SSH - Secure Shell
- Text-based console communication
- Encrypted communication link - tcp/22
  - SFTP - Secure FTP
- Generic file transfer with security
  - Encrypted network communication
- Uses the SSH File Transfer Protocol
  - tcp/22
- Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal
- Uses SSH (port 22)
  - SSH isn't just for console communication

Telnet
- Telnet – Telecommunication Network
  - tcp/23
- Console access
  - Similar functionality to SSH
- In-the-clear communication
  - Not the best choice for production systems

SMTP - Simple Mail Transfer Protocol
- SMTP - Simple Mail Transfer Protocol
  - Server to server email transfer
  - tcp/25 (SMTP using plaintext)
  - tcp/587 (SMTP using TLS encryption)
- 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

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

DHCP - Dynamic Host Configuration Protocol
- Automated configuration of IP address, subnet mask and other options
  - udp/67, udp/68
  - Requires a DHCP server
  - Server, appliance, integrated into a SOHO router, etc.
- Dynamic / pooled
  - IP addresses are assigned in real-time from a pool
  - Each system is given a lease, must renew at set intervals
- DHCP reservation
  - Addresses are assigned by MAC address in the DHCP server
  - Quickly manage addresses from one location

TFTP - Trivial File Transfer Protocol
- TFTP – Trivial File Transfer Protocol
  - udp/69
- Very simple file transfer application
  - Read files and write files
- No authentication
  - Not used on highly secure systems
- Useful when starting a system
  - Transfer configuration files
  - Quick and easy

HTTP and HTTPS
- Hypertext Transfer Protocol
  - Communication in the browser
  - And by other applications
- In the clear or encrypted
  - SSL (Secure Sockets Layer) or TLS (Transport Layer Security)

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 on a local network

1.4 - Common Ports (continued)

SNMP - Simple Network Management Protocol
- Gather statistics from network devices
  - udp/161
- v1 – The original
  - Structured tables and data sent in-the-clear
- v2 – A good step ahead
  - Data type enhancements, bulk transfers
  - Still in-the-clear
- v3 – A secure standard
  - Message integrity, authentication, encryption
- SNMP traps
  - Alerts and notifications from the network devices
  - udp/162

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

SMB - Server Message Block
- Protocol used by Microsoft Windows
  - File sharing, printer sharing
  - Also called CIFS (Common Internet File System)
- Integrated into the operating system
  - Access rights integration across systems
  - File share publishing
  - File locking
- Direct over tcp/445 (NetBIOS-less)
  - Direct SMB communication over TCP

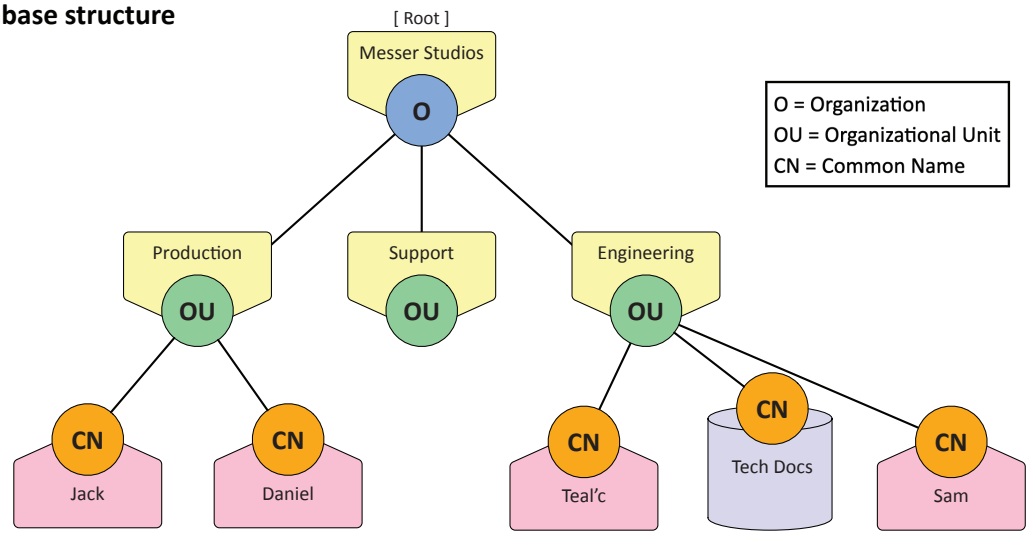
Syslog
- Standard for message logging
  - Diverse systems, consolidated log
  - udp/514
- Usually a central log collector
  - Integrated into the SIEM
  - Security Information and Event Manager
- You're going to need a lot of disk space
  - No, more. More than that.
  - Data storage from many devices over an extended timeframe

Databases
- Collection of information
  - Many different types of data
  - One common method to store and query
- Structured Query Language (SQL)
  - A standard language across database servers
  - SELECT * FROM Customers WHERE Last_Name='Messer';
- Microsoft SQL Server
  - MS-SQL
  - (Microsoft Structured Query Language)
  - tcp/1433

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

SIP - Session Initiation Protocol
- Voice over IP (VoIP) signaling
  - tcp/5060 and tcp/5061
- Setup and manage VoIP sessions
  - Call, ring, play busy signal, hang up
- Extend voice communication
  - Video conferencing
  - Instant messaging
  - File transfer
  - etc.

LDAP database structure



1.4 - Common Ports (continued)

Protocol	Port	Name	Description
ARP	-	Address Resolution Protocol	Resolve IP address to MAC
TCP	-	Transmission Control Protocol	Connection-oriented network communication
UDP	-	User Datagram Protocol	Connectionless network communication
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
SFTP	tcp/22	Secure File Transfer Protocol	Encrypted file transfers using SSH
SSH	tcp/22	Secure Shell	Encrypted console login
Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
SMTP	tcp/25	Simple Mail Transfer Protocol	Transfer email between mail servers
DNS	udp/53, tcp/53	Domain Name Services	Convert domain names to IP addresses
DHCP	udp/67, udp/68	Dynamic Host Configuration Protocol	Update to BOOTP
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
NTP	udp/123	Network Time Protocol	Automatically synchronize clocks
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
SNMP Trap	udp/162	Simple Network Management Protocol Traps	Alerts and notifications from the network devices
LDAP	tcp/389	Lightweight Directory Access Protocol	Directory services
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
SMB	tcp/445	Server Message Block	File and printer sharing for Windows
Syslog	udp/514	System Logging	A standard for message logging
SMTPS	tcp/587	Simple Mail Transfer Protocol Secure	Transfer email between mail servers with encryption
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
RDP	tcp/3389	Remote Desktop Protocol	Graphical display and control of remote device
SIP	tcp/5060-5061	Session Initiation Protocol	Voice over IP signaling protocol

1.4 - 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

VPNs

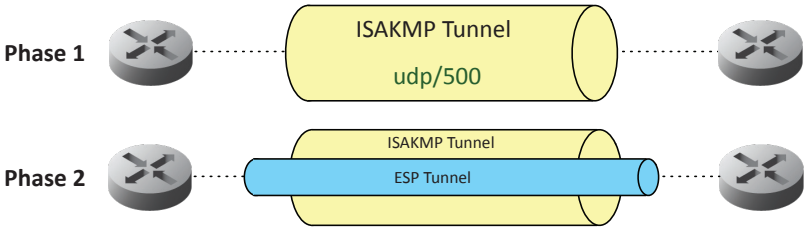
- Virtual Private Networks
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available

1.4 - Other Useful Protocols (continued)

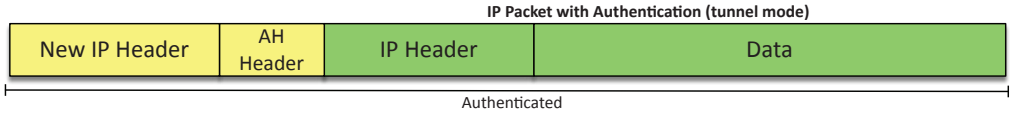
Site-to-site VPN
- Always-on
  - Or almost always
- Firewalls often act as VPN concentrators
  - Probably already have firewalls in place

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)

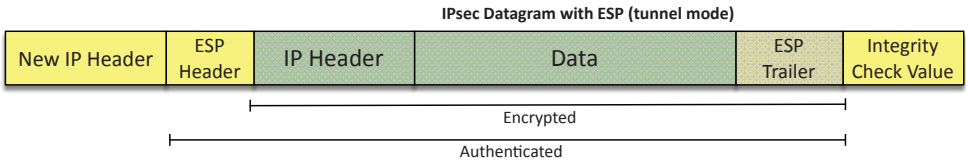
Internet Key Exchange (IKE)
- Agree on encryption/decryption keys
  - Without sending the key across the network
  - Builds a Security Association (SA)
- Phase I
  - Use Diffie-Hellman to create a shared secret key
  - udp/500
  - ISAKMP (Internet Security Association and
  - Key Management Protocol)
- Phase II
  - Coordinate ciphers and key sizes
  - Negotiate an inbound and outbound SA for IPsec



AH (Authentication Header)
- Hash of the packet and a shared key
  - MD5, SHA-1, or SHA-2 are common
  - Adds the AH to the packet header

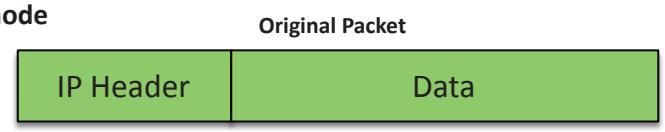


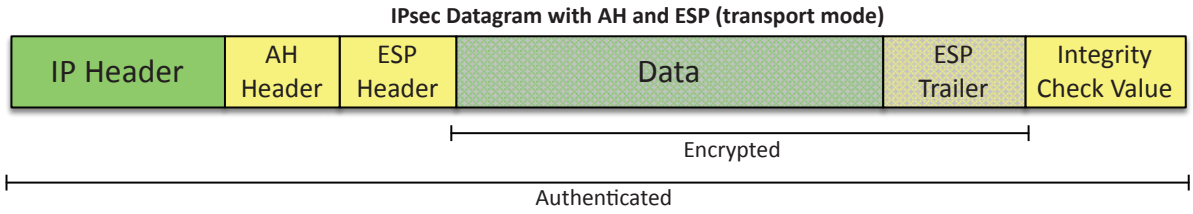
ESP (Encapsulating Security Payload)
- Encrypts the packet
  - MD5, SHA-1, or SHA-2 for hash, and 3DES or AES for encryption
  - Adds a header, a trailer, and an Integrity Check Value

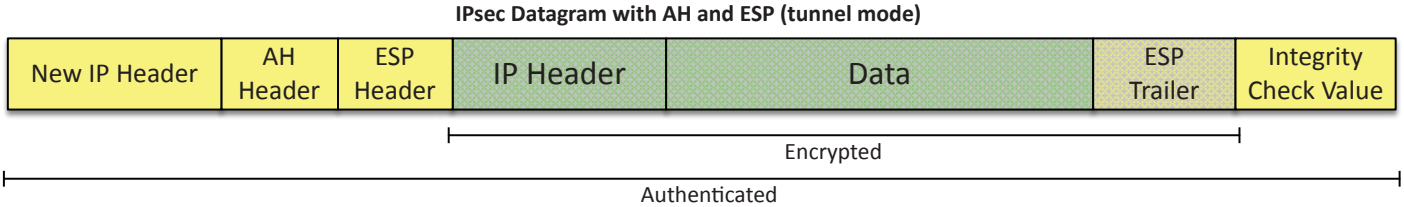


IPsec Transport mode and Tunnel mode

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







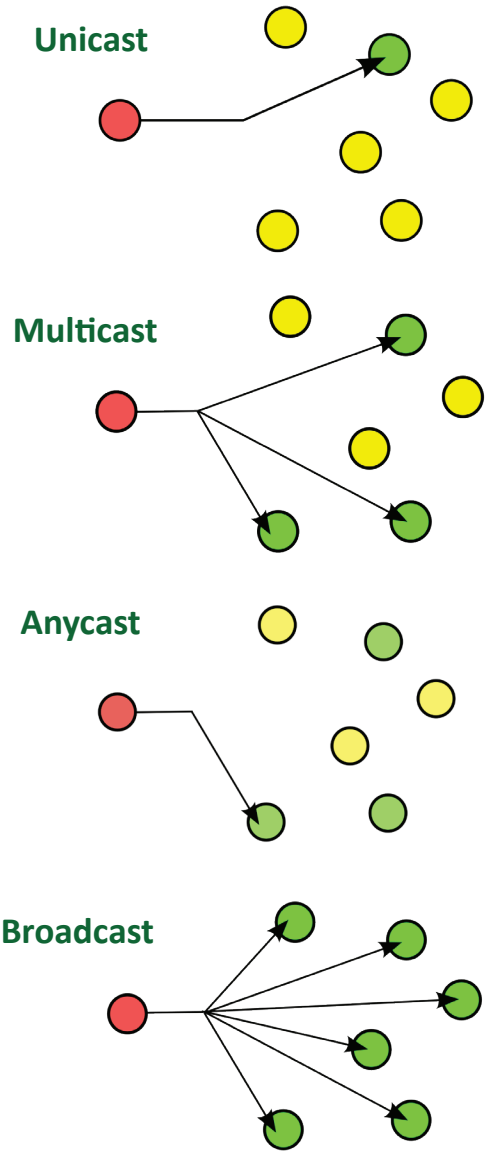
1.4 - Network Communication

Unicast
- One station sending information to another station - One-to-one
- Send information between two systems
  – Web surfing, file transfers
- Does not scale optimally for real-time streaming media
- IPv4 and IPv6

Multicast
- Delivery of information to interested systems - One-to-many-of-many
- Multimedia delivery, stock exchanges, dynamic routing updates
- 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

Broadcast
- Send information to everyone at once - One-to-all
- One packet, received by everyone
  – Limited scope
  – The broadcast domain
- Routing updates, ARP requests
  – Used in IPv4
- Not used in IPv6
  – Uses multicast instead



1.5 - Wireless Networking

Wireless standards
- Wireless networking (802.11)
  – Managed by the IEEE LAN/MAN
  – Standards Committee (IEEE 802)
- Many updates over time
  – Check with IEEE for the latest
- The Wi-Fi trademark
  – Wi-Fi Alliance handles interoperability testing
- Modern standards have a more marketable name
  – For example, 802.11ax is Wi-Fi 6

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

1.5 - Wireless Networking (continued)

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

Satellite networking

- Communication to a satellite
  - Non-terrestrial communication
- High cost relative to terrestrial networking
  - 100 Mbit/s down, 5 Mbit/s up are common
  - Remote sites, difficult-to-network sites
- Relatively high latency
  - 250 ms up, 250 ms down
  - Starlink advertises 40 ms and is working on 20 ms
- High frequencies - 2 GHz
  - Line of sight, rain fade

802.11 wireless networking

IEEE Standard	Generation Name	Frequencies	Maximum theoretical link rate
802.11a	-	5 GHz	6-54 Mbit/s
802.11b	-	2.4 GHz	1-11 Mbit/s
802.11g	-	2.4 GHz	6-54 Mbit/s
802.11n	Wi-Fi 4	2.4 GHz / 5 GHz	72-600 Mbit/s
802.11ac	Wi-Fi 5	5 GHz	433-6,933 Mbit/s
802.11ax	Wi-Fi 6 and 6E	2.4 GHz / 5 GHz / 6 GHz	574-9,608 Mbit/s
802.11be	Wi-Fi 7	2.4 GHz / 5 GHz / 6 GHz	1,376-46,120 Mbit/s

1.5 - 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
  - The standard defines the media

IEEE Ethernet standards

- The 802.3 committee
  - All types and standards of Ethernet
  - Copper and fiber

Deciphering the standard

- Speed, signal, and media
  - All contained in the standard name, i.e., 1000BASE-T
- The number is related to the network speed
  - 1000 is commonly 1,000 megabits per second (or one gigabit/sec)
  - 10G would be 10 gigabits per second
- BASE (baseband)
  - Single frequency using the entire medium
  - Broadband uses many frequencies, sharing the medium
- Media type
  - T is twisted pair copper, F is fiber
  - SX would be short wavelength light

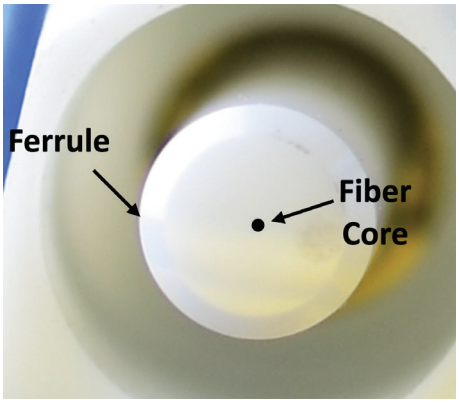
IEEE Standard	Description	Media	Network Speed
1000BASE-T	Gigabit Ethernet	Copper	1 gigabit per second
10GBASE-T	10 Gigabit Ethernet	Copper	10 gigabits per second
1000BASE-SX	Gigabit Ethernet	Fiber	1 gigabit per second

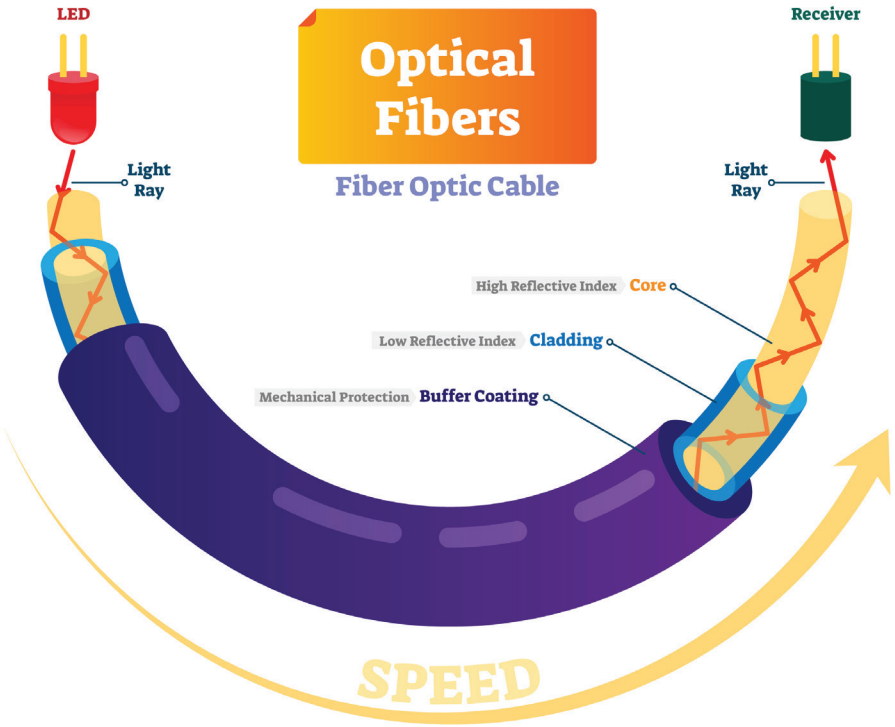
1.5 - Optical Fiber

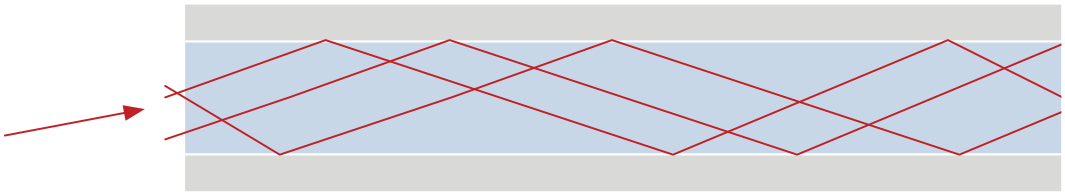
Fiber communication
- Transmission by light
  – The visible spectrum
- No RF signal
  – Very difficult to monitor or tap
- Signal slow to degrade
  – Transmission over long distances
- Immune to radio interference
  – There's no RF

Multimode fiber
- Short-range communication
  – Up to 2 km
- Inexpensive light source
  – LED

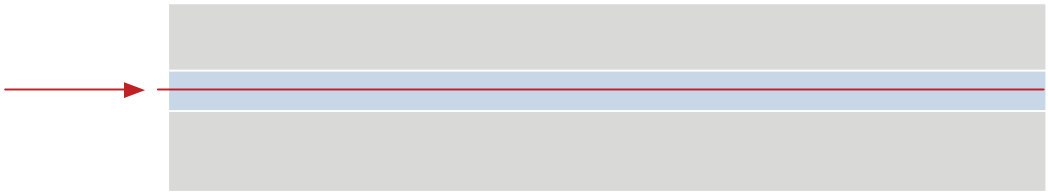
Single-mode fiber
- Long-range communication
  – Up to 100 km without processing
- Expensive light source
  – Laser beams







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



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

1.5 - Copper Cabling

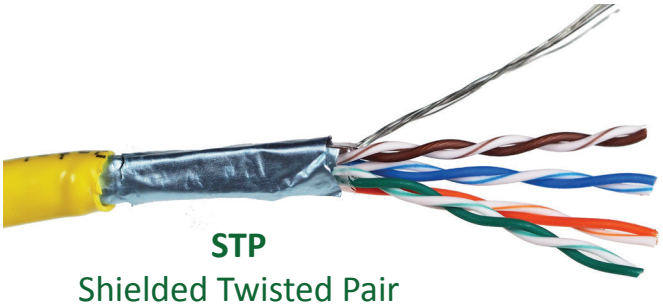
Copper Cabling

- 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
  - Everything eventually touches a cable

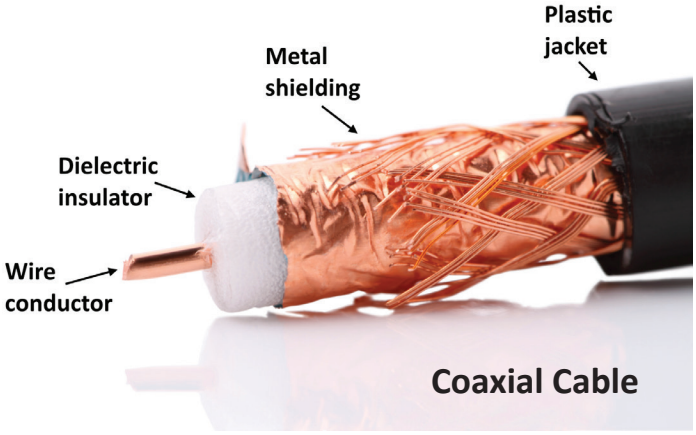
Twisted pair copper cabling

- Balanced pair operation
  - Two wires with equal and opposite signals
  - Transmit+, Transmit- / Receive+, Receive-
- The twist is the secret!
  - 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

UTP
Unshielded Twisted Pair



STP
Shielded Twisted Pair



Coaxial Cable

Cable speeds

- Cables don't have a speed
  - The copper just sits there
- Electrical signals are sent over copper cable
  - The signal encoding determines the data transfer rate
- A cable must be manufactured to specific standards
  - IEEE 802.3 Ethernet standards determine the cable type
- Cable standards are described as a "category" of cable
  - Category 6, Category 7, etc.
  - Check the IEEE standard to determine the minimum cable category
  - The minimum cable category for 1000BASE-T is Category 5

Coaxial cables

- Two or more forms share a common axis
- RG-6 used in television/digital cable
  - And high-speed Internet over cable

Twinaxial cable

- Two inner conductors
  - Twinax
- Common on 10 Gigabit Ethernet SFP+ cables
  - Full duplex
  - Five meters
  - Low cost
  - Low latency compared to twisted pair

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
- Worst-case planning
  - Used in plenum and risers
  - Important concerns for any structure

Twinaxial Cable

1.5 - Network Transceivers

Transceiver

- Transmitter and receiver, usually in a single component
- Provides a modular interface
  - Add the transceiver that matches your network
- Many different types
  - Ethernet or Fibre Channel
  - Not compatible with each other
- Different media types - fiber and copper

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 physical size as SFPs
  - Supports data rates up to 16 Gbit/s
  - Common with 10 Gigabit Ethernet

SFP/SFP+

QSFP/QSFP+

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

1.5 - Fiber Connectors

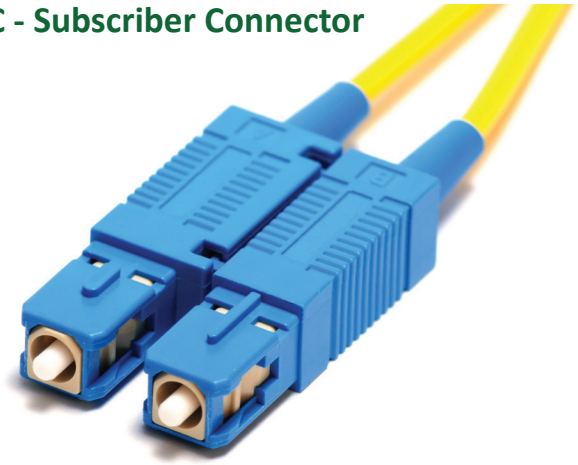
SC - Subscriber Connector

- Not actually an abbreviation
  - We've created our own names
  - Square Connector
  - Standard Connector
- Pushes on to lock
  - Pull connector to unlock
- A popular fiber connector
  - Common in many data centers

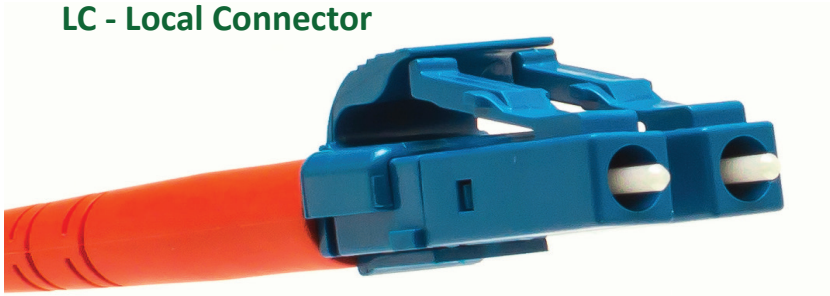
LC - Local Connector

- Another popular fiber type
- Smaller and more compact connector
- Locks in place with a clip
- Press to release
- Other names
- Lucent Connector
- Little Connector

SC - Subscriber Connector



LC - Local Connector



1.5 - Fiber Connectors (continued)

ST - Straight Tip

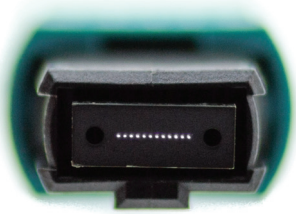
- Bayonet connector
  - Stick and Twist
- Push on and turn
  - Locks in place
  - Turn to unlock

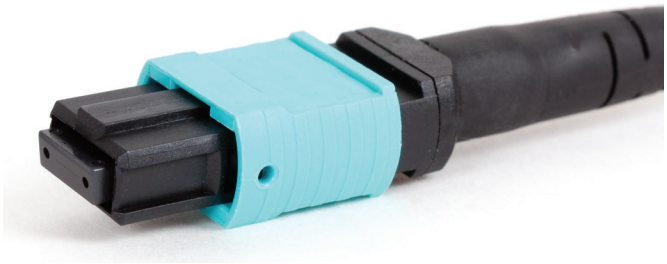
MPO - Multi-fiber Push On

- Twelve fibers in a single connector
  - Save space and manage one cable
- Push to lock in place
  - Pull connector to unlock
- May also see the MTP abbreviation
  - A Corning brand
  - The MTP MPO connector

ST - Straight Tip

MPO - Multi-fiber Push On





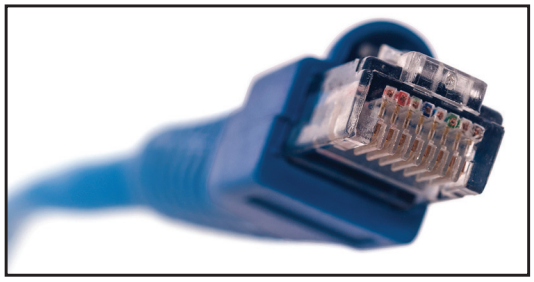
1.5 - Copper Connectors

RJ11 connector

- Registered Jack type 11
  - 6 position, 2 conductor (6P2C)
- Telephone & DSL connection

RJ45 connector

- Registered Jack type 45
  - 8 position, 8 conductor (8P8C)
  - Modular connector
  - Ethernet



RJ-45 Connector

F-connector

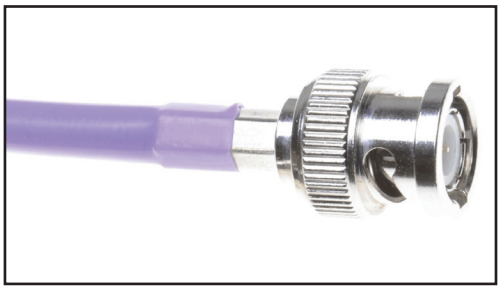
- Coaxial cable
  - Standard connector type
  - Threaded connector
- Cable television infrastructure
  - Cable modem
  - DOCSIS (Data Over Cable Service
  - Interface Specification)

BNC connector

- Bayonet Neill-Concelman
  - Paul Neill (Bell Labs) and Carl Concelman (Amphenol)
- Another common coaxial cable connector
  - Common with twinax and DS3 WAN links
  - Video connections
- Secure connections
  - Twist and lock in place

RJ-11 Connectors

F-connector



BNC connector

1.6 - 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

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

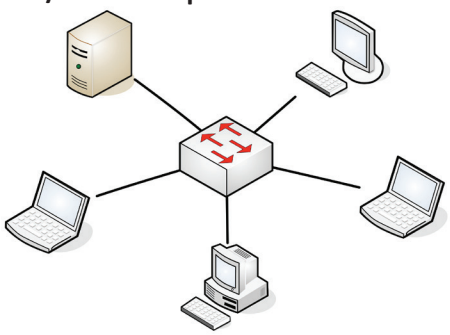
Hybrid
- A combination of one or more physical topologies
  - Most networks are a hybrid

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

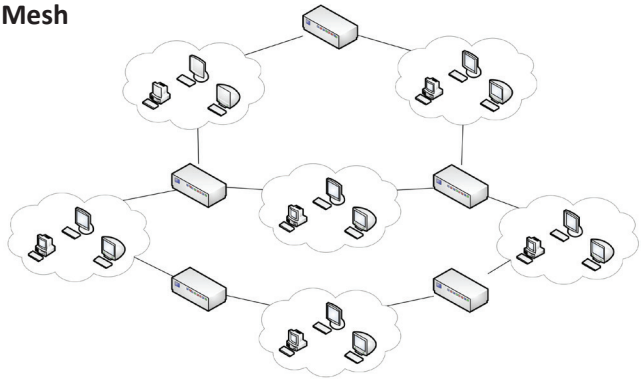
Point-to-point
- One-to-one connection
- Older WAN links
  - "Point to point T-1"
- Connections between buildings

Point-to-point

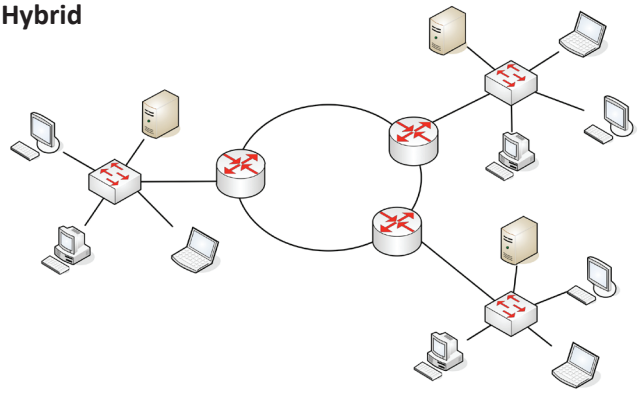
Star / Hub and spoke



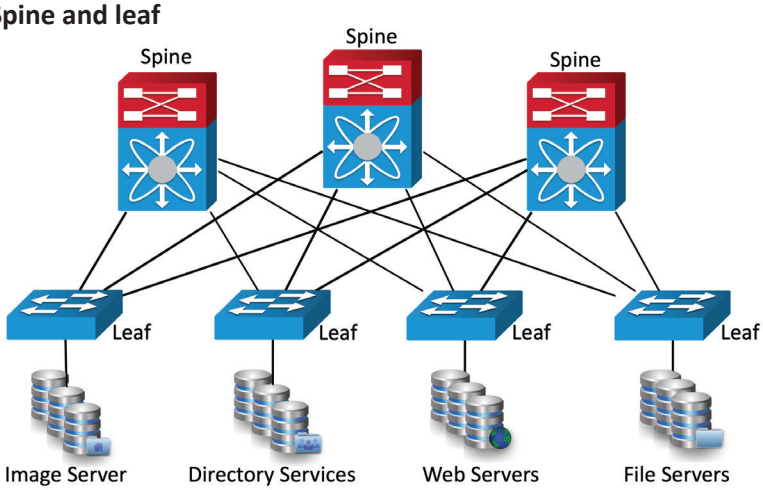
Mesh



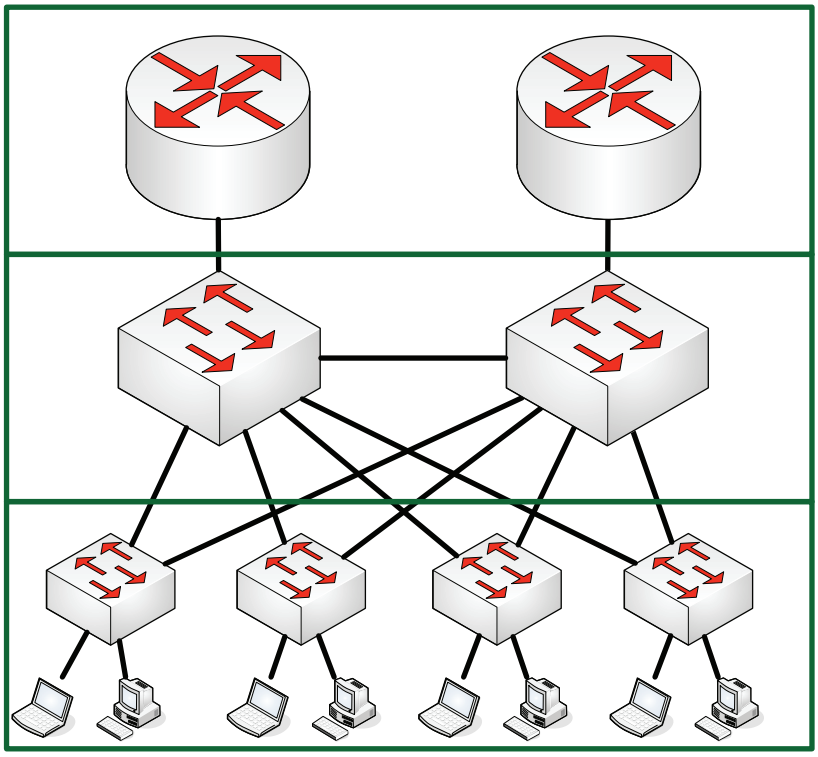
Hybrid



Spine and leaf



1.6 - Network Architecture

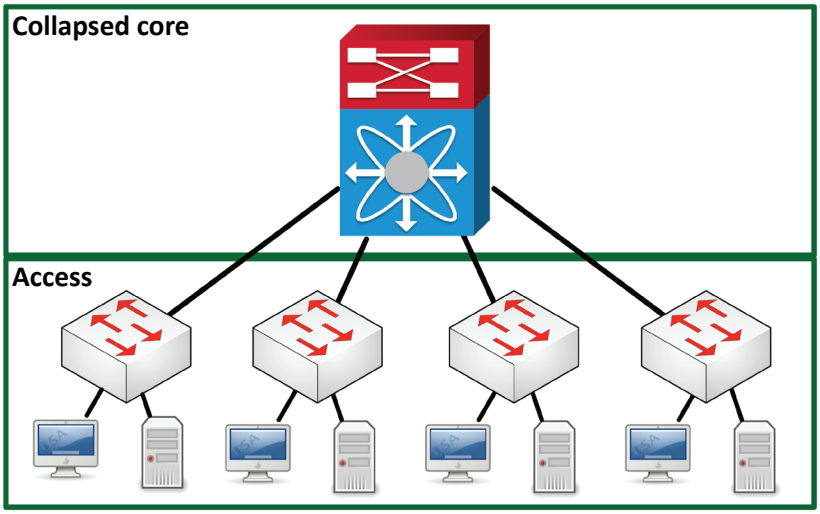


Three-Tier Architecture

- 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

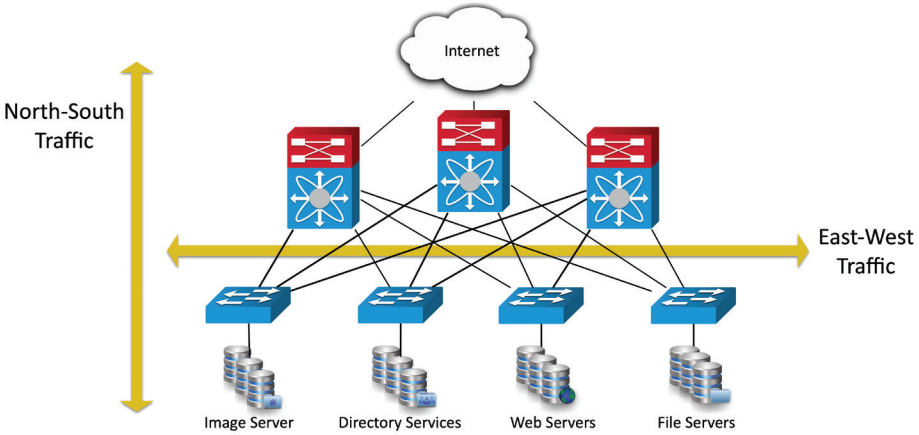
Collapsed core

- Combine the Core and Distribution layers
  - Do more with less
- Good for small and medium sized networks
  - Multiple buildings or campus configuration
- Advantages
  - Costs less
  - Simple to deploy
- Disadvantages
  - Scalability limitations
  - Fewer devices means less redundancy



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



1.7 - Binary Math

Basics of binary math

- A bit - a zero or a one
  - One digit. Off or on. Cold or hot. 0 or 1.
- A byte – Eight bits
  - Often called an "octet" to avoid ambiguity
- A binary-to-decimal conversion chart
- Powers of two
  - Useful for binary calculations and subnetting

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

1.7 - 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
- 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
  - All "Class E" addresses
- Virtual IP addresses (VIP)
  - Not associated with a physical network adapter
  - Virtual machine, internal router address

IPv4 addresses

- Internet Protocol version 4
  - OSI Layer 3 address
  - DHCP
- IPv4 address configuration used to be a manual process
  - IP address, subnet mask, gateway,
  - DNS servers, NTP servers, etc.
- Dynamic Host Configuration Protocol
  - Provides automatic address and
  - IP configuration for almost all devices

Automatic Private IP Addressing (APIPA)

- A link-local address
  - Can only communicate to other local devices
  - 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
- Automatically assigned
  - Uses ARP to confirm the address isn't currently in use

The IPv4 address problem

- There are far more devices than IPv4 addresses
  - This Internet thing could be big
- The use and registration of IP address ranges is problematic
  - Unused and non-continuous address blocks
  - Complete depletion of available addresses
- Not all devices need to communicate across the Internet
  - No, really

Private IP address ranges

- More public IP addresses
  - More Internet connectivity
- Huge private IP address ranges
  - Properly design and scale large networks
- Private IP addresses are not Internet-routable
  - But can be routed internally
  - Use NAT for everything else
- Defined in RFC 1918 - Request for Comment

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

1.7 - Classful Subnetting

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
  - Subnet classes
  - What IP class?

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

Subnet calculations

- IP address: 10.74.222.11
  - Class A
  - Subnet mask 255.0.0.0
- IP address: 172.16.88.200
  - Class B
  - Subnet mask 255.255.0.0
- IP address: 192.168.4.77
  - Class C
  - Subnet mask 255.255.255.0

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

1.7 - IPv4 Subnet Masks

Classless subnetting

- CIDR (Classless Inter-Domain Routing)
  - Created around 1993
  - Removed the restrictions created by classful subnet masks
  - "Cider" block notation
- Subnet masks can be expressed as decimal or in CIDR-block notation
  - IP address, slash, number of subnet bits; 192.168.1.44/24
- You'll usually be provided an IP address, subnet mask, default gateway, and DNS servers
  - Some operating systems are expecting decimal masks
  - Some operating systems are expecting CIDR notation masks

The subnet mask

- Contiguous series of ones
  - Ones on the left
  - Zeros on the right

1.7 - 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^{16}	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}
65,536	32,768	16,384	8,192	4,096	2,048	1,024	512	256	128	64	32	16	8	4	2

1.7 - 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

1.7 - Seven Second Subnetting

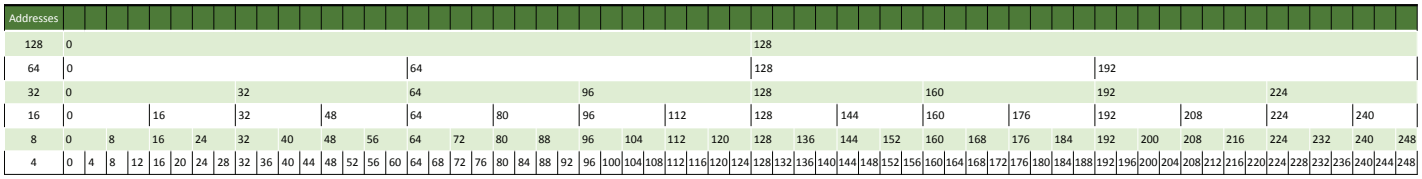
Seven second subnetting

- Designed for exam situations
  - Very fast subnetting
  - No second guessing
- Very little math involved
  - Some simple addition to create the tables
  - Add and subtract one
- Combination of many different techniques
  - Find one that works for you
- Use the in-person or digital whiteboard
- Quickly create the charts - bring your own erasable marker

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



1.8 - Software Defined Networking

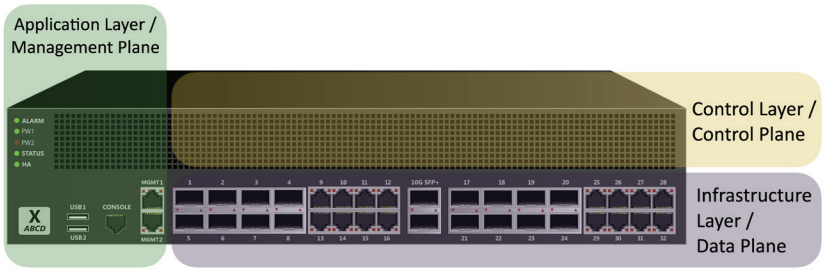
SDN (Software Defined Networking)

- 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
  - SSH, browser, API
  - Extend the physical architecture

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

Extend the physical architecture



SD-WAN characteristics

- Application aware
  - The WAN knows which app is in use
  - Makes routing decisions based on the application data
- Zero-touch provisioning
  - Remote equipment is automatically configured
  - Application traffic uses the most optimal path
  - Can change based on traffic patterns and network health
- Transport agnostic
  - The underlying network can be any type
  - Cable modem, DSL, fiber-based, 5G, etc.
  - Pick the best choice for the location
- Central policy management
  - Management and configuration on a single console
  - One device to configure
  - Changes are pushed to the SD-WAN routers

1.8 - Virtual Extensible LAN

Data center interconnect (DCI)

- Connect multiple data centers together
  - Device networks seamlessly span across these geographic distances
- Connect and segment different customer networks
  - Across multiple data centers
  - All customers share the same core network
- Distribute applications everywhere
  - Increase uptime and availability
  - Workload can be moved to the best location

Scaling across data centers

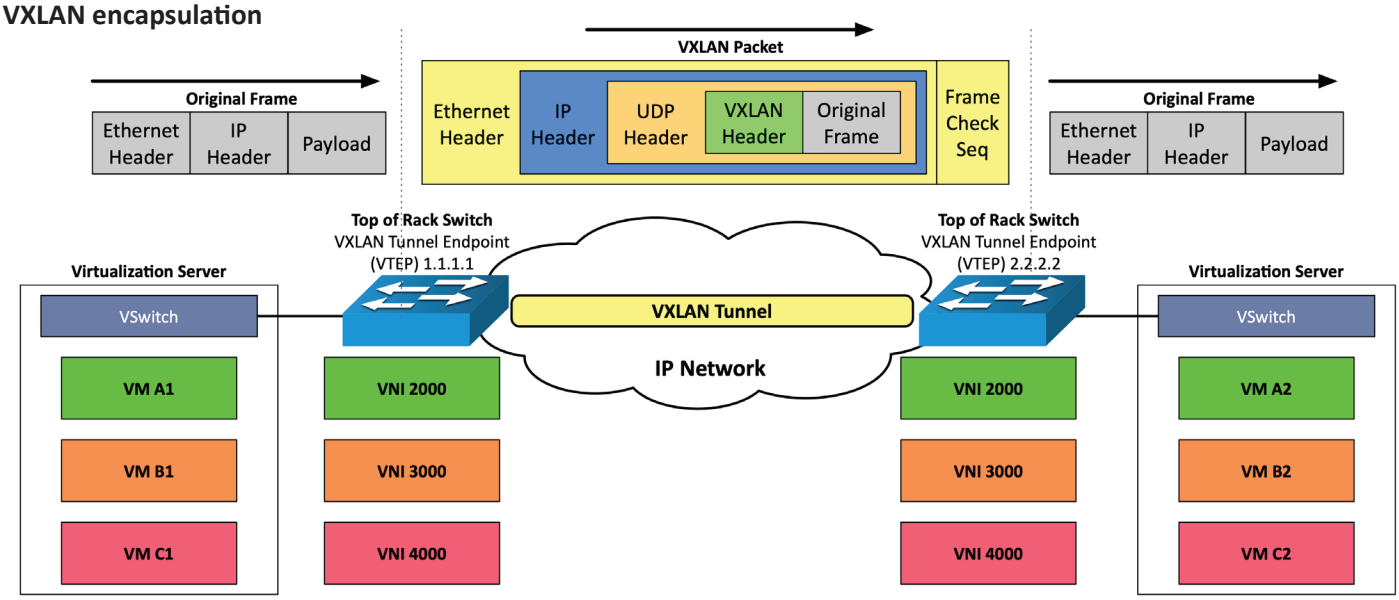
- IP addressing is different across data centers
  - Challenging to manage dynamically created virtual systems
- Data centers can be connected in different ways
  - MPLS, high speed optical, Metro Ethernet, etc.
- Applications shouldn't have to worry about
  - IP addressing, routing, or connectivity
  - Applications should work regardless of physical location
- Extend networks across physical locations
  - Encapsulate, send the data, decapsulate
  - Tunnel the data

Virtual Extensible LAN (VXLAN)

- Designed for large service providers
  - Hundreds or thousands of tenants
- VLANs
  - Maximum of about 4,000 possible virtual networks
  - Fixed layer 2 domain
  - Not designed for large scale and dynamic movement of VMs
- VXLAN support
  - Over 16 million possible virtual networks
  - Tunnel frames across a layer 3 network
  - Built to accommodate large virtual environments

1.8 - Virtual Extensible LAN (continued)

VXLAN encapsulation



1.8 - Zero Trust

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 inherently trusted
  - Multi-factor authentication, encryption, system permissions, additional firewalls, monitoring and analytics, etc.

Policy-based authentication

- Adaptive identity
  - Consider the source and the requested resources
  - Multiple risk indicators - relationship to the organization, physical location, type of connection, IP address, etc.
  - Make the authentication stronger, if needed
- Policy-driven access control
  - Combine the adaptive identity with a predefined set of rules
  - Evaluates each access decision based on policy and other information
  - Grant, deny, or revoke

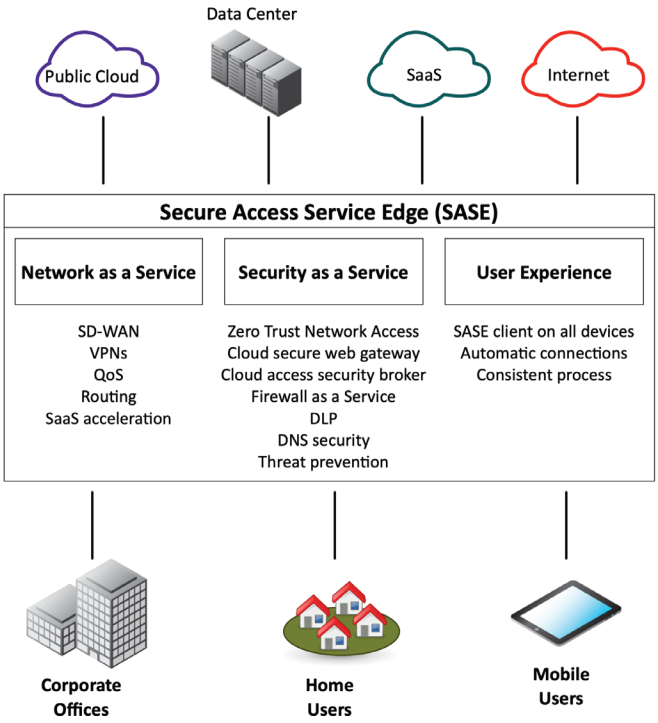
Authorization

- Authentication is complete
  - We can trust your identity
- Authorization process is also required
  - Determine which applications and data are accessible
- Different rights depending on the user
  - Help desk technicians can view the hardware database
  - Help desk managers can modify the database
  - Other users have no access
- Can include other criteria
  - Location, device certificate validation, time of day, etc.
  - Least privilege access
- 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

1.8 - Zero Trust (continued)

Secure Access Service Edge (SASE)

- Update secure access for cloud services
  - Securely connect from different locations
- Secure Access Service Edge (SASE)
  - A "next generation" VPN
- Security technologies are in the cloud
  - Located close to existing cloud services
- SASE clients on all devices
  - Streamlined and automatic



1.8 - Infrastructure as Code

Infrastructure as code (IaC)

- Describe an infrastructure
  - Define servers, network, and applications as definition files
- 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

Playbooks

- Conditional steps to follow; a broad process
  - Investigate a data breach, recover from ransomware
- Step-by-step set of processes and procedures
  - A reusable template
  - Can be used to create automated activities
- Often integrated with a SOAR platform
  - Security Orchestration, Automation, and Response
  - Integrate third-party tools and data sources

Automation use cases

- Configuration drift/compliance
  - Ensure the same configurations for all systems
  - The configuration used in testing should be the same in production
  - IaC provides an identical deployment
- Upgrades
  - Change a configuration with a single line of code
  - Modify configuration and software
- Dynamic inventories
  - Query devices in real-time
  - Manage and make changes based on the results

Source control

- Managing change
  - Developers create the infrastructure requirements
  - Build and publish the definition files
- Manage ongoing changes to the code
  - Version control system
  - Git is a popular example
- Track changes across multiple updates
  - A central repository
  - All changes are tracked and merged together
  - Everyone can participate without causing issues with the code

Controlling the source code

- Conflict identification
  - Some code can't be merged
  - Multiple versions could be modifying the same line of code
- Which one wins?
  - Might be determined automatically
  - May require manual intervention
- Branching
  - Move away from the main line of development
  - Work without making changes to the main code base
  - Branch and merge, branch and merge

1.8 - IPv6 Addressing

IPv4 address exhaustion

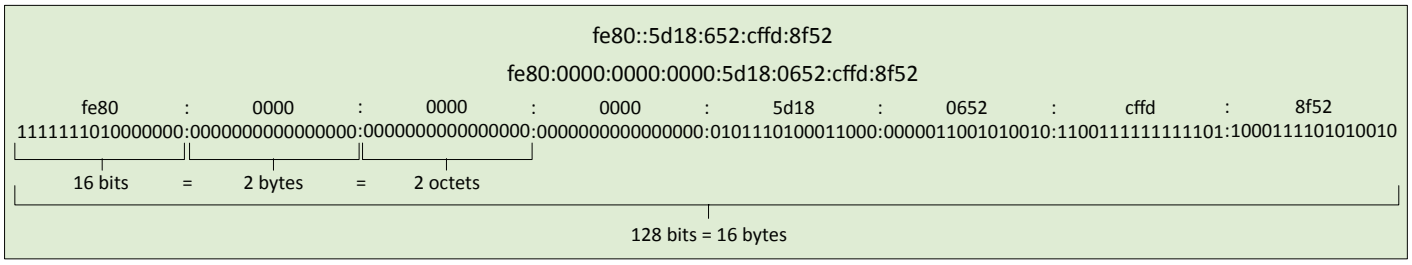
- There are an estimated 20 billion devices connected to the Internet (and growing)
  - IPv4 supports around 4.29 billion addresses
- The address space for IPv4 is exhausted
  - There are no available addresses to assign
- IPv4 and NAT is a workaround
  - Can be a challenge with certain protocols
- IPv6 provides a larger address space
  - With room for growth

IPv6 addresses

- Internet Protocol v6 - 128-bit address
  - 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (340 undecillion)
  - Each grain of sand on Earth could have 45 quintillion unique IPv6 addresses

IPv6 address compression

- Groups of zeros can be abbreviated with a double colon ::
  - Only one of these abbreviations allowed per address
- Leading zeros are optional



Communicating between IPv4 and IPv6

- Not all devices can talk IPv6
  - Legacy devices, embedded systems, etc.
  - How can an IPv4 device talk to an IPv6 server?
  - Can an IPv6 device communicate with a legacy IPv4 server?
- Requires an alternate form of communication
  - Tunnel - Encapsulate one protocol within another
  - Dual-stack - Have the option to use both IPv4 and IPv6
  - Translate and convert between IPv4 and IPv6
- Long-term goal should be a complete migration to IPv6

Tunneling IPv6

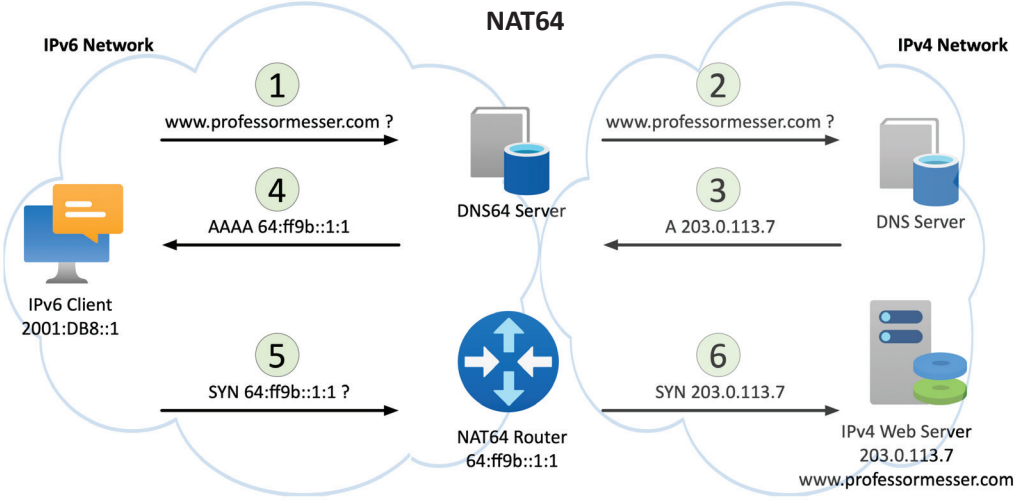
- A migration option - Designed for temporary use
- 6to4 addressing
  - Send IPv6 over an existing IPv4 network
  - Creates an IPv6 address based on the IPv4 address
  - Requires relay routers
  - No support for NAT
  - No longer available as an option in Windows
- 4in6 tunneling - Tunnel IPv4 traffic on an IPv6 network

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

Translating between IPv4 and IPv6

- Network address translation using NAT64
  - Translate between IPv4 and IPv6
  - Seamless to the end user
- Requires something in the middle to translate
  - IPv6 is not backwards compatible with IPv4
  - Use a NAT64-capable router
- Works with a DNS64 server - Translate the DNS requests



2.1 - Static and Dynamic Routing

Static routing

- Administratively define the routes
  - You're in control
- Advantages
  - Easy to configure and manage on smaller networks
  - No overhead from routing protocols (CPU, memory, bandwidth)
  - Easy to configure on stub networks (only one way out)
  - More secure - no routing protocols to analyze
- Disadvantages
  - Difficult to administer on larger networks
  - No automatic method to prevent routing loops
  - If there's a network change, you have to manually update the routes
  - No automatic rerouting if an outage occurs

Dynamic routing

- Routers send routes to other routers
  - Routing tables are updated in (almost) real-time
- Advantages
  - No manual route calculations or management
  - New routes are populated automatically
  - Very scalable
- Disadvantages
  - Some router overhead required (CPU, memory, bandwidth)
  - Requires some initial configuration to work properly

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 this 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?
  - A 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 protocols
- Standard or proprietary protocol?
  - OSPF and BGP are standards, some functions of EIGRP are Cisco proprietary

Enhanced Interior Gateway Routing Protocol

- EIGRP
  - Partly proprietary to Cisco
  - Commonly used on internal Cisco-routed networks
  - Relatively easy to enable and use
- Cleanly manage topology changes
  - Speed of convergence is always a concern
  - Loop free operation
- Minimize bandwidth use
  - Efficient discovery of neighbor routers

OSPF

- Open Shortest Path First
  - A common interior gateway protocol
  - Used within a single autonomous system (AS)
- A well-established standard
  - Available on routers from many different manufacturers
- Link-state protocol
  - Routing is based on the connectivity between routers
  - Each link has a "cost"
  - Throughput, reliability, round-trip time
  - Low cost and fastest path wins, identical costs are load balanced

BGP

- Exterior gateway protocol
  - A common interior gateway protocol
  - Used within a single autonomous system (AS)
- A popular standard - Used around the world for routing

2.1 - Routing Technologies

Routing Technologies

- Building a routing table
  - Routers are digital direction signs
  - How do I get to Google? Go that way.
- Every IP device has a routing table
  - Workstations, servers, routers, etc.
- The list of directions is the routing table
  - The most specific route "wins"
- Sometimes there's a tie
  - Duplicate destinations in the table
  - Which do you choose? There are ways to break the tie

Prefix lengths

- Most specific route "wins"
  - A combination of the subnet ID and prefix length
- Routes are more specific as the prefix increases
  - Router forwards traffic to the most specific destination
- Pick the best route to a server with the address of 192.168.1.6
  - 192.168.0.0/16
  - 192.168.1.0/24
  - 192.168.1.6/32

Route entries

```
R   10.10.30.0/24 [120/1] via 10.10.50.2, 00:00:14, Serial0/3/1
```

- R: Route Code
- 10.10.30.0/24: Subnet ID with Prefix Length
- 120: Administrative Distance
- 1: Metric
- 10.10.50.2: Next Hop
- 00:00:14: Route Timestamp
- Serial0/3/1: Outgoing Interface

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 trust the most?
- Administrative distances
  - Used by the router to determine which routing protocol has priority

Source	Administrative Distance
Local	0
Static route	1
EIGRP	90
OSPF	110
RIPv1 and RIPv2	120
DHCP default route	254
Unknown	255

Routing metrics

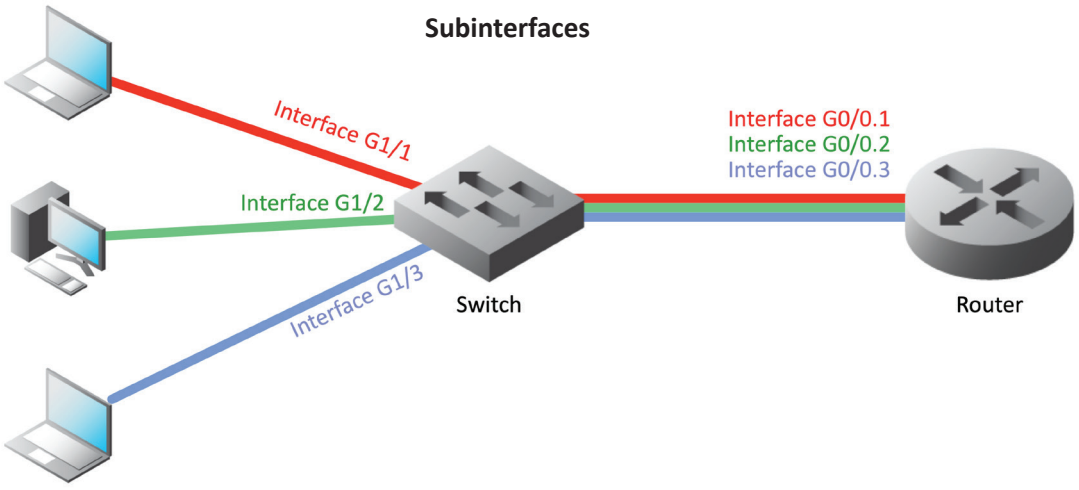
- Each routing protocol has its own way of calculating the best route
  - BGP, OSPF, EIGRP
- Metric values are assigned by the routing protocol
  - BGP metrics aren't useful to OSPF or EIGRP
- Use metrics to choose between redundant links
  - Choose the lowest metric, i.e., 1 is better than 2

First Hop Redundancy Protocol (FHRP)

- Your computer is configured with a single default gateway
  - We need a way to provide uptime if the default gateway fails
- The default router IP address isn't real
  - Devices use a virtual IP (VIP) for the default gateway
  - If a router disappears, another one takes its place
  - Data continues to flow
- Solves a shortcoming with IP addressing
  - One default gateway can really be many different routers

Subinterfaces

- A device has a physical interface
  - Configure options for each interface
- Some interfaces are not physical
  - VLANs in a trunk - These are subinterfaces
- Often referenced with the physical
  - Interface Ethernet1/1
  - Subinterface Ethernet1/1.10
  - Subinterface Ethernet 1/1.20
  - Subinterface Ethernet 1/1.100



2.1 - Network Address Translation

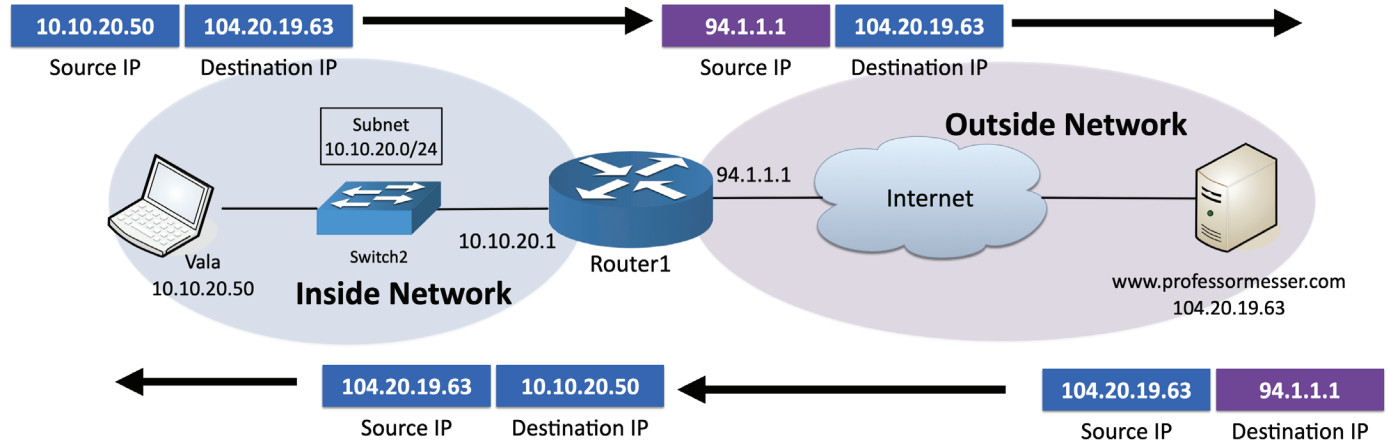
NAT (Network Address Translation)

- 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

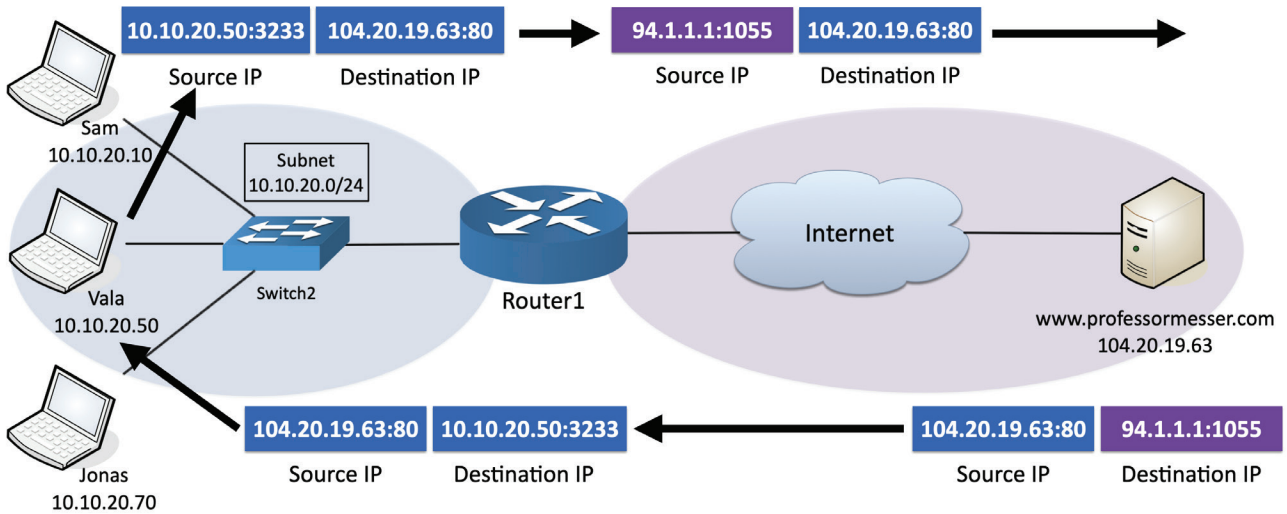
RFC 1918 Private IPv4 Addresses

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



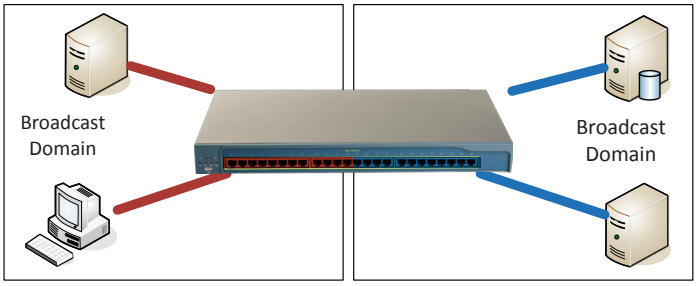
NAT Overload / Port Address Translation (PAT)



2.2 - VLANs and Trunking

LANs

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

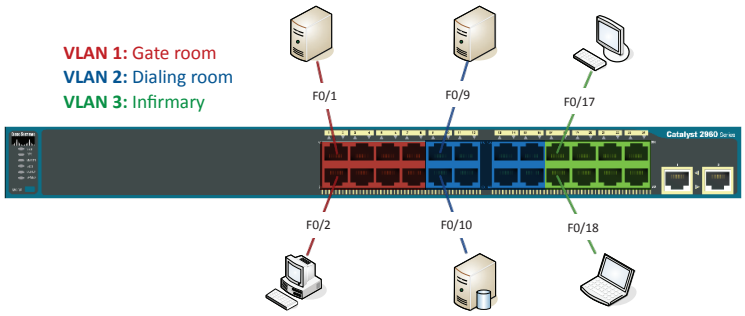


Virtual LANs

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

Configuring VLANs

- VLAN numbers and names are configured in the switch
  - The VLAN database



802.1Q trunking

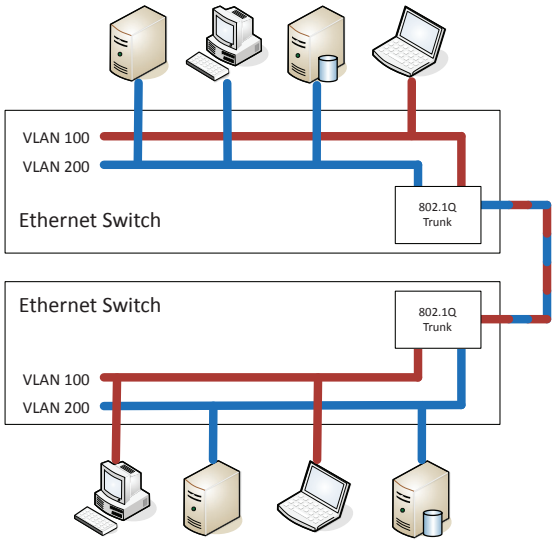
- Take a normal Ethernet frame

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



The native VLAN

- This is different than the "default VLAN"
  - The default VLAN is the VLAN assigned to an interface by default
- Each trunk has a native VLAN
  - The native VLAN doesn't add an 802.1Q header
- The native VLAN connects switches without a tag
  - Some devices won't talk 802.1Q
  - Just use the native VLAN!
- Native VLAN should match between switches
  - You'll get a message if the VLAN IDs don't match

Layer 3 switches

- A switch (Layer 2) and router (Layer 3) in the same physical device
  - 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
- The internal router connects to the VLANs over VLAN interfaces
  - Also called switched virtual interfaces (SVI)
- May need to enable routing on your switch
  - Will operate as an L2 device until enabled
  - May require a switch restart
- Doesn't replace a standalone router
  - Not all designs require extensive routing
  - You probably use a layer 3 switch at home

Configuring voice and data VLANs

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

2.2 - VLANs and Trunking (continued)

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
  - Data and voice cabling

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

2.2 - 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)

Link aggregation

- Port bonding / Link aggregation (LAG)
  - Multiple interfaces act like one big interface
- LACP
  - Link Aggregation Control Protocol
  - Adds additional automation and management

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

Jumbo frames

- Ethernet frames with more than
  - 1,500 bytes of payload
  - Up to 9,216 bytes of an MTU (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

2.2 - 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 - Wireless Technologies

Wireless technologies

- IEEE standards
  - 802.11 committee
  - Everyone follows these standards
- Also referenced as a generation
  - 802.11ac is Wi-Fi 5
  - 802.11ax is Wi-Fi 6 and Wi-Fi 6E
  - 802.11be is Wi-Fi 7
  - Future versions will increment accordingly

802.11 technologies

- Frequencies
  - 2.4 GHz, 5 GHz, and 6 GHz
  - Sometimes a combination
- Channels
  - Groups of frequencies, numbered by the IEEE
  - Using non-overlapping channels would be optimal
- Bandwidth
  - Amount of frequency in use
  - 20 MHz, 40 MHz, 80 MHz, 160 MHz

Band steering

- Many frequencies to choose from
  - Not all of them are optimal
- Some devices may only use one frequency
  - Older devices, specialized systems, etc.
- Other devices may have an choice
  - 2.4 GHz, 5 GHz, or 6 GHz
- Use band steering to direct clients to the best frequency
  - 2.4 GHz and 5 GHz without band steering = strongest frequency
  - 2.4 GHz and 5 GHz with band steering = 5 GHz connection

Regulatory impacts

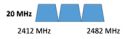
- Managing the wireless spectrum is a challenge
  - Individuals, companies, organizations, countries
- The world is constantly changing
  - Frequency allocations can be fluid
- Industry standards are also often worldwide standards
  - We all have to work together
- IEEE 802.11h standard
  - Add interoperability features to 802.11

The 802.11h standard

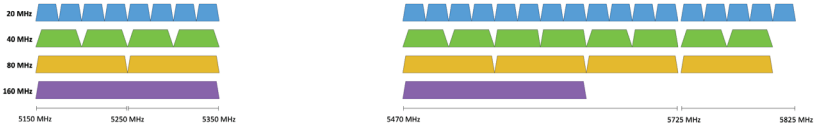
- 802.11 wireless complies with ITU guidelines
  - A worldwide approach
  - Now part of the 802.11 standard
- DFS (Dynamic Frequency Selection)
  - Avoid frequency conflict
  - Access point can switch to an unused frequency
  - Clients move with the access point
- TPC (Transmit Power Control)
  - Avoid conflict with satellite services
  - Access point determines power output of the client

2.3 - Wireless Technologies (continued)

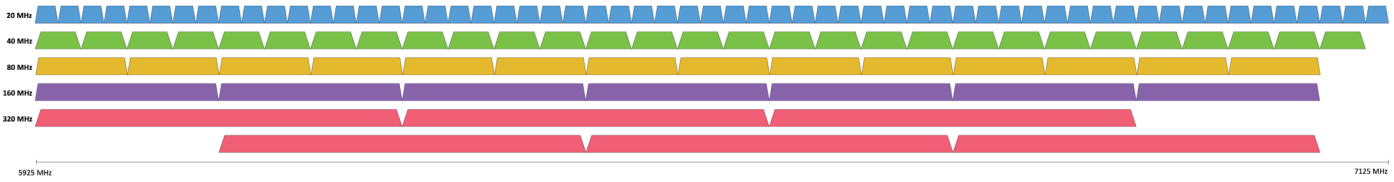
2.4 GHz Spectrum for 802.11 - North America



5 GHz Spectrum for 802.11 - North America



6 GHz Spectrum for 802.11 - North America



2.3 - Wireless Networking

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
  - 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

Wireless security modes

- Configure the authentication on your wireless access point / wireless router
- Open System
  - No authentication password is required
- WPA/2/3-Personal / WPA/2/3-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA/2/3-Enterprise / WPA/2/3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS, LDAP, etc.)

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

2.3 - Wireless Networking (continued)

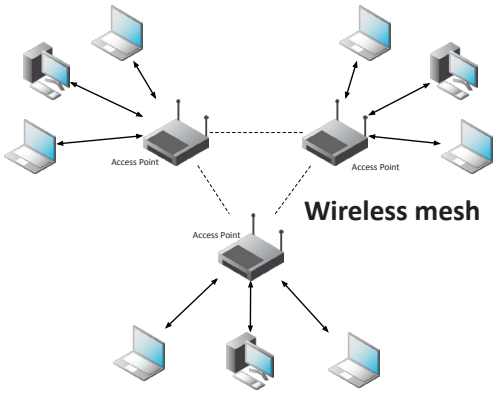
Directional antennas
- Focus the signal - Increased distances
- Send and receive in a single direction
  – Focused transmission and listening
- Antenna performance is measured in dB
  – Double power every 3dB of gain
- Yagi antenna - Very directional and high gain
- Parabolic antenna - Focus the signal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

Managing wireless configurations
- Autonomous access points
  – The access point handles most wireless tasks
  – The switch is not wireless-aware
- Lightweight access points
  – Just enough to be 802.11 wireless
  – The intelligence is in the switch - Less expensive
- Control and provision
  – CAPWAP is an RFC standard
  – Manage multiple access points simultaneously

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
  – The wireless controller is paired with the access points

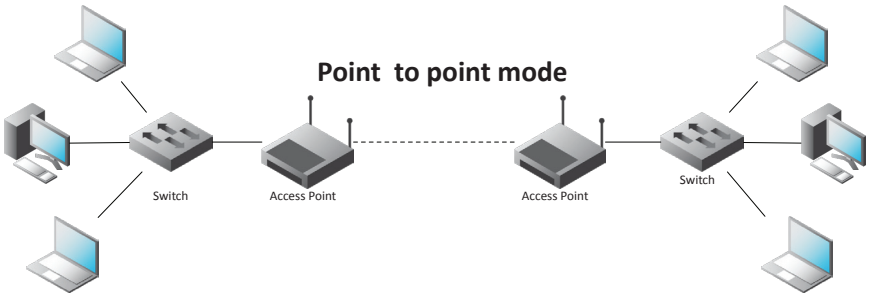
2.3 - Network Types

Wireless mesh
- Multiple access points
  – Access points bridge the gap
  – Clients across an extended distance can communicate with each other
- Ad hoc devices work together to form a mesh “cloud”
  – Self form and self heal

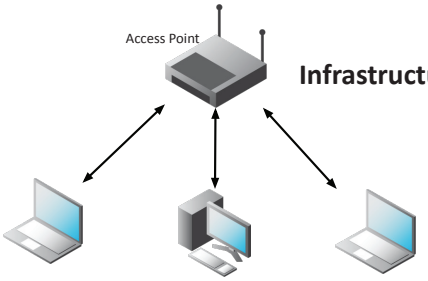


Ad hoc mode
- Ad hoc
  – Created for a particular purpose without any previous planning
  – Without an AP
- Two devices communicate directly to each other using 802.11
  – No access point required
  – Independent basic service set (IBSS)
- Temporary or long-term communication
  – Connect to a device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

Point to point mode
- Connect two access points together
  – Extend a wired network over a distance
  – Building to building
  – Site to site
- May require specialized wireless equipment
  – Outdoor antennas and access points
  – Power adjustments
  – Frequency options



Infrastructure mode
- Clients communicate to an access point
  – Access point forwards traffic
- Clients can communicate to a wired network
  – Access point bridges the networks
- Clients can communicate to each other
  – If the access point allows



2.3 - 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

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)

2.4 - Installing Networks

Installing Networks
- 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

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

Equipment racks
- Rack sizes
  - 19" rack/device width
- Height measured in rack units
  - 1U is 1.75"
  - A common rack height is 42U
- Depth can vary
  - Often determined by the equipment
- Plan and locate
  - Devices follow standard sizing

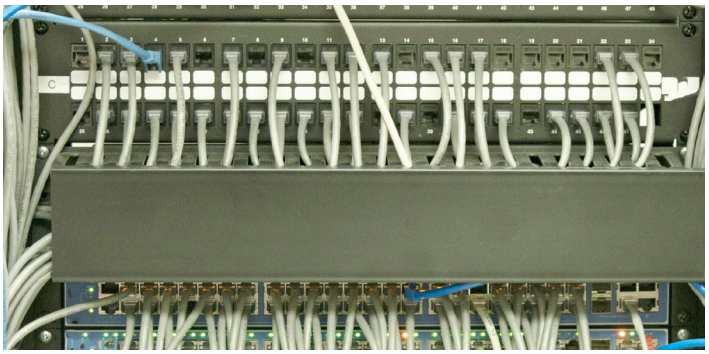
Cooling a data center
- Heating, Ventilating, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- Data centers optimize cooling
  - Separate aisles for heating and cooling
- Heat intake and exhaust is important
  - Front, back, or side

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

2.4 - Installing Networks (continued)

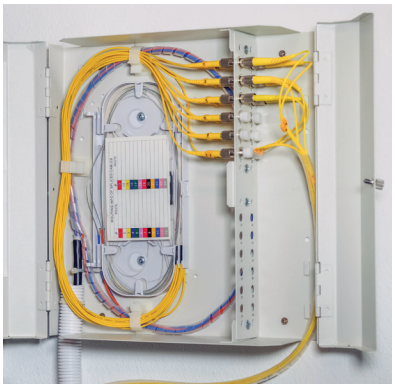
Copper patch panel

- 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



2.4 - Power

WARNING

- Always disconnect from the power source when working on a device
  - Always. Seriously.
- Some devices store a charge in capacitors
  - Know how to discharge before touching
- Never connect your body to any part of an electrical system
  - Do not connect yourself to the ground wire of an electrical system
- Respect electricity
  - It does not respect you

Amp and volt

- Ampere (amp, A) – The rate of electron flow past a point in one second
  - The diameter of the hose
- Voltage (volt, V)
  - Electrical "pressure" pushing the electrons
  - How open the faucet is
  - 120 volts, 240 volts

Watt

- Watt (W)
  - How much energy is being consumed?
  - Electrical load is measured in watts
- Easy to calculate volts * amps = watts
  - 120 V * 0.5 A = 60 W

Current

- Alternating current (AC)
  - Direction of current constantly reverses
  - Distributes electricity efficiently over long distances
- Frequency of this cycle is important
  - US/Canada – 110 to 120 volts of AC (VAC), 60 hertz (Hz)
  - Europe – 220-240 VAC, 50 Hz
- Direct current (DC)
  - Current moves in one direction with a constant voltage

Device power supplies

- Devices commonly use DC voltage
  - Most power sources provide AC voltage
- Convert 120 V AC or 240 V AC
  - To DC voltages
- You'll know when this isn't working
  - An important component

UPS

- Uninterruptible Power Supply
  - Short-term backup power
  - Blackouts, brownouts, surges
- Common UPS types
  - Offline/Standby UPS
  - Line-interactive UPS
  - On-line/Double-conversion 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

2.4 - Environmental Factors

Humidity

- We use a lot of power for data centers
  - One estimate is nearly 2% of all U.S. power consumption
- Humidity level
  - High humidity promotes condensation
  - Low humidity promotes static discharge
- Industry guidelines for data centers
  - Somewhere around 40% to 60% humidity
  - Specific settings vary on location and equipment type

Temperature

- Electrical equipment has an optimal operating temperature
  - Usually part of the device specifications
  - Industry best practices are around 64°to 81° F
- Many external influences
  - Outdoor temperature
  - Temperature increases as system load increases
- HVAC is used to manage temperature and humidity
  - Sensors are placed in strategic locations

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

3.1 - Network Documentation

Physical network maps

- Follows the physical wire and device
  - Can include physical rack locations

Logical network maps

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

Rack diagrams

- A network admin might never walk into the data center
  - Physical access is often limited
- Provide documentation for installation or changes
  - A picture is worth a thousand words
- Detailed digram of rack components
  - Often listed by physical location of the rack (row 3, rack W)
  - Each rack unit (U) is documented

Cable maps and diagrams

- The foundation of the network
  - Physical cable and fiber
- Valuable documentation
  - Planning the installation
  - Numbering each network drop
  - Troubleshooting after installation
- An OSI Layer 1 representation
  - The physical layer

Asset management

- A record of every asset
  - Laptops, desktops, servers, routers, switches, cables, fiber modules, tablets, etc.
- Associate support tickets with a device make and model
  - A record of hardware and software
- Financial records, audits, depreciation
  - Make/model, configuration, purchase date, location, etc.
- Add an asset tag
  - Barcode, RFID, visible tracking number, organization name

Asset database

- A central asset tracking system
  - Used by different parts of the organization
- Assigned users
  - Associate a person with an asset
  - Useful for tracking a system
- Warranty
  - A different process if out of warranty
- Licensing
  - Software costs
  - Ongoing renewal deadlines

IP Address Management (IPAM)

- Manage IP addressing
  - Plan, track, configure DHCP
- Report on IP address usage
  - Time of day, user-to-IP mapping
- Control DHCP reservations
  - Identify problems and shortages
- Manage IPv4 and IPv6
  - One console

3.1 - Network Documentation (continued)

Service level agreement (SLA)
- Minimum terms for services provided
  - Uptime, response time agreement, etc.
  - Commonly used between customers and service providers
- Contract with an Internet provider
  - SLA is no more than four hours of unscheduled downtime
  - Technician will be dispatched
  - May require customer to keep spare equipment on-site

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

3.1 - Life Cycle Management

Life Cycle Management
- End-of-life
  - End of life (EOL)
  - Manufacturer stops supporting the hardware
  - May continue to provide security patches and updates
  - May provide warranty repair
- End of support (EOS)
  - Manufacturer stops updating a product
  - Current version is the final version
  - No ongoing security patches or updates
- Technology EOS is a significant concern
  - Security patches are part of normal operation

Patches and bug fixes
- 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

Operating system updates
- Many and varied
  - Windows, Linux, iOS, Android, et al.
- Updates
  - Operating system updates/service packs, security patches
- User accounts
  - Minimum password lengths and complexity
  - Account limitations
- Network access and security
  - Limit network access
- Monitor and secure
  - Anti-virus, anti-malware

Firmware management
- The software inside of the hardware
  - The operating system of the hardware device
- 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
- Trane Comfortlink II thermostats
  - Control the temperature from your phone
  - Trane notified of three vulnerabilities in April 2014
  - Two patched in April 2015, one in January 2016

Decommissioning
- Managing asset disposal
  - Desktops, laptops, tablets, mobile devices
  - Sanitize media or destroy
- May be 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

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
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

3.1 - Configuration Management

Configuration management
- The only constant is change
  - Operating systems, patches, application updates, network modifications, new application instances, etc.
- Identify and document hardware and software settings
  - Manage the security when changes occur
- Rebuild those systems if a disaster occurs
  - Documentation and processes will be critical

Production configuration
- The most current running configuration
  - Everyone uses this config
- Covers all aspects of the configuration
  - Hardware devices and firmware versions
  - Device driver versions
  - Application software updates
- Usually tested before installation
  - This must work properly
  - Not everything can be tested
  - Plan for the unforeseen issues

Backup configuration
- There always needs to be a backup
  - Not everything works as expected
- Create a backup before making a change
  - Revert to the backup if problems occur
  - Copy files, create a snapshot of a VM, etc.
- Problems during the change
  - Easily go back to the previous production configuration
- Problems after the change
  - Future issues can be rolled back

Baseline/golden configuration
- An application environment should be well defined
  - All application instances must follow this baseline
  - Firewall settings, patch levels, OS file versions
  - May require constant updates
- Integrity measurements check for the secure baseline
  - These should be performed often
  - Check against well-documented baselines
  - Failure requires an immediate correction

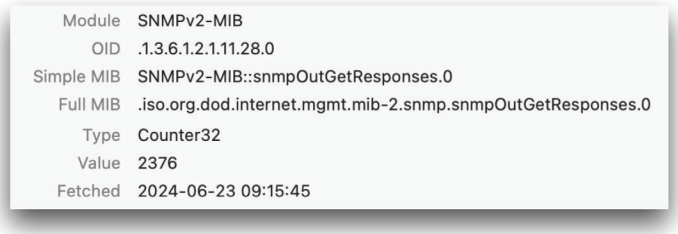
3.2 - SNMP

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 v2c – 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).snmpOutGetResponses(28).0
  - .1.3.6.1.2.1.11.28.0
- 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

Authentication
- Community string
  - A simple password-style authentication method
  - Read-only, read-write, and trap
  - Common community strings are public and private
  - Used with SNMP v1 and SNMP v2c
- Username and password
  - Used in SNMP v3
  - Transmitted as a password hash



3.2 - Logs and Monitoring

Logs and monitoring
- The network never sleeps
  - 24/7/365
- Monitor all important points
  - Routers, switches, firewalls, services, remote access, authentication logs, etc.
- React to events
  - Account access, redundant devices, bandwidths
- Status dashboards
  - Get the status of all systems at a glance

Flow data
- 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

Protocol analyzers
- Solve complex application issues
  - Get into the details
- Gathers frames on the network
  - Or in the air
  - Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Large scale storage - Big data analytics

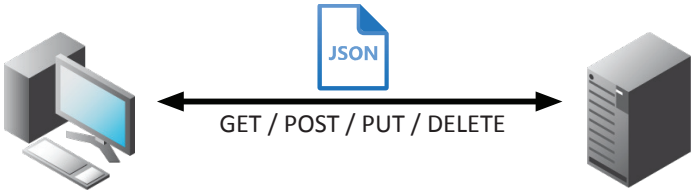
Network performance baseline
- Troubleshooting starts with a blank slate
  - A baseline can add context
- Intermittent or all-day issues
  - Check utilization, individual device performance, etc.
- Some organizations already collect this data
  - Check the SIEM or management console
- Look for patterns and correlation
  - Alarm and alert when anomalies occur

Syslog
- Standard for message logging
  - Diverse systems create a consolidated log
- Usually a central logging collector
  - Integrated into the SIEM (Security Information and Event Manager)
- Each log entry is labeled
  - Facility code (program that created the log) and severity level
- Common with most devices
  - Firewalls, switches, routers, servers, etc.

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
  - Data is sent to the SIEM using syslog
  - Operating systems
  - Infrastructure devices
  - NetFlow sensors
- Sensitivity settings
  - Easy to be overwhelmed with data
  - Some information is unnecessary
  - Informational, Warning, Urgent

API integration
- Control and manage devices
  - Hundreds of firewalls, routers, switches, and servers
  - Log in to each device and make changes manually
- Automate the command line
  - Batch processes
  - Very little control or error handling



- Application programming interfaces (APIs)
  - Interact with third-party devices and services
  - Cloud services, firewalls, operating systems
  - Talk their language

Port mirroring
- Copy traffic from one or more interfaces
  - Used for packet captures, IDS, performance monitoring
- Mirror traffic on the same switch
  - Mirror traffic from one switch to another
  - Gather data from a remote switch

3.2 - Network Solutions

Network discovery
- Difficult to see beyond the wall jack
  - LLDP (Link Layer Discovery Protocol),
  - CDP (Cisco Discovery Protocol), etc.
  - IP scanners (Nmap)
  - Commercial network scanners
  - SNMP
- Ad hoc
  - Scan as needed or required
- Scheduled
  - Scan occurs at regular intervals
  - Report on moves, adds, and changes

Traffic analysis
- 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

Performance monitoring
- 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

Availability monitoring
- Up or down
  - The most important statistic
  - No special rights or permissions required
  - Green is good, red is bad
- Alarming and alerting
  - Notification should an interface fail to report
  - Email, SMS
- Short-term and long-term reporting
  - View availability over time
  - Not focused on additional details
  - Additional monitoring may require SNMP

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

Configuration monitoring
- Ten identical web servers
  - Should have ten identical configurations
  - How to confirm?
- Monitor the configurations
  - Verify consistency
  - Alert on any changes
  - Backup and restore
- Often part of a larger management system or strategy
  - Central console and access

3.3 - Disaster Recovery

Disaster recovery plan (DRP)
- Detailed plan for resuming operations after a disaster
  - Application, data center, building, campus, region, etc.
- Extensive planning prior to the disaster
  - Backups
  - Off-site data replication
  - Cloud alternatives
  - Remote site
- Many third-party options
  - Physical locations
  - Recovery services

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

3.3 - Disaster Recovery (continued)

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

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

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

Tabletop exercises
- Performing a full-scale disaster drill can be costly
  - And time consuming
- Many of the logistics can be determined through analysis
  - You don't physically have to go through a disaster or drill
- Get key players together for a tabletop exercise
  - Talk through a simulated disaster

Validation tests
- Test yourselves before an actual event
  - Scheduled update sessions (annual, semi-annual, etc.)
- Use well-defined rules of engagement
  - Do not touch the production systems
- Very specific scenario - Limited time to run the event
- Evaluate response - Document and discuss

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

3.4 - DHCP

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

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

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: Acknowledgment** - DHCP Server to client
  - DHCP server sends an acknowledgment to the client

3.4 - Configuring DHCP

Scope properties
- IP address range - and excluded addresses
- Subnet mask
- Lease durations
- Other scope options
  - DNS server
  - Default gateway
  - VOIP servers

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 exclusions 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 assignment
  - Similar to dynamic allocation
  - DHCP server keeps a list of past assignments
  - You'll always get the same IP address

Address reservation
- Address reservation
  - Administratively configured
- Table of MAC addresses
  - Each MAC address has a matching IP address
- Other names
  - Static DHCP Assignment, Static DHCP, IP Reservation

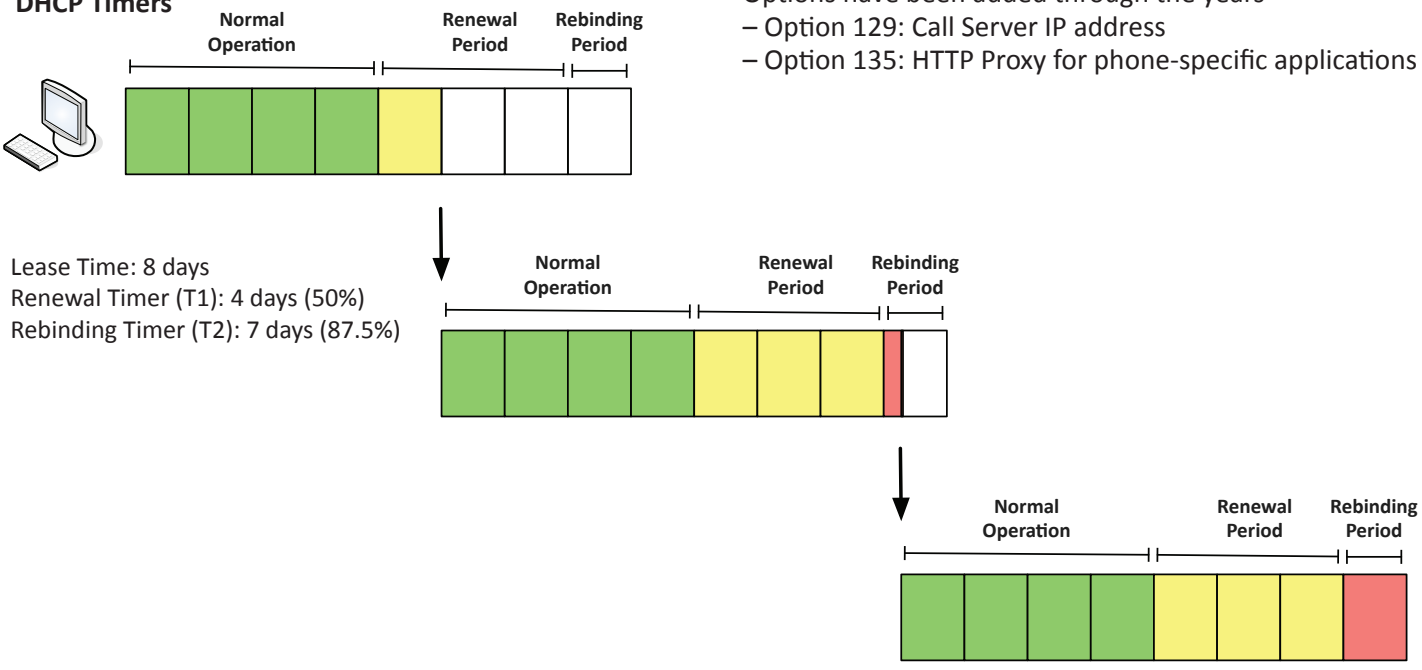
DHCP leases
- Leasing your address
  - It's only temporary - but it can seem permanent
- Allocation
  - Assigned a lease time by the DHCP server
  - Administratively configured
- Reallocation
  - Reboot your computer
  - Confirms the lease
- Workstation can also manually release the IP address
  - Moving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

The DHCP lease process

DHCP options
- A special field in the DHCP message
  - Many, many options
- Options are part of the DHCP RFC
  - BOOTP called them "vendor extensions"
- 256 (254 usable) options
  - 0 through 255 - 0 is pad, 255 is end
- Many common options
  - Subnet mask, domain name server, domain name, etc.
- Options are configured on the DHCP server
  - Not all DHCP servers support option configuration
- Options have been added through the years
  - Option 129: Call Server IP address
  - Option 135: HTTP Proxy for phone-specific applications

DHCP Timers



3.4 - IPv6 and SLAAC

Automatic IP addressing in IPv6

- DHCP servers
  - Similar process as IPv4
  - Requires redundant DHCP servers
  - Ongoing administration
- Stateless addressing
  - No separate server keeping the state
  - No tracking of IP or MAC addresses
  - Lease times don't exist

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, prefix length, DNS server, etc.

SLAAC (Stateless Address Autoconfiguration)

- Determine the IP prefix using NDP (Neighbor Discovery Protocol)
  - Router Solicitation (RS) and Router Advertisement (RA)
- Use the IP Prefix with a modified EUI-64 address (or randomize)
  - Put them together to make a complete IPv6 address
  - Before using, use NDP's DAD (Duplicate Address Detection)
  - Just to be sure you're the only one with the IPv6 address

3.4 - An Overview of DNS

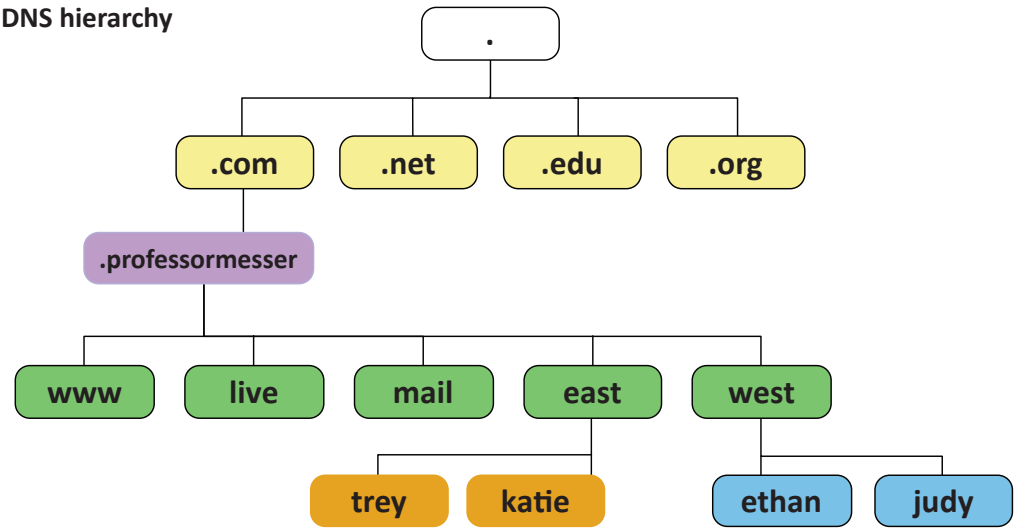
Domain Name System

- 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.

Primary and secondary DNS servers

- DNS is an important service
  - Internet, Active Directory, application access
  - Redundant servers are commonly used
- Primary DNS server
  - Contains all of the zone information for a domain
  - Changes and updates are made to the primary server
- Secondary DNS server
  - Zone information is read-only
  - Zone transfers are pushed from the primary DNS server
- The primary/secondary updates are invisible to the end user

The DNS hierarchy

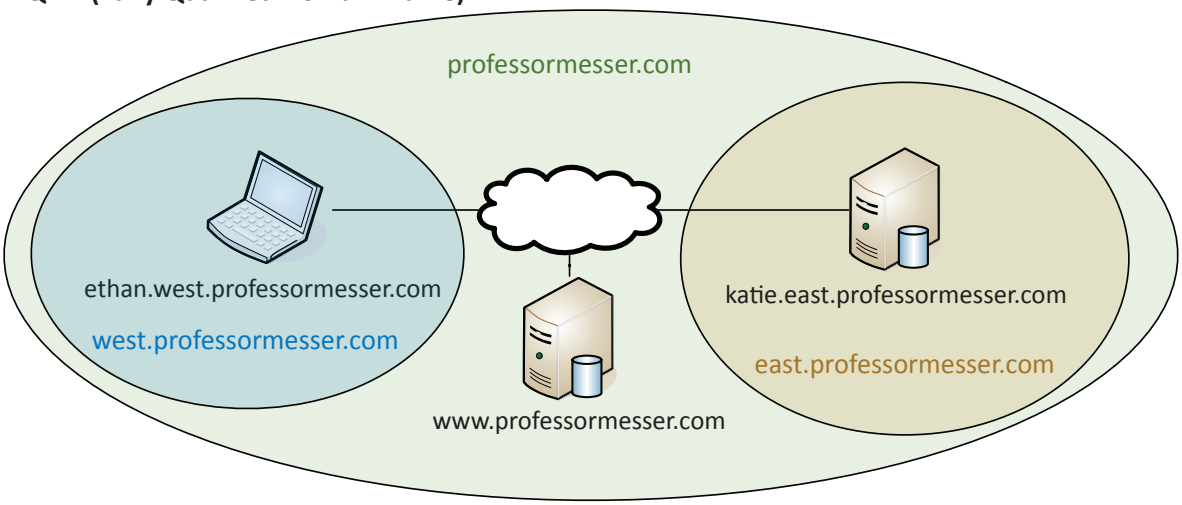


3.4 - An Overview of DNS (continued)

Local name resolution
- You might need to override the DNS server
  - Access a test server
  - DNS server might be configured incorrectly
- Hosts file
  - Contains a list of IP addresses and host names
  - These are the preferred resolutions
- Some apps may not use the hosts file
  - Check the browser or app docs

Lookups
- Forward lookup
  - Provides the DNS server with an FQDN
  - DNS server responds with an IP address
- Reverse DNS
  - Provides the DNS server with an IP address
  - The DNS server responds with an FQDN

FQDN (Fully Qualified Domain Name)



The authority
- Authoritative
  - The DNS server is the authority for the zone
- Non-authoritative
  - Does not contain the zone source files
  - Probably cached information
- TTL (time to live)
  - Configured on the authoritative server
  - Specifies how long a cache is valid
  - A very long TTL can cause problems if changes are made

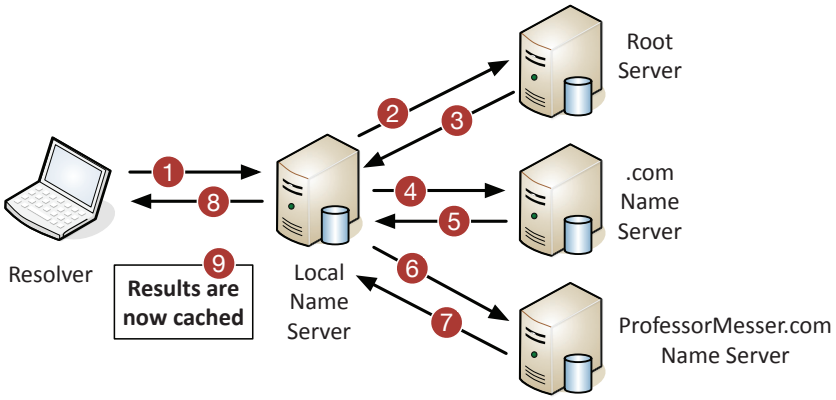
Recursive DNS queries
- Recursive query
  - Delegate the lookup to a DNS server
- The DNS server does the work and reports back
  - Large DNS cache provides a speed advantage
- Future queries use the local cache
  - Cache entries eventually timeout and are removed
  - Securing DNS
- DNS is often transmitted in the clear
  - No built-in encryption
  - Relatively easy to spoof
  - Redirect email to a different mail server
- Domain Name Security Extensions (DNSSEC)
  - DNS responses from the server are digitally signed
  - A forgery would be easily identified
  - Requires additional configurations on the DNS server

Encrypting DNS
- DNS requests and responses are sent in the clear
  - Anyone can view the traffic
  - Security and privacy concerns
- DNS over TLS (DoT)
  - Send DNS traffic over tcp/853, but encrypt with TLS/SSL
- DNS over HTTPS (DoH)
  - Send DNS traffic in an HTTPS packet
  - Looks like a web server communication over tcp/443
  - Some browsers use DoH by default

3.4 - An Overview of DNS (continued)

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



3.4 - DNS Records

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 example.com.  postmaster.example.com. (
      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
    chat     IN CNAME    mail.example.com.
    ftp      IN CNAME    mail.example.com.
    www      IN CNAME    mail.example.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.example.com.

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

; A list of machine names & addresses
    jack.mydomain.name.     IN A    123.12.41.40    ; Windows 10
    mail.mydomain.name.     IN A    123.12.41.41    ; Linux (main server)
    sam.mydomain.name.      IN A    123.12.41.42    ; Windows 11
```

3.4 - DNS Records (continued)

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")
```

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.
```

3.4 - Time Protocols

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 commonly measured in the tens of milliseconds

NTP clients and servers

- NTP server
  - Listens on udp/123, responds 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?

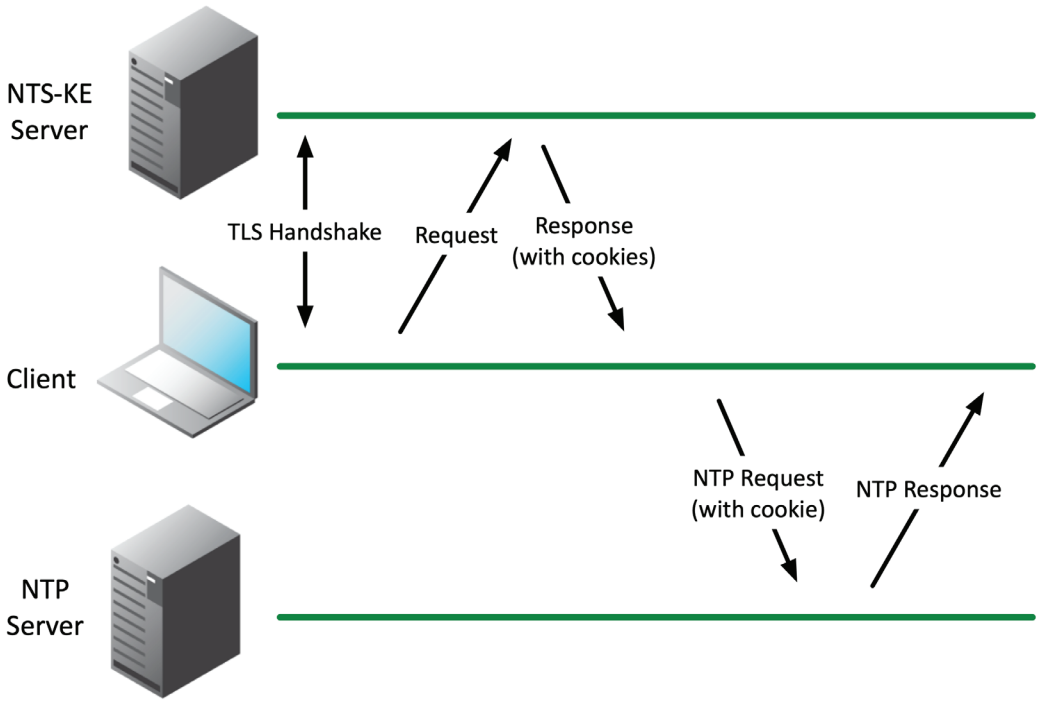
Network Time Security (NTS)

- NTP sends traffic in the clear
  - The time of day isn't really a secret
- The wrong time can be a significant problem
  - How do you know your NTP server response can be trusted?
- NTP is updated to provide authentication
  - NTP information can be trusted
- TLS handshake is used for key exchange
  - Get authorization cookie from an NTS key exchange server
- Connect to an NTP server using this authentication
  - Both requests and responses are validated

Precision Time Protocol (PTP)

- A more precise time protocol
  - A hardware-based time synchronization
- Nanosecond granularity
  - Important for industrial applications, financial trading, etc.
- Often implemented as specialized hardware
  - Avoids delays from the operating system and applications

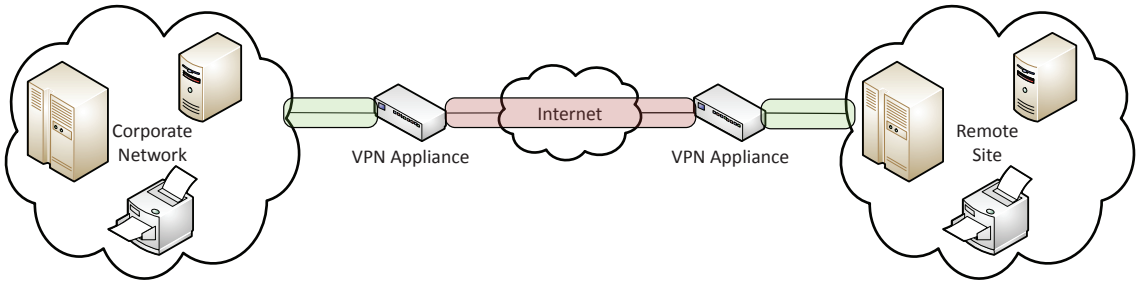
Network Time Security (NTS)



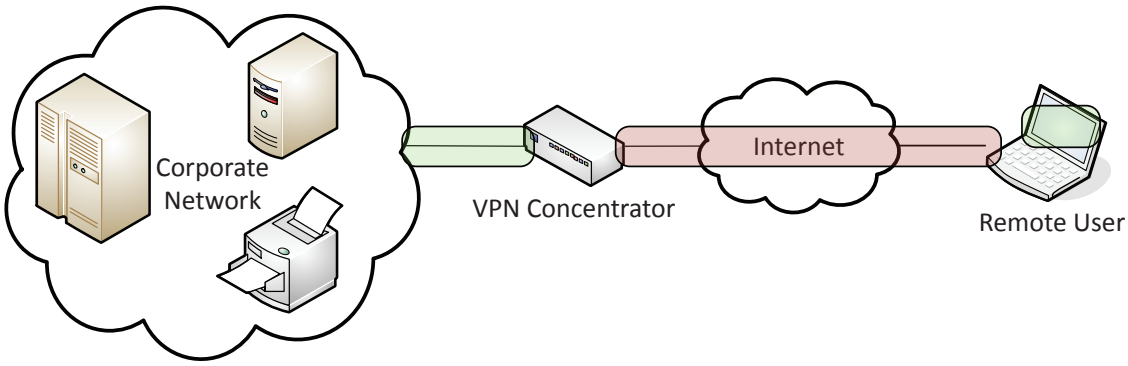
3.5 - VPNs

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



Client-to-Site VPNs
- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on



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

Split tunnel vs. full tunnel
- Full tunnel
  - All traffic is sent through the VPN tunnel
  - The client makes no additional forwarding decisions
  - May require additional routing at the concentrator
- Split tunnel
  - VPN traffic is sent through the tunnel
  - Non-VPN traffic is sent normally
  - Configured in the VPN software

3.5 - Remote Access

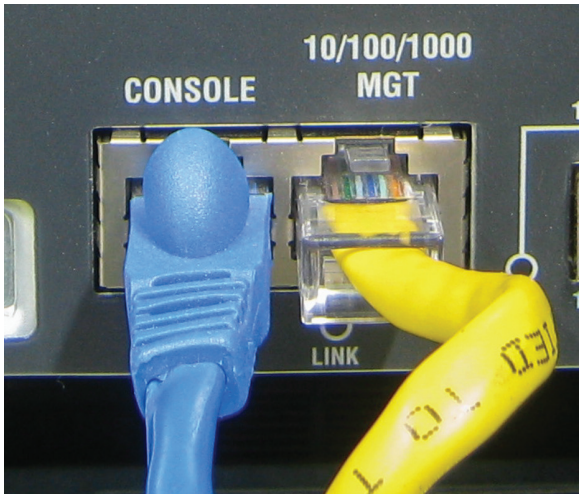
SSH (Secure Shell)
- Encrypted console communication - tcp/22
- Looks and acts the same as Telnet - tcp/23

Graphical user interface (GUI)
- 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

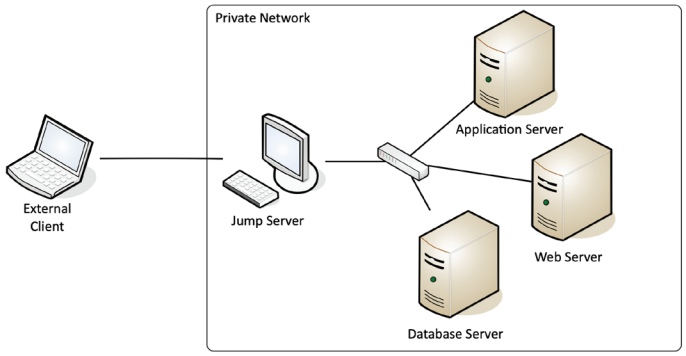
API integration
- Control and manage devices
  - Hundreds of firewalls, routers, switches, and servers
  - Log in to each device and make changes manually
- Automate the command line
  - Batch processes
  - Very little control or error handling
- Application programming interfaces (APIs)
  - Interact with third-party devices and services
  - Cloud services, firewalls, operating systems
  - Talk their language

Console
- Directly connect to the device
  - Traditionally a serial connection
  - DB9 connector, RJ45 serial, USB connection
- When all else fails
  - The console will be available
- A text-based serial interface
  - The console
- Requires a serial or USB connection
  - May need a USB to DB9 serial adapter

Out-of-band and in-band management



Jump box
- Access secure network zones
  - Provides an access mechanism to a protected network
- Highly-secured device
  - Hardened and monitored
- SSH / Tunnel / VPN to the jump server
  - RDP, SSH, or jump from there
- A significant security concern
  - Compromise of the jump server is a significant breach



In-band management
- Assign an IP address to a device
  - Switch, router, firewall, etc.
- May be a separate Ethernet interface
  - Often marked on the device
- May be accessible from any connected device
  - The IP address is inside the device
- Access the device
  - SSH
  - Browser-based console

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 to manage
  - Or Cable, DSL, satellite, etc.
- Console router / comm server
  - Out-of-band access for multiple devices
  - Connect to the console router, then choose where you want to go

4.1 - Security Concepts

Data in transit
- Data transmitted over the network
  - Also called data in-motion
- Not much protection as it travels
  - Many different switches, routers, devices
- Network-based protection
  - Firewall, IPS
- Provide transport encryption
  - TLS (Transport Layer Security)
  - IPsec (Internet Protocol Security)

Data at rest
- The data is on a storage device
  - Hard drive, SSD, flash drive, etc.
- Encrypt the data
  - Whole disk encryption
  - Database encryption
  - File- or folder-level encryption
- Apply permissions
  - Access control lists
  - Only authorized users can access the data

Public Key Infrastructure (PKI)
- Policies, procedures, hardware, software, people
  - Digital certificates: create, distribute, manage, store, revoke
- This is a big, big, endeavor
  - Lots of planning
- Also refers to the binding of public keys to people or devices
  - The certificate authority
  - It's all about trust

Digital certificates
- A public key certificate
  - Binds a public key with a digital signature
  - And other details about the key holder
- A digital signature adds trust
  - PKI uses Certificate Authorities for additional trust
  - Web of Trust adds other users for additional trust
- Certificate creation can be built into the OS
  - Part of Windows Domain services
  - Many 3rd-party options

Certificate Authorities
- You connect to a random website
  - Do you trust it?
- Need a good way to trust an unknown entity
  - Use a trusted third-party
  - An authority
- Certificate Authority (CA) has digitally signed the website certificate
  - You trust the CA, therefore you trust the website
  - Real-time verification

Self-signed certificates
- Internal certificates don't need to be signed by a public CA
  - Your company is the only one going to use it
  - No need to purchase trust for devices that already trust you
- Build your own CA
  - Issue your own certificates signed by your own CA
- Install the CA certificate/trusted chain on all devices
  - They'll now trust any certificates signed by your internal CA
  - Works exactly like a certificate you purchased

Identity and Access Management (IAM)
- Applications are available anywhere
  - Desktop, browser, mobile device, etc.
- Data can be located anywhere
  - Cloud storage, private data centers, etc.
- Many different application users
  - Employees, vendors, contractors, customers
- Give the right permissions to the right people at the right time
  - Prevent unauthorized access
- Identify lifecycle management
  - Every entity (human and non-human) gets a digital identity
- Access control
  - An entity only gets access to what they need
- Authentication and authorization
  - Entities must prove they are who they claim to be
- Identity governance
  - Track an entity's resource access
  - May be a regulatory requirement

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

4.1 - Security Concepts (continued)

Geographic restrictions
- Network location
  - Identify based on IP subnet
  - Can be difficult with mobile devices
- Geolocation - determine a user's location
  - GPS - mobile devices, very accurate
  - 802.11 wireless, less accurate
  - IP address, not very accurate
- Geofencing
  - Automatically allow or restrict access when the user is in a particular location
  - Don't allow this app to run unless you're near the office

Cameras
- CCTV (Closed circuit television) - Can replace physical guards
- Camera features are important
  - Motion recognition can alarm and alert when something moves
  - Object detection can identify a license plate, a person's face, or a type of animal
- Often many different cameras
  - Networked together and recorded over time

Door locks
- Conventional - Lock and key
- Deadbolt - Physical bolt
- Electronic - Keyless, PIN
- Token-based - RFID badge, magnetic swipe card, or key fob
- Biometric - Hand, fingers or retina
- Multi-factor - Smart card and PIN

4.1 - Authentication

AAA framework
- Identification
  - This is who you claim to be
  - Usually your username
- Authentication
  - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

Single sign-on (SSO)
- Provide credentials one time
  - Get access to all available or assigned resources
  - No additional authentication required
- Usually limited by time
  - A single authentication can work for 24 hours
  - Authenticate again after the timer expires
- The underlying authentication infrastructure must support SSO
  - Not always an option

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

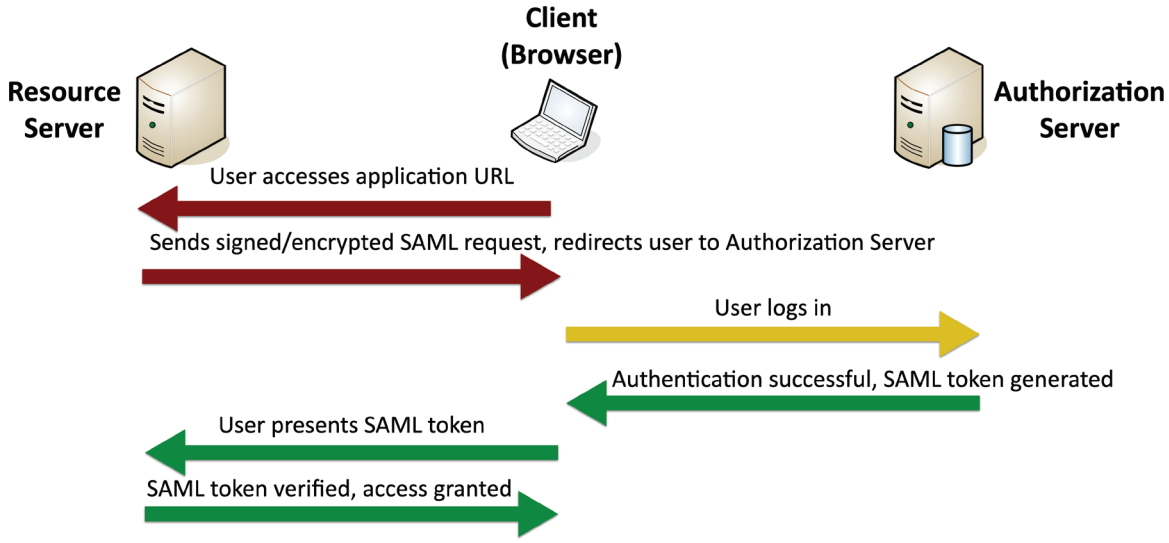
LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, Novell eDirectory, etc.

X.500 Distinguished Names
- Attribute=value pairs
- Most specific attribute is listed first
  - This may be similar to the way you already think

X.500 Directory Information Tree
- Hierarchical structure
  - Builds a tree
- Container objects
  - Country, organization, organizational units
- Leaf objects
  - Users, computers, printers, files

4.1 - Authentication (continued)

Security Assertion Markup Language (SAML)
- Open standard for authentication and authorization
  - You can authenticate through a third-party to gain access
  - One standard does it all, sort of
- Not originally designed for mobile apps
  - This has been SAML's largest roadblock



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

Multifactor authentication
- Prove who you are
  - Use different methods
  - A memorized password
  - A mobile app
  - Your GPS location
- Factors
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are
- There are other factors as well

TOTP
- Time-based One-Time Password algorithm
  - Use a secret key and the time of day
  - No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOTP code
- One of the more common OTP methods
  - Used by Google, Facebook, Microsoft, etc.

4.1 - Security Technologies

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
  - Most are open source and available to download
- Constant battle to discern the real from the fake

Honeynets
- A real network includes more than a single device
  - Servers, workstations, routers, switches, firewalls
- Honeynets
  - Build a larger deception network with one or more honeypots
- More than one source of information
  - Stop spammers - https://projecthoneypot.org

4.1 - Security Technologies (continued)

Risk
- An exposure to harm or danger
  - The possibility of something bad happening
- An important consideration
  - Growth brings risk
  - It's useful to get ahead of any potential problems
- Most things have an associated risk
  - Manage potential risk
  - Qualify internal and external threats
  - Risk analysis helps plan for contingencies

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

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

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

The CIA Triad
- Combination of principles
  - The fundamentals of security
  - Sometimes referenced as the AIC Triad
- 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

4.1 - Regulatory Compliance

Compliance
- Compliance
  - Meeting the standards of laws, policies, and regulations
- A healthy catalog of regulations and laws
  - Across many aspects of business and life
  - Many are industry-specific or situational
- Penalties
  - Fines, incarceration, loss of employment
- Scope
  - Covers national, territory, or state laws
  - Domestic and international requirements

Data localization
- Data from a region or country is stored within the borders of that region or country
  - Data collected in Vegas stays in Vegas
- Laws may prohibit where data is stored
  - GDPR (General Data Protection Regulation)
  - A complex mesh of technology and legalities
- Where is your data stored?
  - Compliance laws may prohibit moving data out of the country

GDPR - General Data Protection Regulation
- European Union regulation
  - Data protection and privacy for individuals in the EU
  - Name, address, photo, email address, bank details, posts on social networking websites, medical information, a computer's IP address, etc.
- Controls personal data
  - Data collected on EU citizens must be stored in the EU
  - Users can decide where their data goes
  - Can request removal of data from search engines
- Gives "data subjects" control of their personal data
  - A right to be forgotten

PCI DSS
- Payment Card Industry Data Security Standard (PCI DSS)
  - A standard for protecting credit cards
- Six control objectives
  - Build and maintain a secure network and systems
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

4.1 - Segmentation Enforcement

Segmenting the network
- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation (PCI compliance)
  - Makes change control much easier

IoT (Internet of Things)
- Sensors - Heating and cooling, lighting
- Smart devices - Home automation, video doorbells
- Wearable technology - Watches, health monitors
- Weak defaults
  - IOT manufacturers are not security professionals

IIoT (Industrial Internet of Things)
- IoT for companies - Machine to machine communication
- Segmentation is just as important
  - More data is at stake
- Facility automation - Temperature, air quality, lighting
- Industrial equipment/ICS monitoring
  - Oil and gas, robotics, medical devices
  - Specialized monitoring systems
  - Wired and wireless connectivity

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

Operational Technology (OT)
- The hardware and software for industrial equipment
  - Electric grids, traffic control, manufacturing plants, etc.
- This is more than a web server failing
  - Power grid drops offline
  - All traffic lights are green
  - Manufacturing plant shuts down
- Requires a different approach
  - A much more critical security posture

Guest networks
- A network for visitors
  - No access to the private network
  - Separate wireless network
  - For guests only
- Controlled access
  - Password or captive portal
- Firewalled from the rest of the network
  - Internet access only

BYOD
- Bring Your Own Device
  - Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- A challenge to secure
  - Segment the device from the internal network
  - It's both a home device and a work device

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)

Distributed Denial of Service (DDoS)

- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the attackers have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim

DDoS reflection and amplification

- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common network DDoS technique
  - Turn Internet services against the victim
- Uses protocols with little (if any) authentication or checks
  - NTP, DNS, ICMP
  - A common example of protocol abuse

4.2 - VLAN Hopping

VLAN hopping

- Define different VLANs
  - Organizational, network engineering, security
- You only have access to your VLAN
  - Good security best practice
- "Hop" to another VLAN
  - This shouldn't happen
- Two primary methods
  - Switch spoofing
  - Double tagging

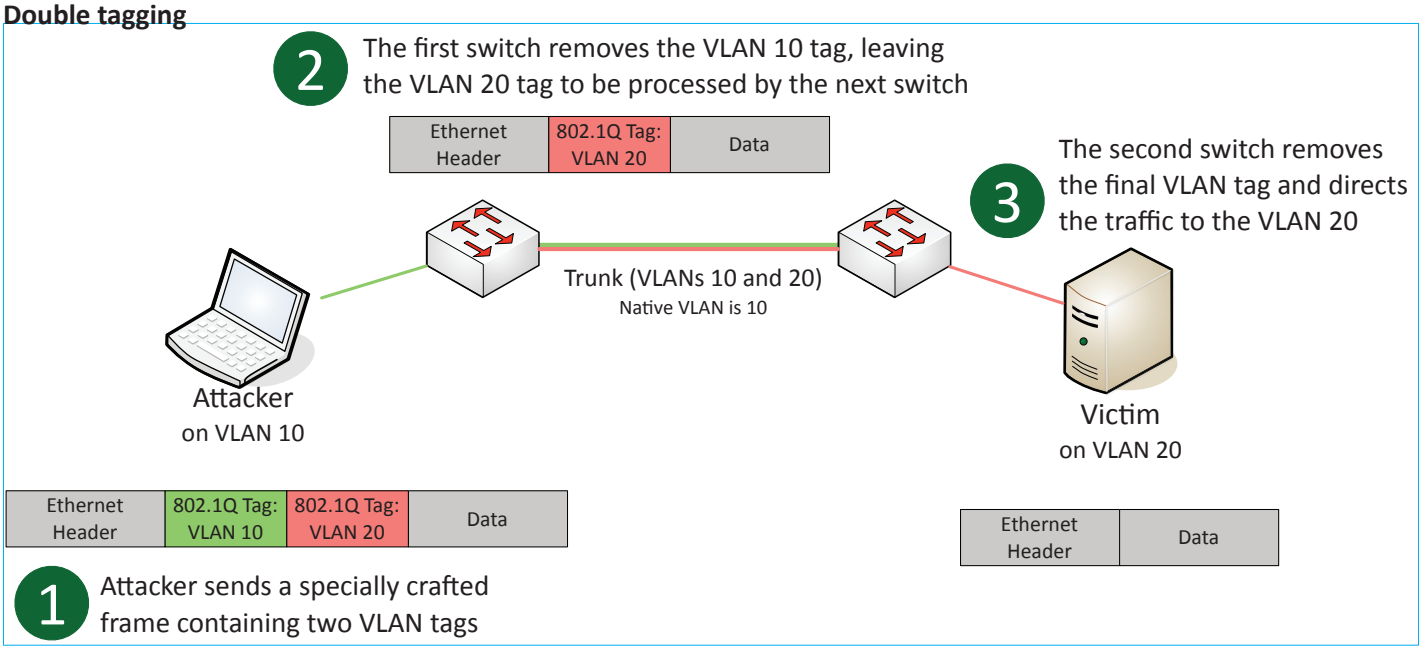
Switch spoofing

- 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

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
  - Good for DoS
- Don't put any devices on the native VLAN
  - Change the native VLAN ID
  - Force tagging of the native VLAN

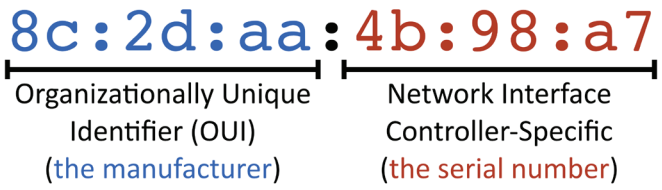
Double tagging



4.2 - MAC Flooding

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



LAN switching

- 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
  - These age out periodically, often in 5 minutes
- 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

MAC flooding

- The MAC table is only so big
  - Attacker starts sending traffic with different source MAC addresses
  - Force out the legitimate MAC addresses
- The table fills up
  - Switch begins flooding traffic to all interfaces
- This effectively turns the switch into a hub
  - All traffic is transmitted to all interfaces
  - No interruption in traffic flows
- Attacker can easily capture all network traffic!
- Flooding can be restricted in the switch's port security settings

4.2 - ARP and DNS Poisoning

Spoofing and poisoning

- 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

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

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

4.2 - Rogue Services (continued)

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 VPN

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
  - On-path attack on the local IP subnet
  - ARP has no security

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 - 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
- Usually there's something not quite right
  - Spelling, fonts, graphics

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

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?

Dumpster diving
- Mobile garbage bin
  - United States brand name "Dumpster"
  - Similar to a rubbish skip
- Important information thrown out with the trash
  - Thanks for bagging your garbage for me!
- Gather details that can be used for a different attack
  - Impersonate names, use phone numbers
- Timing is important
  - Just after end of month, end of quarter
  - Based on pickup schedule

4.2 - Social Engineering (continued)

Is it legal to dive in a dumpster?
- I am not a lawyer.
- In the United States, it's legal
  - Unless there's a local restriction
- If it's in the trash, it's open season
  - Nobody owns it
- Dumpsters on private property or
  - "No Trespassing" signs may be restricted
  - You can't break the law to get to the rubbish
  - Questions? Talk to a legal professional.

Protect your rubbish
- Secure your garbage
  - Fence and a lock
- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Go look at your trash
  - What's in there?

4.2 - Malware

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
- Worms
- Ransomware
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Bloatware
- Logic bomb

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

Your data is valuable
- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth? There's a number

4.3 - Device Security

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 access point or router
  - http://www.routerpasswords.com

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

4.3 - Device Security

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

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

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

Key management system

- Services are everywhere
  - On-premises, cloud-based
  - Many different keys for many different services
- Manage all keys from a centralized manager
  - Often provided as third-party software
  - Separate the encryption keys from the data
- All key management from one console
  - Create keys for a specific service or cloud provider (SSL/TLS, SSH, etc.)
  - Associate keys with specific users
  - Rotate keys on regular intervals
  - Log key use and important events

4.3 - Security Rules

Access control lists (ACLs)

- Allow or disallow traffic
  - 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
- Can be implemented in many ways
  - Router, firewall, operating system policies, etc.

Firewall rules

- A logical path
  - Usually top-to-bottom
- Can be very general or very specific
  - Specific rules are usually at the top
- Implicit deny
  - Most firewalls include a deny at the bottom
  - Even if you didn't put one

Sample firewall ruleset

Rule Number	Remote IP	Remote Port	Local Port	Protocol	Action
1	All	Any	22	TCP	Allow
2	All	Any	80	TCP	Allow
3	All	Any	443	TCP	Allow
4	All	Any	3389	TCP	Allow
5	All	53	Any	UDP	Allow
6	All	123	Any	UDP	Allow
7	All			ICMP	Deny

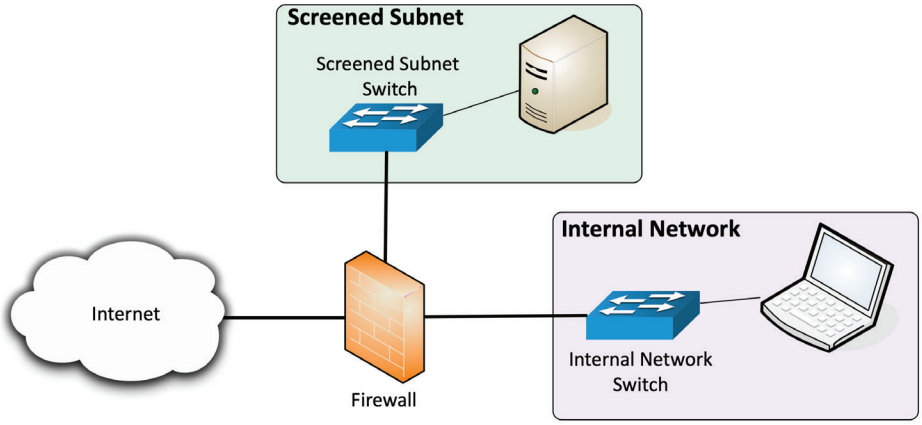
4.3 - Security Rules (continued)

URL filtering
- Allow or restrict based on Uniform Resource Locator
  - Also called a Uniform Resource Identifier (URI)
  - Allow list / Block list
- Managed by category
  - Auction, Hacking, Malware,
  - Travel, Recreation, etc.
- Can have limited control
  - URLs aren't the only way to surf
- Often integrated into an NGFW
  - Filters traffic based on category or specific URL

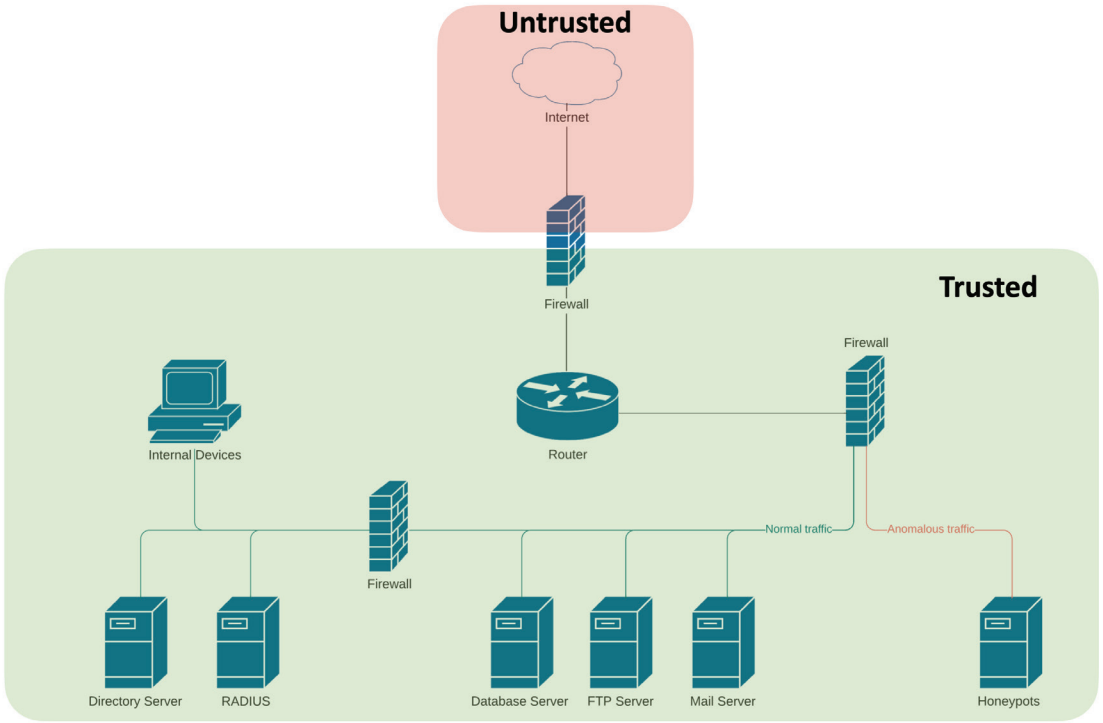
Content filtering
- Control traffic based on data within the content
  - URL filtering, website category filtering
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work
  - Parental controls
- Protection against evil
  - Anti-virus, anti-malware

Screened subnet
- An additional layer of security between you and the Internet
  - Public access to public resources
  - Private data remains inaccessible

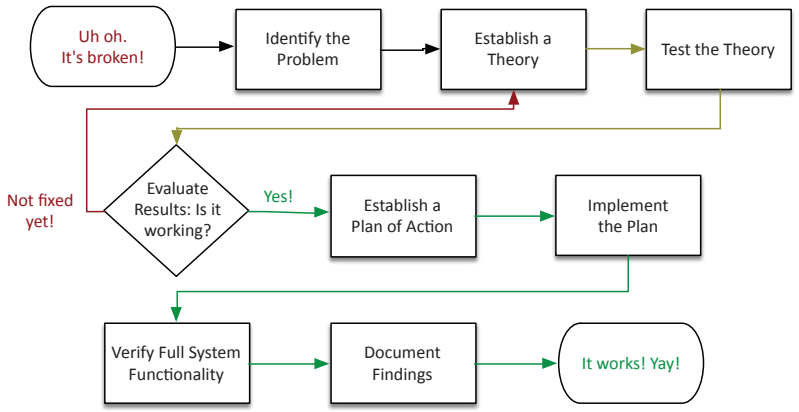
Security zones
- Zone-based security technologies
  - More flexible (and secure) than IP address ranges
- Each area of the network is associated with a zone
  - Trusted, untrusted / Internal, external
  - Inside, Internet, Servers, Databases, Screened
- This simplifies security policies
  - Trusted to Untrusted
  - Untrusted to Screened
  - Untrusted to Trusted



Trusted and untrusted security zones



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

Identify the problem
- Gather information
  - – Get as many details as possible
  - – Duplicate the issue, if possible
- Question users - Your best source of details
- Identify symptoms
  - – May be more than a single symptom
- Determine if anything has changed
  - – Who's in the wiring closet?
- Duplicate the problem, if possible
  - – The issue is much easier to troubleshoot if you can see it happening
- Approach multiple problems individually
  - – Break problems into smaller pieces
  - – Establish a theory of probable cause
- Start with the obvious - Occam's razor applies
- Consider everything
  - – Even the not-so-obvious
  - – Examine the problem from the top of the OSI model to the bottom
  - – And then from the bottom to the top
- Divide and conquer
  - – Break the problem into smaller pieces
  - – Remove the pieces that don't apply

Test the theory
- Confirm the theory
  - – Determine next steps to resolve problem
- Theory didn't work?
  - – Re-establish new theory or escalate
  - – Call an expert

Create a plan of action
- Build the plan
  - – Correct the issue with a minimum of impact
  - – Some issues can't be resolved during production hours
- Identify potential effects
  - – Every plan can go bad
  - – Have a plan B
  - – And a plan C

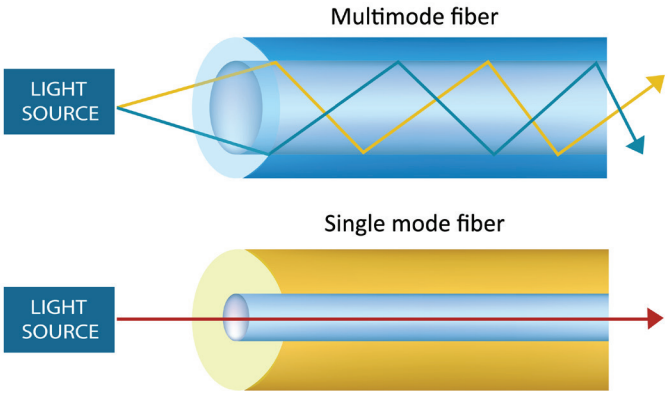
Implement the solution
- Try the fix
  - – Implement during the change control window
- Escalate as necessary
  - – You may need help from a 3rd party

Verify full system functionality
- It's not fixed until it's really fixed
  - – The test should be part of your plan
  - – Have your customer confirm the fix
- Implement preventive measures
  - – Let's avoid this issue in the future

Document findings
- It's not over until you update the knowledge base
  - – Important lessons were learned
  - – Don't lose valuable knowledge!
- Consider a formal database
  - – Help desk case notes
  - – Searchable database

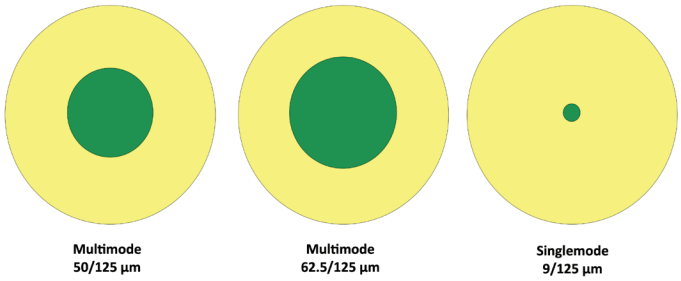
Troubleshooting a network
- Identify the problem:
  - – Information gathering, identify symptoms, question users, determine if anything has changed
- Establish a theory of probable cause
  - – Question the obvious
- Test the theory to determine cause
  - – Once theory is confirmed determine next steps to resolve problem.
  - – If theory is not confirmed, re-establish new theory or escalate.
- 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 Issues



Fiber mismatching

- Core and cladding sizes are relatively standard
  - Fiber and frequencies must match equipment
  - Signal errors will be seen on the interface



Cable categories

- Cable construction is standardized
  - Telecommunications Industry Association (TIA)
- TIA sets the minimum physical cable parameters
  - Cables meeting the standard are assigned a category (cat)
  - Insertion loss, near end crosstalk, far end crosstalk, etc.
- IEEE networking standards refer to the TIA cable categories
  - 1000BASE-T minimum cable is category 5
  - 10GBASE-T minimum cable is category 6 and 6A

Cable categories by Ethernet standard

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

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.

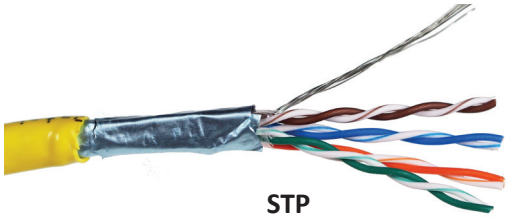
The right cable category

- Validate the cable
  - Use best practices during installation
  - Tester matches to the closest cable category
- Cable should meet the minimum requirements
  - Physical errors will increase error counts
  - Signal attenuation, loss of signal, CRC errors

Unshielded and shielded cable

- UTP (Unshielded Twisted Pair)
  - No additional metal 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

UTP
Unshielded Twisted Pair



STP
Shielded Twisted Pair

Crosstalk (XT)

- Signal on one circuit affects another circuit
  - In a bad way
- Leaking of signal
  - You can sometimes hear the leak
- Measure XT with cable testers
  - Some training may be required

5.2 - Cable Issues (continued)

Crosstalk metrics
- Near End Crosstalk (NEXT)
  - Interference measured at the transmitting end
  - The near end
- Far End Crosstalk (FEXT)
  - Interference measured at away from the transmitter
- Alien Crosstalk (AXT)
  - Interference from other cables
- Attenuation to Crosstalk Ratio (ACR)
  - Difference between insertion loss and NEXT
  - Signal-to-Noise Ratio (SNR)

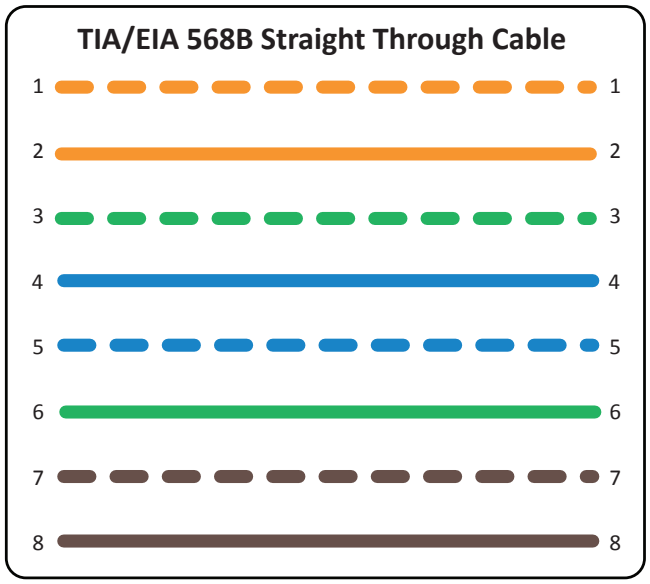
Troubleshooting crosstalk
- Almost always a wiring issue
  - Check your crimp
- Maintain your twists
  - The twist helps to avoid crosstalk
- Category 6A increases cable diameter
  - Increased distance between pairs
- Test your installation
  - Solve problems before they are problems

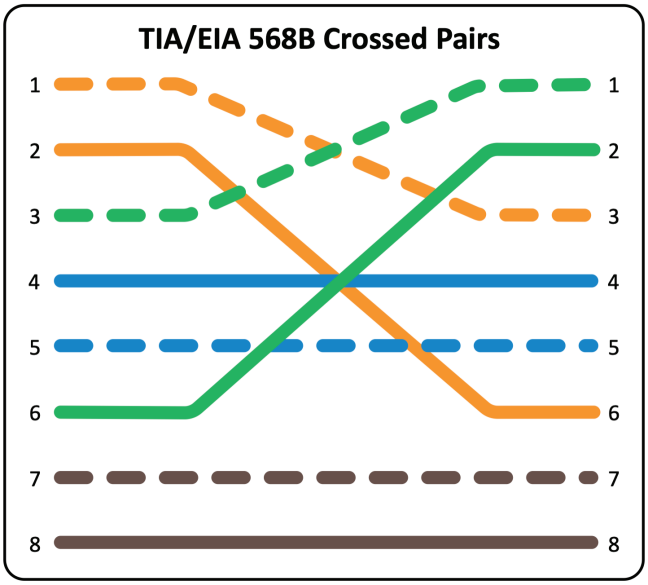
Avoiding EMI and interference
- Electromagnetic interference
- Cable handling
  - No twisting - don't pull or stretch
  - Watch your bend radius
  - Don't use staples, watch your cable ties
- EMI and interference with copper cables
  - Avoid power cords, fluorescent lights, electrical systems, and fire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

Attenuation
- Usually gradual
  - Signal strength diminishes over distance
  - Loss of signal intensity as signal moves through a medium
- Happens across all mediums
  - Electrical signals through copper
  - Light through fiber
  - Radio waves through the air

Troubleshooting termination
- 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
  - Improper termination
- 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

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)
  - Don't rely on this functionality





5.2 - Interface Issues

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
- Utilization
  - Per-interface network usage
  - Run bandwidth tests to view throughput
- Error rate
  - Problems with the signal
  - CRC errors, runts, giants, drops

Counting the errors

- CRC (Cyclic Redundancy Check) error detecting
  - Add a frame check sequence to an Ethernet frame
  - Receive the frame, recalculate the CRC, and compare to the original
  - Non-matching CRC is an error
- Runts - Frames that are less than 64 bytes
  - May be a result of a collision
- Giants - Frames that are more than 1518 bytes
  - Or more than the configured maximum frame size
- Drops
  - Frames not transmitted or received due to contention

Error disabled

- Some problems should be stopped in their tracks
  - They go on and on
- Disable the interface to fix the symptom
  - This does not fix the problem
- Many different reasons
  - Link flapping (up/down), port security violations, duplex mismatch, etc.
- Must be administratively re-enabled
  - Intervention is required

Port status

- Administratively down
  - The device admin has “turned off” an interface
  - This was intentional
  - Does not work again until administratively enabled
- Suspended
  - The configuration is not compatible with the current connection
  - This is similar in function to “error disabled,” but occurs immediately
  - Set LACP (Link Aggregation Control Protocol) on one side, but not the other

Error counts

```
5 minute output rate 2000 bits/sec, 2 packets/sec
     5701 packets input, 1157662 bytes, 0 no buffer
     Received 5130 broadcasts (2269 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 2269 multicast, 0 pause input
     0 input packets with dribble condition detected
     600 packets output, 71161 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The Ethernet frame

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

5.2 - Hardware Issues

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

PoE, PoE+, PoE++
- PoE
  - The original PoE specification
  - 15.4 watts DC power, 350 mA max current
- PoE+
  - 25.5 watts DC power, 600 mA max current
- PoE++
  - 51 W (Type 3), 600 mA max current
  - 71.3 W (Type 4), 960 mA max current
  - PoE with 10GBASE-T
- Compare the device with the switch support
  - PoE+ won't power a PoE++ device

PoE switch
- Power over Ethernet interfaces
  - Commonly marked on the switch or interfaces
- Check switch for total PoE power supported
  - "Up to 600 W"
  - Calculate the device requirements for the power budget

Single mode vs. multimode
- 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

Transceiver signal strength
- Devices must receive enough signal
  - Can't work if the signal isn't strong enough
- Each device has a sensitivity level
  - Some devices can "hear" better than others
- Calculate the power budget
  - Determine transmitter power (often measured in dBm)
  - Calculate signal loss based on distance, connectors, splices, etc.
  - Subtract signal loss from the transmitter power
  - Compare to minimum receive power

5.3 - Switching Issues

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)

Spanning Tree Protocol (STP)
- Bridges are always talking to each other
  - Uses MAC-layer multicasts (01:80:C2:00:00:00)
  - Bridge Protocol Data Unit (BPDU)
  - Sends configuration and any topology changes
- Default "hello" interval is 2 seconds
  - Miss three of those, and the link is considered down

Root bridge selection
- When starting, the bridges elect a root bridge
  - All other bridges choose the best connection to the root
- All bridges/switches are assigned a bridge ID between 0 and 61440
  - If there's a tie, the lowest
  - MAC address number wins
- Each bridge assigns a port role to each interface
  - Root, designated, or blocked

STP port states
- Blocking/Discarding
  - 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

5.3 - Switching Issues (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 - A quick fix

ACLs break perfectly good networks
- Clients are working
  - DHCP is assigning correct IP addresses
  - Routing tables look correct
- Packets are still dropping
- Everything could be configured perfectly
  - ACLs would still break the traffic flow
- Always include an ACL check when troubleshooting
  - Save lots of time

ACL best practices
- More granular rules should be first
  - Very similar to a firewall
  - The ACL stops evaluating after a match
  - Broader rules at the top would prevent more specific rules from firing
- Best practice: Before editing an ACL, disable on an interface
  - Adding an access list without any rules will filter all traffic
  - ACLs deny all by default

5.3 - Routing and IP Issues

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

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

Gateway of last resort
- Destination IP has to match a routing table entry
  - If not, it's dropped
- Adding a static default route can simplify your routing table
  - If it doesn't match an entry, use this route
- Add in global router configuration
  - Create a route to 0.0.0.0/0

Address pool exhaustion
- 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

Troubleshooting IP configurations
- Check your documentation
  - IP address, subnet mask, default gateway
  - Confirm these settings!
- Monitor the traffic
  - 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

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?

5.4 - Performance Issues

Congestion

- The network is a finite resource
  - 1000BASE-T is one gigabit per second
  - It can't go any faster
- A busy network may attempt to send 2 gigabits per second
  - Contention brings packet queueing, buffering, etc.
- There are only so many resources
  - Buffers will fill - Some data may be dropped
- Increase the size of the road- Or decrease the number of cars

Bottlenecks

- There's never just one performance metric
  - A series of technologies working together
- I/O bus, CPU speed, storage access speed,
  - WAN bandwidth, local network speeds, 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

Bandwidth usage

- The fundamental network statistic
  - Amount of network use over time
- Throughput
  - The amount of data successfully transferred through the network
- Many different ways to monitor
  - SNMP, NetFlow, sFlow, IPFIX protocol analysis, software agent
- Throughput capacity
  - Total throughput has a maximum value
  - Based on the slowest link

Latency

- A delay between the request and the response
  - Waiting time
- Some latency is expected and normal
  - Laws of physics always 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

Packet loss

- Discards, packet drops
  - No errors in the packet, but system could not transmit or receive the data
- Packets are lost
  - Corrupted during transmission
  - Dropped after validation
- Data must be retransmitted
  - Overall communication is delayed
  - Uses additional resources

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

5.4 - Wireless Issues

Wireless interference

- 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
  - Nearby access points using the same frequencies would cause problems
- Most access points can monitor frequency usage
  - Can move automatically to unused space
  - Manual configuration is an option

Managing channel usage

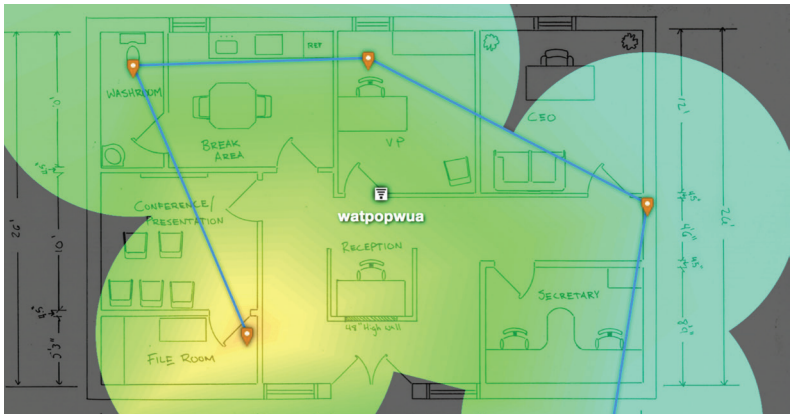
- Disable legacy, low speed support
  - Use the fastest possible speeds and configurations
- Check your channels
  - Avoid overlap between access points
- Adjust the output power
  - Avoid conflicts with other access points
  - Interference can steal valuable network time
- Split the network - You might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

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

5.4 - Wireless Issues (continued)

Insufficient wireless coverage
- 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



Client disassociation issues
- A denial of service attack
  - Takes advantage of older
  - 802.11 management frame transmission
- Device keeps dropping from the wireless network
  - Or never connects
- Disassociation 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

Roaming misconfiguration
- A wireless network often has a single name
  - SSID (Service Set Identifier)
  - Appears as one big wireless network
- There might be multiple access points supporting an SSID
  - Extend the network
- Users will move to the best access point
  - These must have identical configurations
  - Users will be dropped if configurations differ

5.5 - Software Tools

Protocol analyzers
- Solve complex application issues - Get into the details
- Gathers frames on the network
  - Or in the air / Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Large scale storage - Big data analytics

Nmap
- Network mapper
  - Find and learn more about network devices
- Port scan - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device? Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE) - extend capabilities, vulnerability scans
- Active - scan for IP addresses and open ports
  - And operating systems, services, etc.
- Pick a range of IP addresses - See who responds to the scan
- Visually map the network
  - Gather information on each device
  - IP, operating system, services, etc.
- Rogue system detection
  - - It's difficult to hide from a layer 2 ARP

Discovering network devices
- Switched networks can be a challenge
  - Many different interfaces
  - Each interface can have a very different configuration
  - Identify the port number, MAC address, VLAN ID, etc.
- CDP - Cisco Discovery Protocol
  - Proprietary Cisco protocol
  - Still very common
- LLDP - Link Layer Discovery Protocol
  - Vendor neutral
  - A more common discovery method

Speed test sites
- Bandwidth testing
  - Transfer a file, measure the throughput
- Provide useful pre- and post- change analysis
  - Test, install firewall/packet shaper, test again
- Measure at different times of the day
  - Can be automated or manual
- Not all sites are the same
  - Number of servers (point of presence - POP)
  - Bandwidth at the POP
  - Testing methodology
- ISP sites
  - speedtest.xfinity.net, www.att.com/speedtest
- SpeedOf.Me, speedtest.net, testmy.net

5.5 - 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 -n <count> <ip address>` - Send # of echo requests

traceroute - Determine the route a packet takes to a destination

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

nslookup and dig - Lookup information from DNS servers

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

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

netstat - Display network statistics

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

ipconfig, ifconfig, ip

- View and manage IP configuration
- `ipconfig` - Windows TCP/IP config
- `ipconfig /all` - Display all IP config details
- `ipconfig /release` - Release the DHCP lease
- `ipconfig /renew` - Renew the DHCP lease
- `ipconfig /flushdns` - Flush the resolver cache
- `ifconfig` - Linux interface configuration
- `ip address` - The latest Linux utility

arp - Address resolution protocol information

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

5.5 - Hardware Tools

Tone generator

- Where does that wire go?
  - Follow the tone
- Tone generator
  - Puts an analog sound on the wire
- Inductive probe
  - Doesn't need to touch the copper
  - Hear through a small speaker

Using the tone generator and probe

- Easy wire tracing
  - Even in complex environments
- Connect the tone generator to the wire
  - Modular jack
  - Coax
  - Punch down connectors
- Use the probe to locate the sound
  - The two-tone sound is easy to find

Cable testers

- Relatively simple
  - Continuity test
  - A simple wire map
- Can identify missing pins
  - Or crossed wires
- Not usually used for frequency testing
  - Crosstalk, signal loss, etc.

Taps and port mirrors

- Intercept network traffic
  - Send a copy to a packet capture device
- Physical taps
  - Disconnect the link, put a tap in the middle
  - Can be an active or passive tap
- Port mirror
  - Port redirection, SPAN (Switched Port ANalyzer)
  - Software-based tap
  - Limited functionality, but can work well in a pinch

Wireless survey tools

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

Wi-Fi analyzer

- Hardware-based Wi-Fi analysis
  - Avoids operating system limitations
  - View all of the 802.11 information in the air
- View Wi-Fi information
  - Frequencies/channels, signal strength, access points, interference, wireless devices
- Get frequency information from a spectrum analyzer
  - Useful when many different devices are part of the bigger picture

Visual fault locator

- A flashlight for optical fiber
  - Shine a bright light down the fiber
- Light will show through the fiber jacket where fiber is broken
  - You may need to turn the lights out
- Relatively low-tech
  - But very efficient

5.5 - Basic Network Device Commands

Basic platform commands

- There are some commands that are common across switch and router manufacturers
  - It's remarkable how similar they can be
  - Once you know one, you effectively know them all
- Not all devices use exactly the same syntax
  - Refer to the documentation for specifics
  - The fundamentals are the same, however
- Learn the technology
  - The commands will come naturally

`show mac-address-table`

- All switches maintain a MAC address table
  - Media Access Control addresses
  - The Ethernet hardware
- View the MAC address table
  - The show command
  - Many options are available for showing information
- Switch forwarding uses this table
  - This MAC address is connected to this interface

`show route`

- Routers maintain a list of next hops
  - The routing table
- View the current routing table
  - Dynamic routes can change
  - Static routes must be manually configured
- Use this list to find errors in the routes
  - Or use the table to manually determine the next hop
  - Useful when troubleshooting

`show interface`

- The status of an interface
  - Up, down, connected, disabled, speed, duplex, etc.
- View configuration information
  - Speed, MTU, encapsulation type, etc.
- Identify errors
  - Problems with the interface
  - CRC errors, drops, input and output errors
- View overall performance
  - Total frames, broadcasts
  - Queue capacity

`show config`

- Every device has a configuration
  - View the device settings
- Display the currently running configuration
  - Or configuration settings stored on the device
  - Everything in once place
- Requires a bit of training
  - Learn the syntax

`show arp`

- View ARP protocol information
  - Address Resolution Protocol
- Useful when troubleshooting connectivity
  - Do we see the MAC address associated with an IP address?

`show vlan`

- View the VLANs associated with switch interfaces
  - Virtual Local Area Network ID
- View default VLAN ID and assigned VLAN ID numbers
  - Confirm the assignment for each interface

`show power`

- Display power-related information
  - Power supply status, Power over Ethernet usage
- Monitor power usage
  - Available, used, and remaining power
- Manage PoE devices
  - Plan for future PoE devices and troubleshoot power issues

Continue your journey on
ProfessorMesser.com:

Professor Messer's Free
CompTIA Network+ Training Course

Monthly Network+ Study Group Live Streams

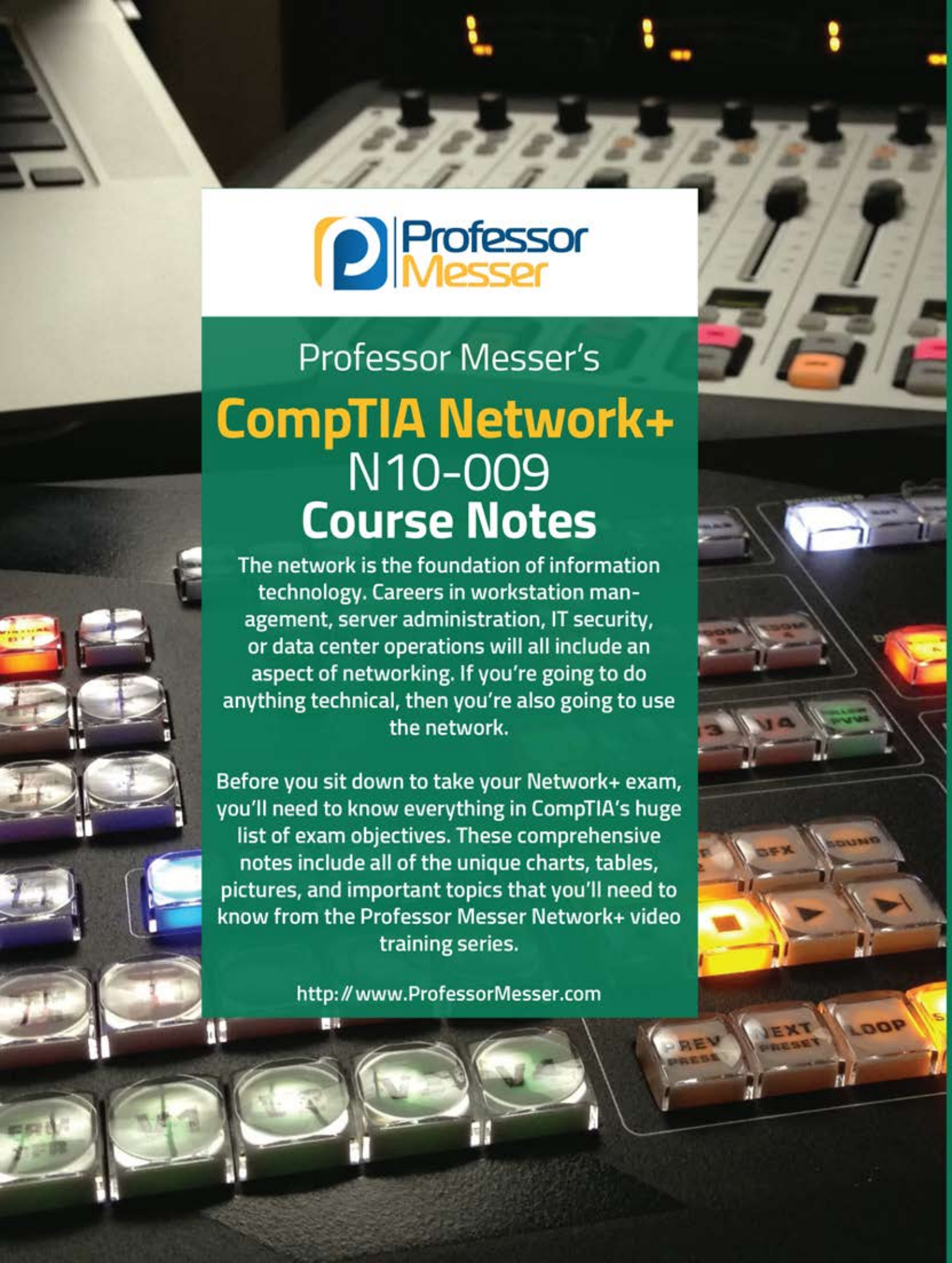
24 x 7 Live Discord Chat

Professor Messer's
CompTIA Network+ Success Bundle

Voucher Discounts

Professor Messer

https://www.ProfessorMesser.com



Professor Messer

Professor Messer's

CompTIA Network+

N10-009

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