Professor Messer

Professor Messer's

CompTIA Network+

N10-007

Course Notes

James "Professor" Messer

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

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's CompTIA N10-007 Network+ Course Notes
Written by James "Professor" Messer

http://www.ProfessorMesser.com

First Edition: February 2018

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA N10-007 Network+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

Introduction

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

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

- Professor Messer

The CompTIA Network+ certification

To earn the Network+ certification, you must pass a single N10-007 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 N10-007 exam:

Section 1.0 - Networking concepts - 23%
Section 2.0 - Infrastructure - 18%
Section 3.0 - Network Operations - 17%
Section 4.0 - Network Security - 20%
Section 5.0 - Network Troubleshooting and Tools - 22%

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

http://www.professormesser.com/objectives/

How to use this book

Once you're comfortable with all of the sections in the official CompTIA N10-007 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.
- Manage your time wisely. You've got 90 minutes to get through everything.
- 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+

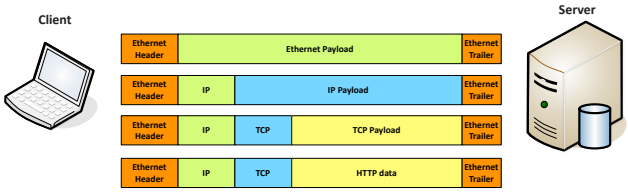
N10-007 Course Notes

http://www.ProfessorMesser.com

1.1 - Introduction to IP

A Series of Moving Vans

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



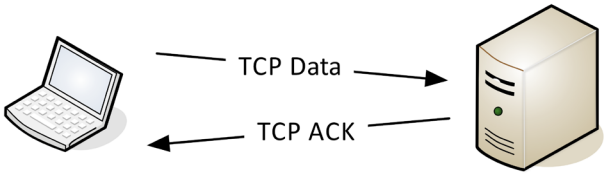
TCP and UDP

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

TCP - Transmission Control Protocol

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

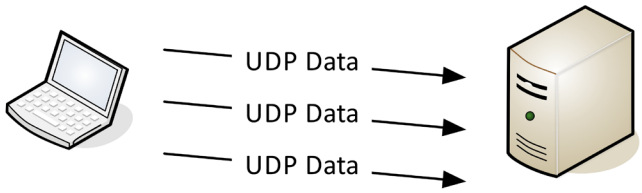
TCP - Transmission Control Protocol Communication



UDP - User Datagram Protocol

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

UDP - User Datagram Protocol Communication



Lots of Ports

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

Port Numbers

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

ICMP

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

1.1 - Common Ports

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

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

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

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

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

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

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

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

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

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

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

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

SMB - Server Message Block
- Protocol used by Microsoft Windows
  - File sharing, printer sharing
  - Also called CIFS (Common Internet File System)
- Direct over tcp/445 (NetBIOS-less)
  - Direct SMB communication over TCP without the NetBIOS transport

1.1 - Common Ports (continued)

POP/IMAP

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

LDAP/LDAPS

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

H.323

- Voice over IP (VoIP) signaling - tcp/1720
  - ITU Telecommunication H.32x protocol series
- Setup and manage VoIP sessions
  - Call, ring, hang up
- One of the earliest VoIP standards
  - Still in use today

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
Common Network Protocols			
SSH	tcp/22	Secure Shell	Encrypted console login
DNS	udp/53	Domain Name System	Convert domain names to IP addresses
SMTP	tcp/25	Simple Mail Transfer Protocol	Transfer email between mail servers
SFTP	tcp/22	Secure FTP	Secure file transfer
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
DHCP	udp/67, udp/68	Dynamic Host Configuration Protocol	Automated IP addressing and configuration
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
RDP	tcp/3389	Remote Desktop Protocol	Graphical display of remote device
NTP	udp/123	Network Time Protocol	Synchronize clocks
SIP	tcp/5060-5061	Session Initiation Protocol	Voice over IP signaling protocol
SMB	tcp/445	Server Message Block	Windows file transfers and printer sharing
POP3	tcp/110	Post Office Protocol version 3	Receive mail into a mail client
IMAP4	tcp/143	Internet Message Access Protocol v4	A newer mail client protocol
LDAP	tcp/389	Lightweight Directory Access Protocol	Communicate with network directories
LDAPS	tcp/636	Lightweight Directory Access Protocol Secure	LDAP over SSL
H.323	tcp/1720	ITU Telecommunication H.32x protocol series	Voice over IP signaling

1.2 - Understanding the OSI Model

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

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

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

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

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

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

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

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

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

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

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

1.3 - Introduction to Ethernet

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

1.3 - Introduction to Ethernet (continued)

The MAC address

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

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

Organizationally Unique Identifier (OUI) (the manufacturer)	Network Interface Controller-Specific (the serial number)

Duplex

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

CSMA/CD

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

CSMA/CD operation

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

CSMA/CA

- CA - Collision Avoidance
  - Common on wireless networks
- Collision detection isn't possible
  - A sending station can't "hear" other stations
- Common to see RTS/CTS
  - I'm ready! You're clear!
- Solves the "hidden node" problem
  - Station A can hear the access point
  - Station B can hear the access point
  - Station A can't hear station B

1.3 - Network Switching Overview

The Switch

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

Learning the MACs

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

Flooding for unknown Macs

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

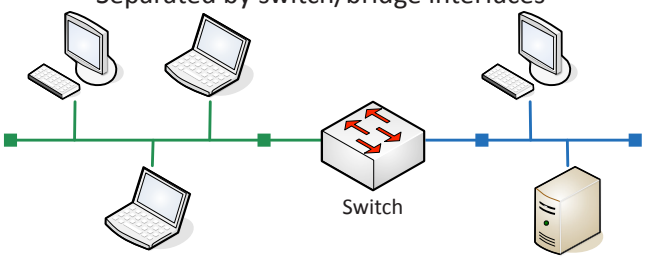
Address Resolution Protocol

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

1.3 - Broadcast Domains and Collision Domains

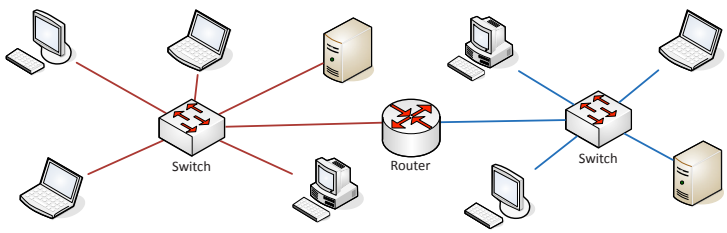
Collision Domains

Separated by switch/bridge interfaces



Broadcast Domains

Separated by router interfaces



1.3 - Broadcast Domains and Collision Domains (continued)

Collision domains

- A historical footnote
  - It's difficult to find a collision these days
  - The word "collision" is misleading
- The network was one big segment
  - Everyone heard everyone else's signals
  - One big conference call
- Only one station can "talk" at a time
  - Is the line clear? Ok, I can talk.
  - Carrier Sense Multiple Access (CSMA)
- When two people spoke at the same time, there was a collision
  - Collision Detection (CD) - Send the jam signal

Broadcast Domains

- Spread the word!
  - Everyone must know!
  - ARP probes, operating system notifications
- How far can a broadcast go?
  - Passed by a switch/bridge
  - Stops at the router
- This can be important
  - More devices, more broadcasts

1.3 - Unicasts, Broadcasts, and Multicasts

Unicast

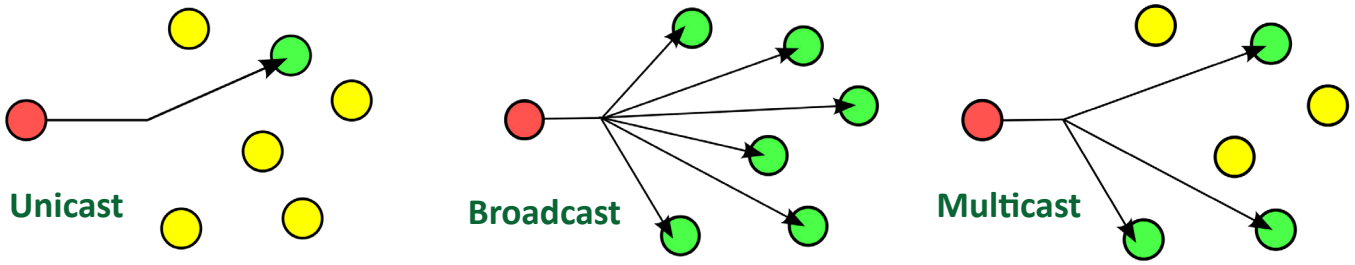
- One station sending information to another station
- Send information between two systems
- Web surfing, file transfers
- Does not scale optimally for streaming media

Broadcast

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

Multicast

- Delivery of information to interested systems
  - One to many
- Multimedia delivery, stock exchanges
- Very specialized
  - Difficult to scale across large networks



1.3 - Protocol Data Units

PDU (Protocol Data Unit)

- A unit of transmission
  - A different group of data at different OSI layers
- Ethernet operates on a frame of data
  - It has no idea what's inside
- IP operates on a packet of data
  - Inside is TCP or UDP, but IP doesn't know that
- TCP or UDP PDU - TCP segment, UDP datagram

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

Troubleshooting MTU

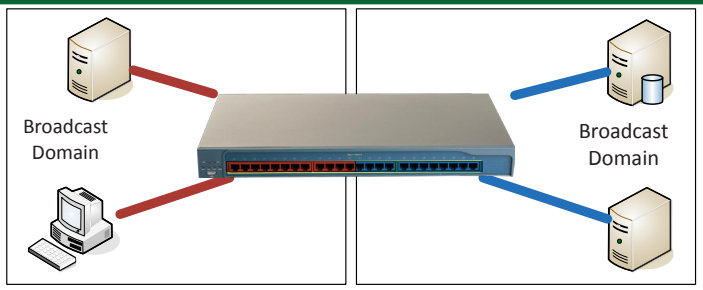
- MTU sizes are usually configured once
  - Based on the network infrastructure and don't change often
- A significant concern for tunneled traffic
  - The tunnel may be smaller than your local Ethernet segment
- What if you send packets with Don't Fragment (DF) set?
  - Routers will respond back and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

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

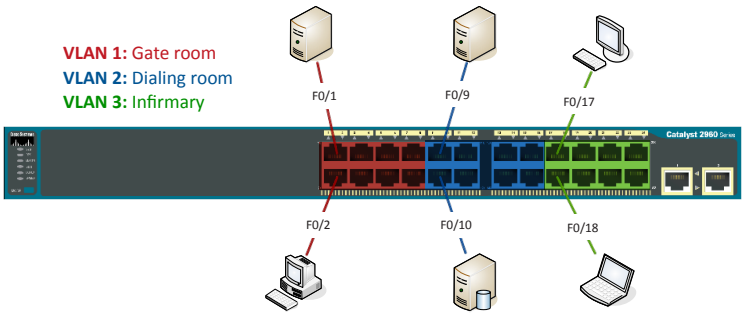
  - Windows: `ping -f -l 1472 8.8.8.8`

1.3 - Network Segmentation

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



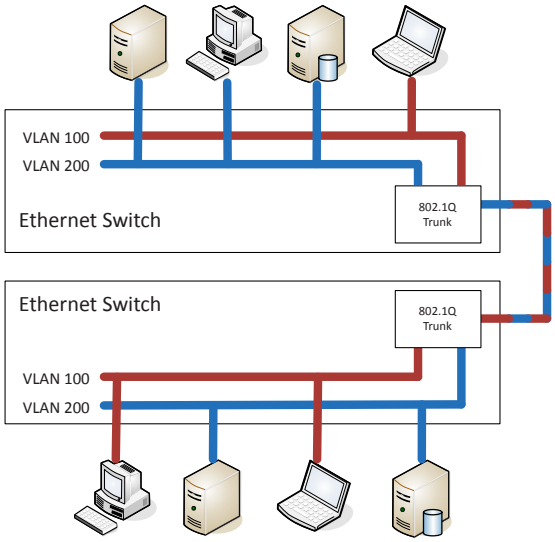
802.1Q trunking
- Take a normal Ethernet frame

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



1.3 - Spanning Tree Protocol

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

Switch operation
- Forwarding decisions made by MAC address
  - Keeps a big table of MAC address that have been seen
  - All forwarding decisions are filtered through this list
- If the destination MAC is unknown, the frame is flooded
  - Sent to every switch port in the local subnet/VLAN
  - Hopefully the destination station will respond
- Flooding is hopefully a temporary process
  - Directed traffic resumes when the MAC is seen

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

1.3 - Switch Interface Properties

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

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

DMZ
- Demilitarized zone
  - An additional layer of security between the Internet and you

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

PoE and POE+
- PoE: IEEE 802.3af-2003
  - The original PoE specification
  - Included in 802.3at
  - Now part of 802.3-2012
  - 15.4 watts DC power
  - Maximum current of 350 mA
- POE+: IEEE 802.3at-2009
  - The updated PoE specification
  - Now also part of 802.3-2012
  - 25.5 watts DC power
  - Maximum current of 600 mA

Port mirroring
- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

1.3 - Static and Dynamic Routing

Routing
- Send IP packets across the network
  - Forwarding decisions are based on destination IP address
- Each router only knows the next step
  - The packet asks for directions every hop along the way
  - The list of directions is held in a routing table

Routing
- Different topologies use different data link protocols
  - Ethernet, HDLC, etc.
- Each router rewrites the frame to add its own data-link header
  - The IP packet remains intact

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 sub 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
  - Requires some initial configuration to work properly

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

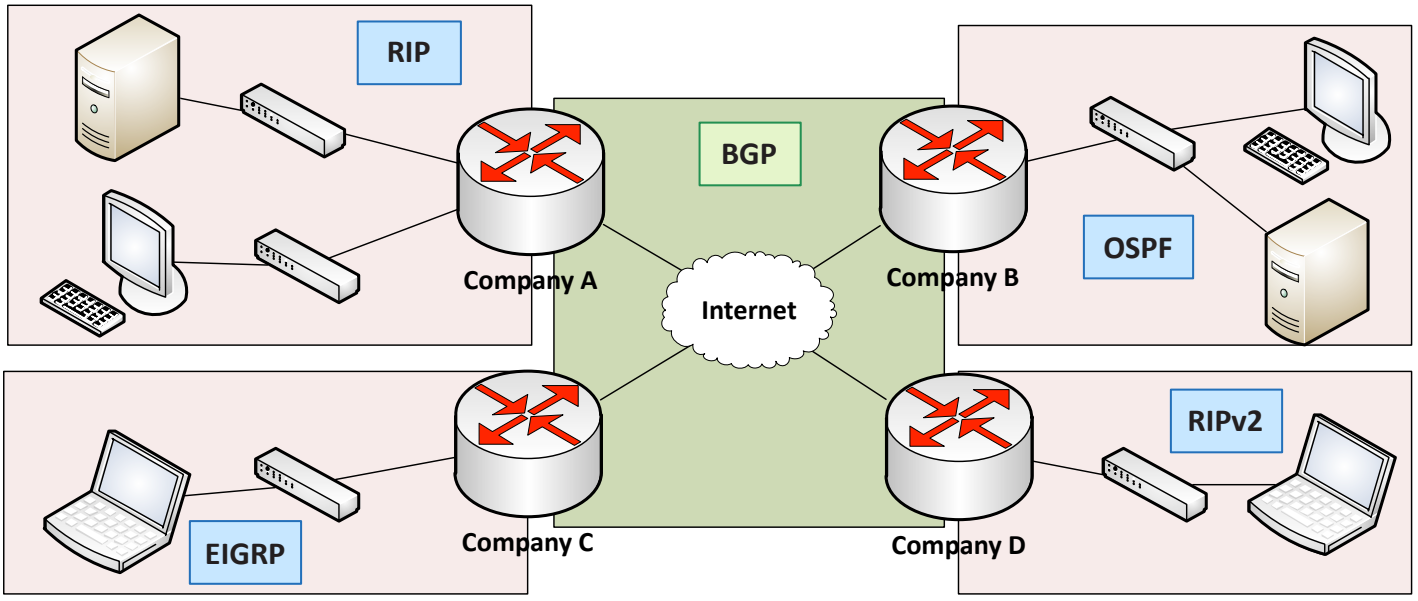
1.3 - IGP and EGP

AS (Autonomous System)
- Autonomous
  - Existing as an independent entity
- Group of IP routes under common control
- RFC 1930, Section 3: Definitions
  - "An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy."
- Important point of reference for discussing Interior Gateway Protocols and Exterior Gateway Protocols

IGP (Interior Gateway Protocol)
- Used within a single autonomous system (AS)
  - Not intended to route between AS
  - That's why there's Exterior Gateway Protocols (EGPs)
- IPv4 dynamic routing
  - OSPFv2 (Open Shortest Path First)
  - RIPv2 (Routing Information Protocol version 2)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
- IPv6 dynamic routing
  - OSPFv3
  - EIGRP for IPv6
  - RIPng (RIP next generation)

EGP (Exterior Gateway Protocol)
- Used to route between autonomous systems
  - Leverages the IGP at the AS to handle local routing
- BGP (Border Gateway Protocol)
  - Many organizations use BGP as their EGP

Interior and Exterior Routing



1.3 - Dynamic Routing Protocols

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

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

1.3 - Dynamic Routing Protocols (continued)

Distance-vector routing protocols

- Information passed between routers contains routing tables
  - How many "hops" away is another network?
  - The deciding "vector" is the "distance"
- Usually automatic
  - Very little configuration
- Good for smaller networks
  - Doesn't scale well to very large networks
- RIP, RIPv2, EIGRP

Link-state routing protocols

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

Hybrid routing protocols

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

1.3 - IPv4 and IPv6 Addressing

The IP address of a device

- 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 workstation to determine what subnet it's on
  - The subnet mask isn't (usually) transmitted across the network
- You'll ask for the subnet mask all the time
  - What's the subnet mask of this network?

The secret behind the IP address

- The IP address isn't really a single address.
- An IP address is a combination of a network ID and a host ID
  - The subnet mask determines what part of the IP address is the network and which part is the host
  - The subnet mask is just as important as your IP address!
- The best way to see this work is in binary
  - This is the (very easy) math part

IPv4 addresses - Internet Protocol version 4

- OSI Layer 3 address
- Since one byte is 8 bits, the maximum decimal value for each byte is 255

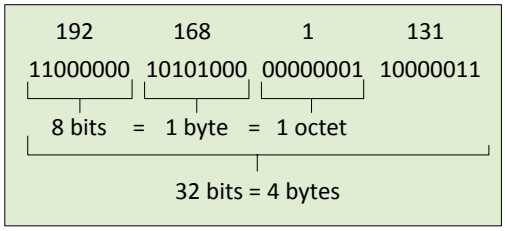
IPv6 addresses

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

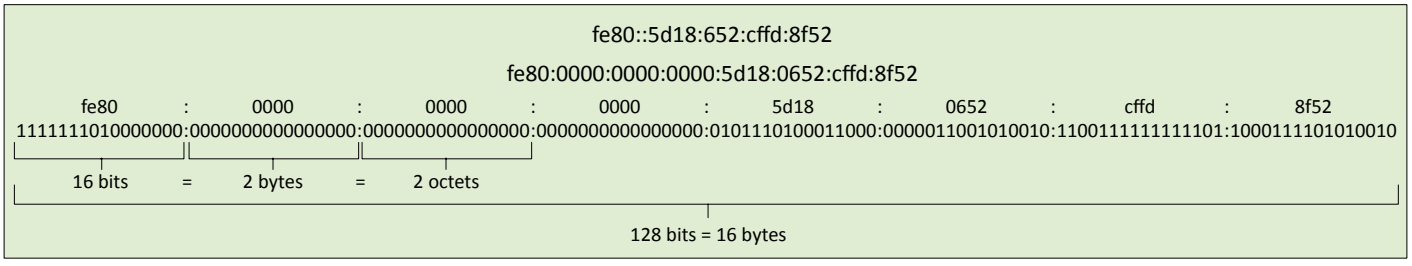
IPv6 address compression

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

IPv4 Address



IPv6 Address



1.3 - Configuring IPv6

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

Tunneling IPv6

- 6 to4 addressing
  - Send IPv6 over an existing IPv4 network
  - Creates an IPv6 based on the IPv4 address
  - Requires relay routers -
    - IP protocol 41 - a transition technology
  - No support for NAT
- 4in6
  - Tunnel IPv4 traffic on an IPv6 network

Teredo/Miredo

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

NDP (Neighbor Discovery Protocol)

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

Finding Router

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

Howdy Neighbor

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

1.3 - Prioritizing Traffic

Managing Network Traffic

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

Packet shaping

- Packet shaping, traffic shaping
- Control by bandwidth usage or data rates
- Set important applications to have higher priorities than other apps

QoS (Quality of Service)

- Prioritize traffic performance
  - Voice over IP traffic has priority over web-browsing
  - Prioritize by maximum bandwidth, traffic rate, VLAN, etc.
- Quality of Service
  - Describes the process of controlling traffic flows
- Many different methods - Across many different topologies

Managing QoS

- CoS (Class of Service)
  - OSI Layer 2
  - Ethernet frame header in an 802.1q trunk
  - Usually applied in the intranet (not from an ISP)
- Differentiated Services (DiffServ)
  - OSI Layer 3
  - QoS bits are enabled in the IPv4 header
  - Bits are set external to the application
  - Routers and switches have to play along
- DSCP (Differentiated Services Code Point)
  - DS (Differentiated Services) field in the IP header

1.3 - 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

Port Forwarding

- 24x7 access to a service hosted internally
  - Web server, gaming server, security system, etc.
- External IP/port number maps to an internal IP/port
  - Does not have to be the same port number
- Also called Destination NAT or Static NAT
  - Destination address is translated from a public IP to a private IP
  - Does not expire or timeout

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

1.3 - Access Control Lists

Packet filtering

- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs can evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?
- ACLs have evolved through the years
  - More options and features available for traffic filtering

Firewall rules

- Access control lists (ACLs)
  - Allow or disallow traffic based on tuples
  - Groupings of categories
    - Source IP, Destination IP, port number, time of day, application, etc.
- 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

1.3 - Circuit Switching and Packet Switching

Circuit switching

- Circuit is established between endpoints before data passes
  - Like a phone call
- Nobody else can use the circuit when it's idle
  - Inefficient use of resources
- Connection is always there
  - It's mine. You can't use it.
- Capacity is guaranteed
  - You'd better use it, you paid for it.

Circuit switching

- POTS (plain old telephone service) and PSTN (public switched telephone network)
- T1 / E1 / T3 / E3
  - Create a circuit between two sites
- ISDN
  - Use a phone number to call another ISDN modem

1.3 - Circuit Switching and Packet Switching (continued)

Packet switching
- Data is grouped into packets
  - Voice, data, video, etc.
  - Like a network
- The media is usually shared
  - Someone else can use it, even when you don't
- One connection may have more bandwidth allocated than another
  - How much money would you like to spend?

Packet switching
- SONET, ATM
- DSL
- Frame relay
- MPLS
- Cable modem
- Satellite
- Wireless

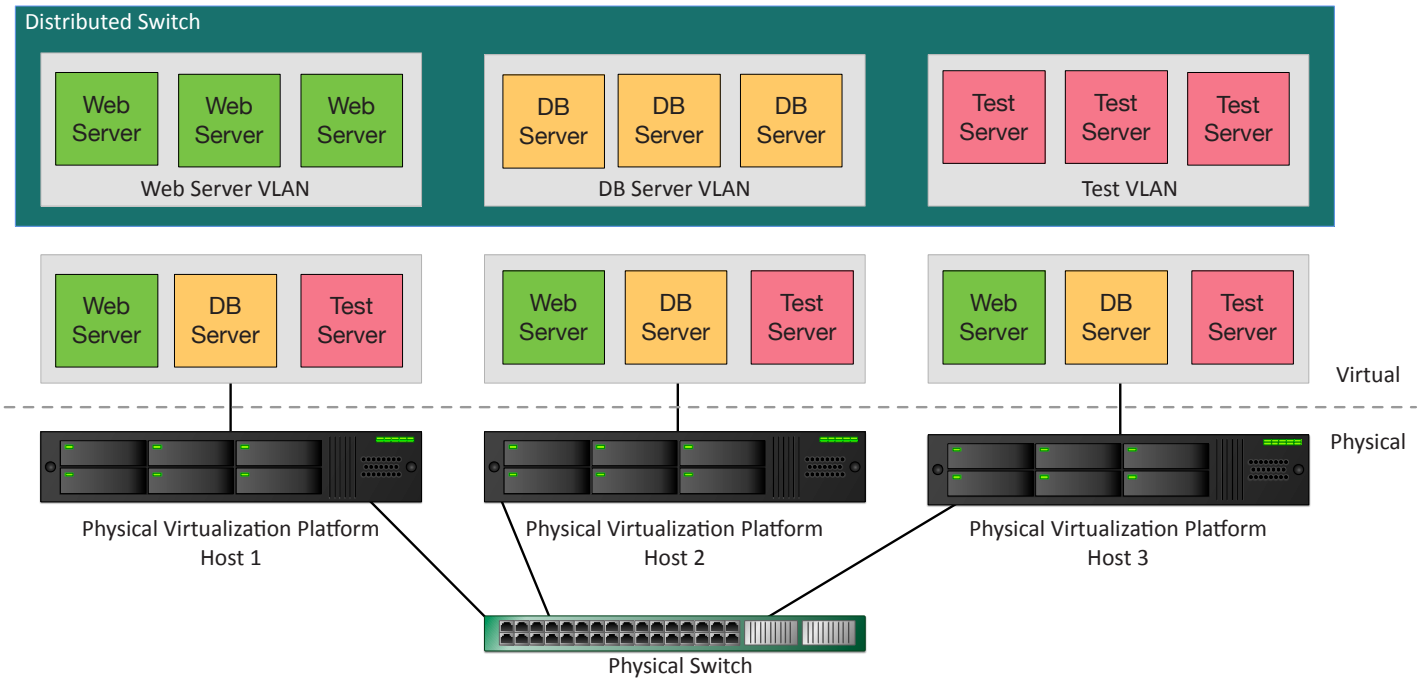
1.3 - Software Defined Networking

SDN (Software Defined Networking)
- Networking devices have two functional planes of operation
  - Control plane
  - Data plane
- Directly programmable
  - Configuration is different than forwarding
- Agile
  - Changes can be made dynamically

SDN (Software Defined Networking)
- Centrally managed - Global view, single pane of glass
- Programmatically configured
  - Orchestration - No human intervention
- Open standards / vendor neutral
  - A standard interface to the network

Distributed switching
- Remove the physical segmentation
  - A virtual network distributed across all physical platforms
- When a VM moves, the network doesn't change
  - Servers will always connect to the right VLAN

Distributed Switching



1.4 - Binary Math

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

1.4 - IPv4 Addresses

Networking with IPv4

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

Special IPv4 addresses

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

1.4 - Classful Subnetting and IPv4 Subnet Masks

Classful Subnetting

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

The construction of a subnet

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

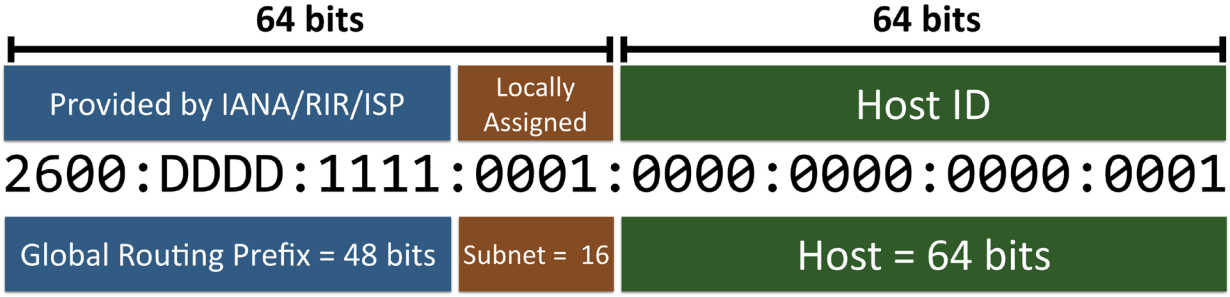
Binary	Decimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts per Network	Default Subnet Mask
Class A	0xxx (1-126)	8	24	128	16,777,214	255.0.0.0
Class B	10xx (128-191)	16	16	16,384	65,534	255.255.0.0
Class C	110x (192-223)	24	8	2,097,152	254	255.255.255.0
Class D (multicast)	1110 (224-239)	Not defined	Not defined	Not defined	Not defined	Not defined
Class E (reserved)	1111 (240-254)	Not defined	Not defined	Not defined	Not defined	Not defined

1.4 - IPv6 Subnet Masks

Assigning IPv6 Addresses

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



1.4 - 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

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

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

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

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

1.4 - Seven Second Subnetting

Seven second subnetting

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

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

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

1.4 - Assigning IPv4 Addresses

DHCP

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

The DHCP Process

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

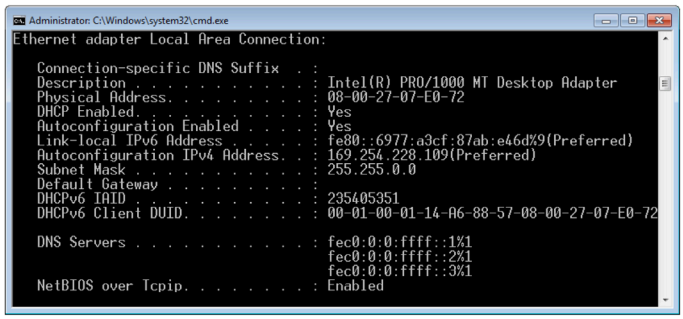
1.4 - Assigning IPv4 Addresses (continued)

Turning dynamic into static

- DHCP assigns an IP address from the first available from a large pool of addresses
  - Your IP address will occasionally change
- You may not want your IP address to change
  - Server, printer, or personal preference
- Disable DHCP on the device
  - Configure the IP address information manually
  - Requires additional administration
- Configure an IP reservation on the DHCP server
  - Associate a specific MAC address with an IP address

APIPA - Automatic Private IP Addressing

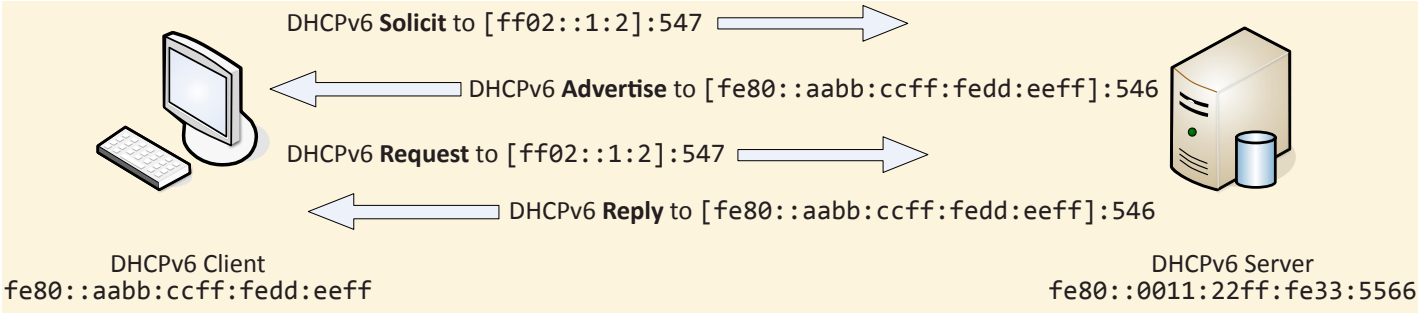
- A link-local address - No forwarding by routers
- IETF has reserved 169.254.0.1 - through 169.254.255.254
  - First and last 256 addresses are reserved
  - Functional block of 169.254.1.0 through 169.254.254.255



1.4 - Assigning IPv6 Addresses

Stateful DHCPv6

- Very similar process to DHCPv4 - udp/546 (client) and udp/547 (server)

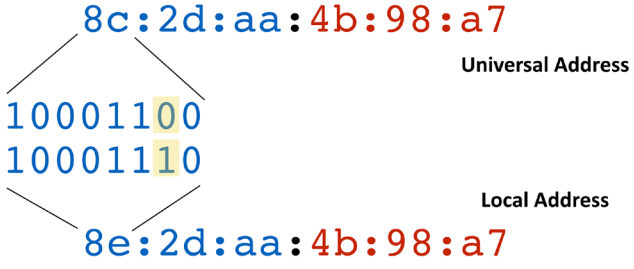


Configuring IPv6 with a modified EUI-64

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

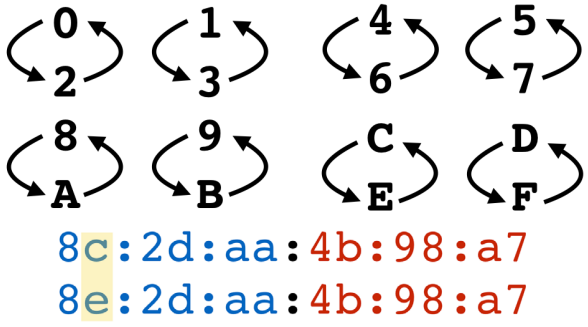
Converting EUI-48 to EUI-64

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



Shortcut for flipping the 7th bit

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

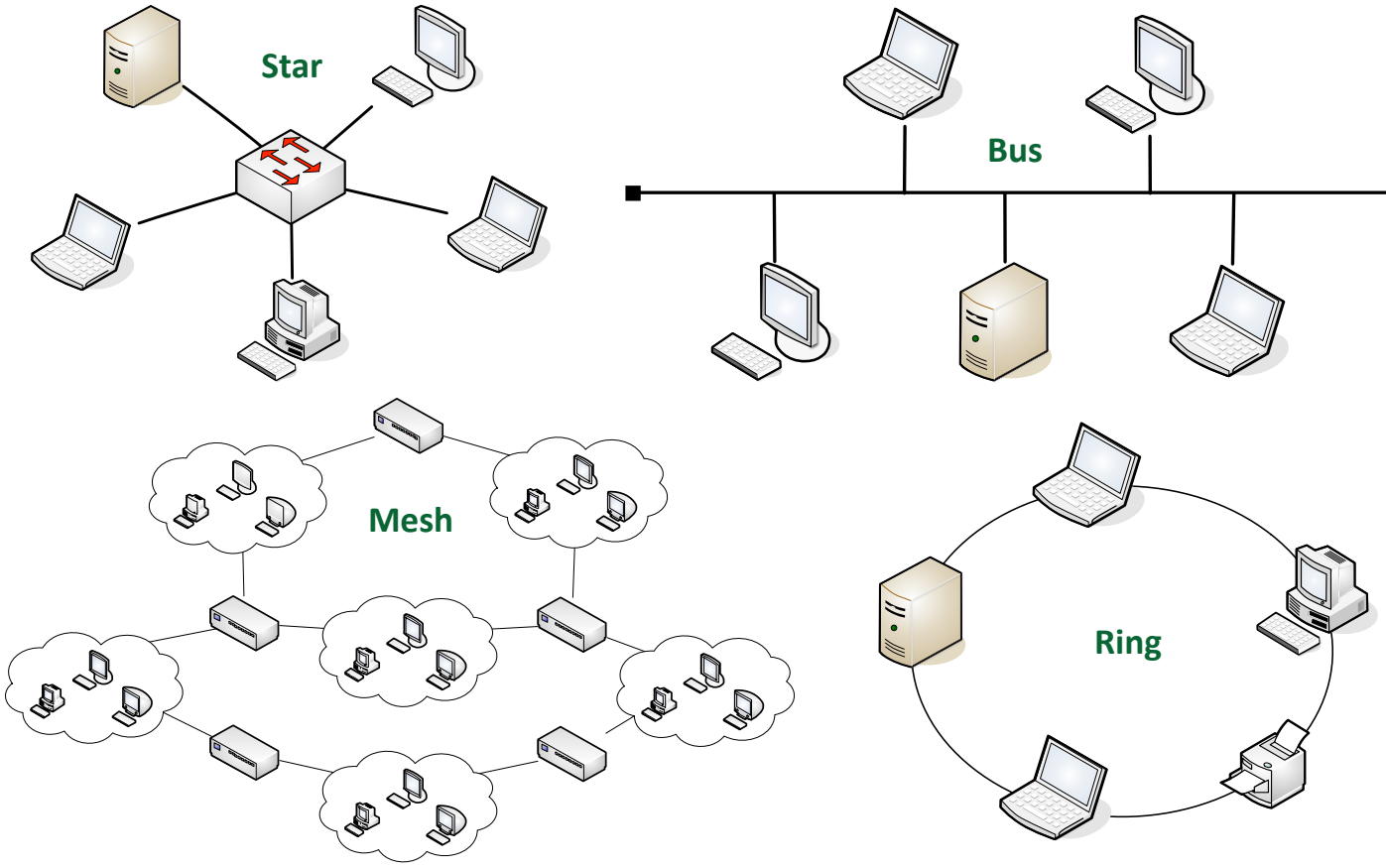


1.5 - Network Topologies

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

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

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



1.5 - Common Network Types

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

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

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

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

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

1.5 - Common Network Types (continued)

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

PAN - Personal Area Network

- Personal Area Network
- Your own private network - Bluetooth, IR, NFC
- Automobile - audio output, integrate with phone
- Mobile phone - wireless headset
- Health - workout telemetry, daily reports

1.5 - Internet of Things Topologies

Internet of Things

- Wearable technology
  - Watches, health monitors, glasses
  - Track our location
  - Where is that data and how is it stored?
- Home automation
  - Video doorbells
  - Internet-connected garage door openers
  - Heating and cooling
  - It knows when you are home (and when you aren't)

Z-Wave

- Home automation networking
  - Control lights, locks, garage doors, etc.
- Wireless mesh networking
  - Nodes can hop through other nodes on the way to the destination
- Uses the ISM band
  - Industrial, Scientific, and Medical
  - 900 MHz frequencies in the US
  - No conflicts with 802.11

ANT / ANT+

- Wireless sensor network protocol
  - 2.4 GHz ISM band (industrial, scientific, and medical)
  - An "Internet of Things" ultra-low-power protocol
  - Fitness devices, heart rate monitors, etc.
- A separate wireless service
  - Not 802.11 or Bluetooth
- Denial of service
  - Spectrum jamming
- Optional encryption
  - And no method to maintain integrity

Bluetooth

- High speed communication over short distances
  - PAN (Personal Area Network)
- Connects our mobile devices
  - Smartphones, tethering, headsets and headphones, health monitors, automobile and phone integration, smartwatches, external speakers

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which is mostly one-way
- Payment systems
  - Google wallet and MasterCard partnership
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

IR (Infrared)

- Included on many smartphones, tablets, and smartwatches
  - Not really used for file transfers and printing
- Control your entertainment center
  - Many IR options

RFID (Radio-frequency identification)

- It's everywhere
  - Access badges
  - Inventory/Assembly line tracking
  - Pet/Animal identification
  - Anything that needs to be tracked
- Radar technology
  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag formats can be active/powered

IEEE 802.11

- 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

1.6 - 802.11 Wireless Standards

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

802.11a

- One of the original 802.11 wireless standards
  - October 1999
- Operates in the 5 GHz range
  - Or other frequencies with special licensing
- 54 megabits per second (Mbit/s)
- Smaller range than 802.11b
  - Higher frequency is absorbed by objects in the way
  - Many rules-of-thumb calculate 1/3rd the range of 802.11b or 802.11g
- Today, only seen in very specific use cases

802.11b

- Also an original 802.11 standard - October 1999
- Operates in the 2.4 GHz range
- 11 megabits per second (Mbit/s)
- Better range than 802.11a - Less absorption problems
- More frequency conflict
  - Baby monitors, cordless phones, microwave ovens, Bluetooth

802.11g

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

802.11n

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

802.11ac

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

	Frequencies	Maximum MIMO streams	theoretical throughput (per stream)	theoretical throughput (total)
802.11a	5 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	Not applicable	11 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11n	5 GHz and/or 2.4 GHz	4 MIMO	150 Mbit/s	600 Mbit/s
802.11ac	5 GHz	8 MU-MIMO	866.7 Mbit/s	~6.8 Gbit/s

1.6 - Cellular Network Standards

Cellular networks

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

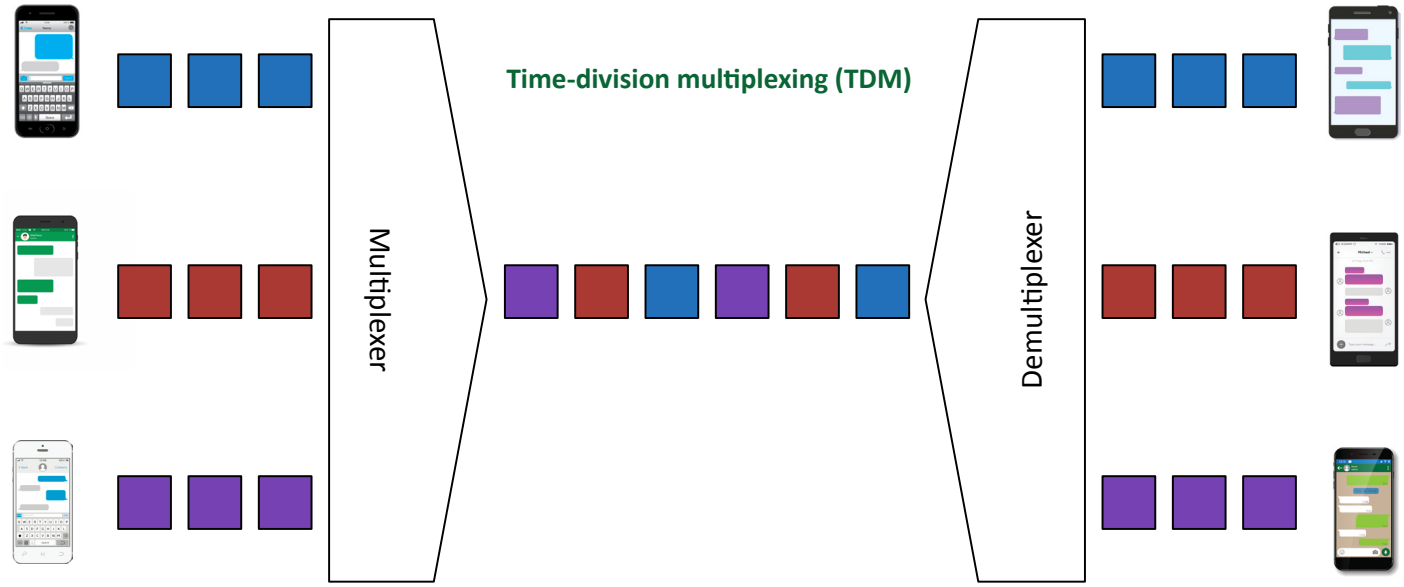
GSM

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

1.6 - Cellular Network Standards (continued)

Time-Division Multiple Access (TDMA)

- Multiple streams are combined into a single stream, and then broken out again - "Muxing"



CDMA

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

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

1.6 - Wireless Network Technologies

802.11 technologies

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

Counting antennas

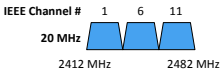
- New technologies were added to 802.11n and 802.11ac
  - Send multiple streams of information over the same frequency at the same time
  - 802.11n - MIMO - Multiple-Input and Multiple-Output
  - 802.11ac - MU-MIMO - Multi-user MIMO
- Number of antennas (802.11n and 802.11ac)
  - Used to determine the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

802.11 channel bandwidths

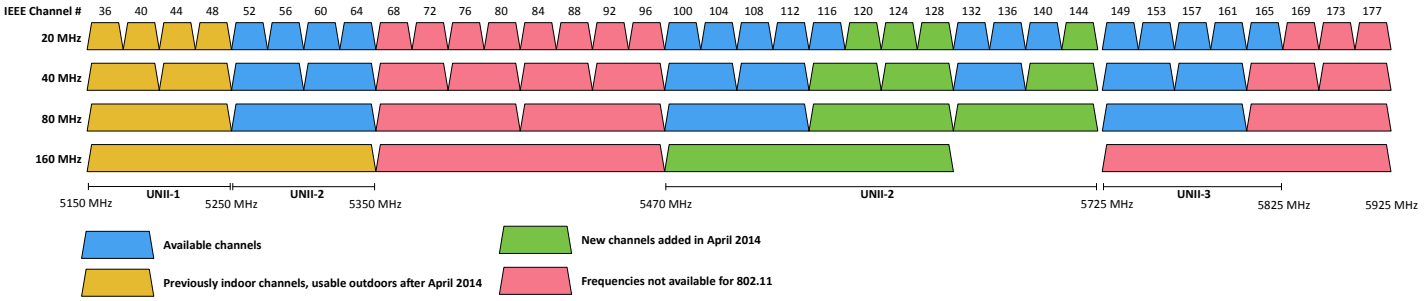
- 802.11a - 20 MHz
- 802.11b - 22 MHz
- 802.11g - 20 MHz
- 802.11n
  - 20 MHz or 40 MHz (two contiguous 20 MHz bonded channels)
  - In 2.4 GHz, a 40 MHz channel uses over 80% of the available bandwidth
- 802.11ac
  - 40 MHz for 802.11n stations
  - 80 MHz required for 802.11ac stations
  - 160 MHz optional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

1.6 - Wireless Network Technologies (continued)

2.4 GHz Spectrum for 802.11 - North America



5 GHz Spectrum for 802.11 - North America



Power level controls

- Usually a wireless configuration
  - Set it as low as you can
- How low is low?
  - This might require some additional site surveys
  - Maintain speeds across required distances
- Consider the receiver
  - High-gain antennas can hear a lot
  - Location, location, location

Omnidirectional antennas

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

Directional antennas

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

Wireless survey tools

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

1.7 - Cloud Services and Delivery Models

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

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

Cloud deployment models

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

1.7 - Cloud Services and Delivery Models (continued)

Local and cloud resources

- On-premise
  - Your applications are on local hardware
  - Your servers are in your data center in your building
- Hosted
  - Your servers are not in your building
  - They may not even be running on your hardware
  - Usually a specialized computing environment
- Cloud
  - Entire application instances can be created and torn down on-demand
  - Resources are available as needed

Connecting to the cloud

- Existing Internet connection
  - Browser-based, SSL encryption
- VPN (Virtual Private Network)
  - Encrypted tunnel for all traffic between you and the cloud
  - Will probably require some additional hardware on both ends
- Direct connection
  - Co-location, same shared data center
  - High speed 10 Gigabit connection
  - No external traffic (added security)

Managing cloud security policies

- Clients are at work, data is in the cloud
  - How do you keep everything secure?
  - The organization already has well-defined security policies
- How do you make your security policies work in the cloud?
  - Integrate a CASB (Cloud Access Security Broker)
  - Implemented as client software, local security appliances, or cloud-based security solutions

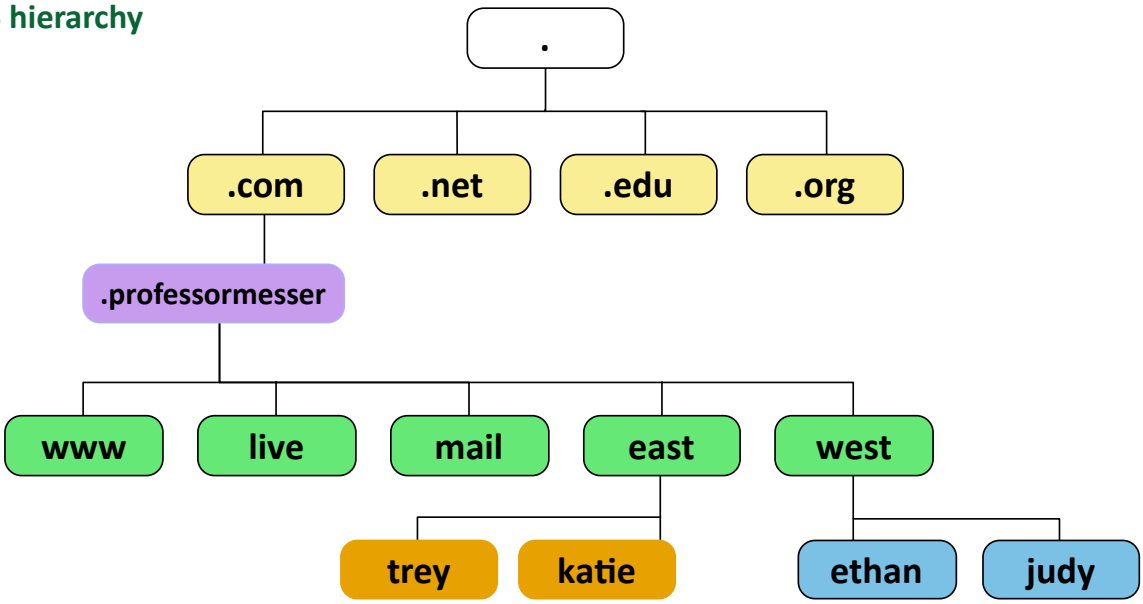
Cloud access security broker (CASB)

- Visibility
  - Determine what apps are in use
  - Are they authorized to use the apps?
- Compliance
  - Are users complying with HIPAA? PCI?
- Threat prevention
  - Allow access by authorized users, prevent attacks
- Data security
  - Ensure that all data transfers are encrypted
  - Protect the transfer of PII with DLP

1.8 - An Overview of DNS

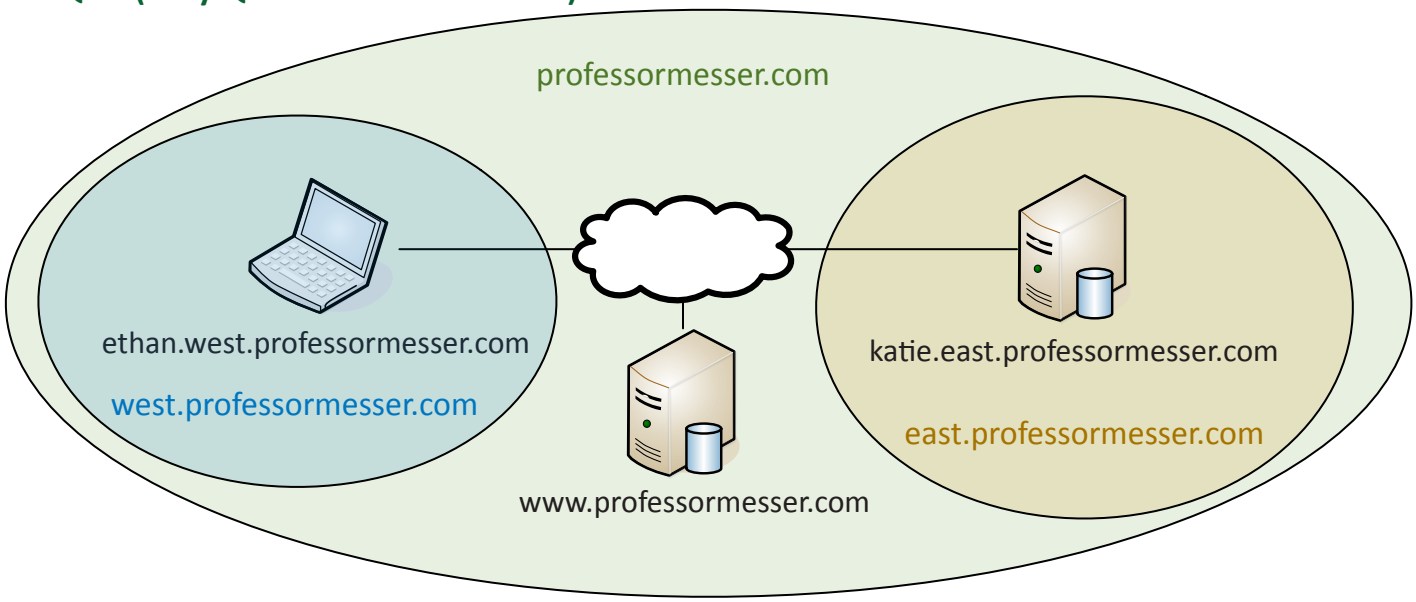
- Translates human-readable names into computer-readable IP addresses
  - You only need to remember www.ProfessorMesser.com
- Hierarchical
  - Follow the path
- Distributed database
  - Many DNS servers
  - 13 root server clusters
  - Hundreds of generic top-level domains (gTLDs) - .com, .org, .net,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

The DNS hierarchy



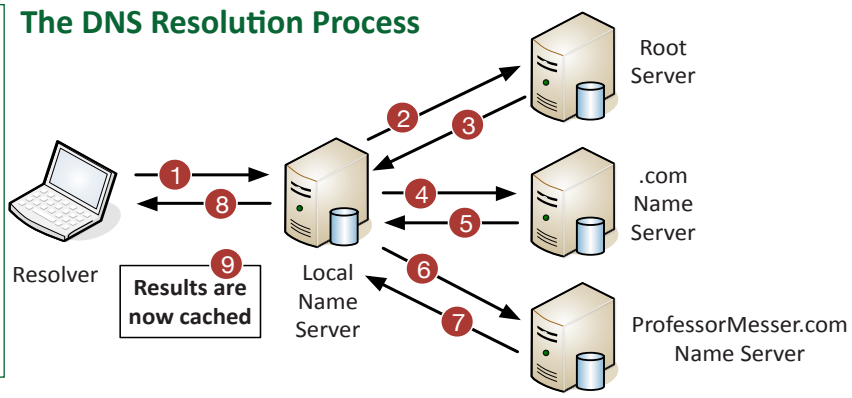
1.8 - An Overview of DNS (continued)

FQDN (Fully Qualified Domain Name)



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

The DNS Resolution Process



Internal vs. External DNS

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

Third-party DNS

- Managing DNS can be challenging
  - Especially in large environments
- Outsource the DNS
  - Cloud-based DNS services
- Features not available on a privately-hosted DNS server
  - High-availability, low latency, and scaling options

1.8 - DNS Record Types

Resource Records (RR)

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

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
```

1.8 - DNS Record Types (continued)

Canonical name records (CNAME)

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

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

Service records (SRV)

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

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

Mail exchanger record (MX)

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

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

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

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

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.
```

1.8 - DNS Record Types (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")
```

1.8 - DHCP Addressing Overview

DHCP

- IP 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

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

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

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

1.8 - Configuring DHCP

Scope properties

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

DHCP pools

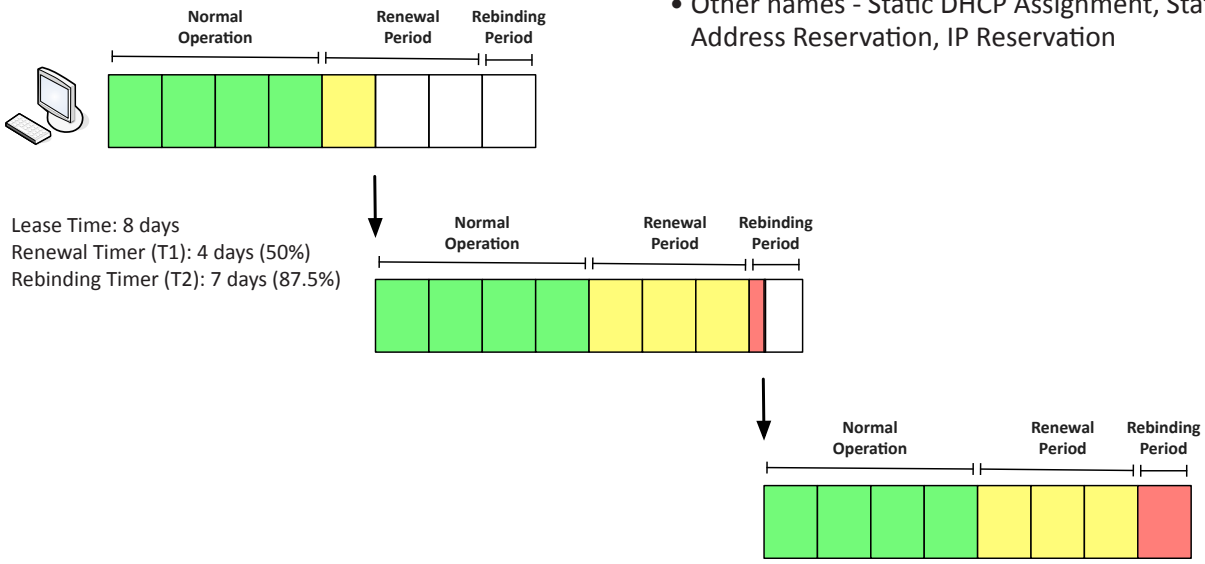
- Grouping of IP addresses
  - Each subnet has its own scope
  - 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, etc.
- A scope is generally a single contiguous pool of IP addresses
  - DHCP exceptions can be made inside of the scope

1.8 - Configuring DHCP (continued)

DHCP address allocation

- 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)

DHCP Timers



DHCP address allocation

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

1.8 - An Overview of NTP

NTP (Network Time Protocol)

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

NTP clients and servers

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

NTP stratum layers

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

Configuring NTP

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

2.1 - Copper Cabling

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

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

Cable Category	Maximum Supported Ethernet Standard	Maximum Supported Distance
Category 3	10BASE-T	100 meters
Category 5	100BASE-TX, 1000BASE-T	100 meters
Category 5e (enhanced)	100BASE-TX 1000BASE-T	100 meters
Category 6	10GBASE-T	37 to 55 meters
Category 6A (augmented)	10GBASE-T	100 meters
Category 7	10GBASE-T	100 meters

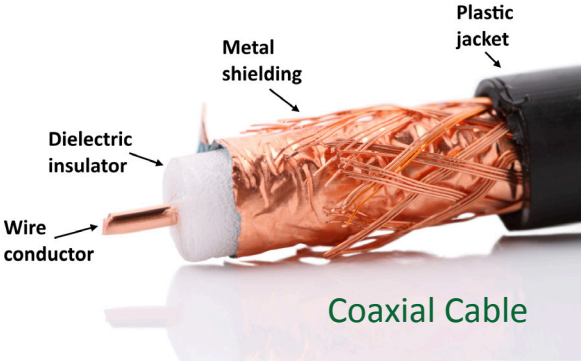
Network cabling standards
- Electronic Industries Alliance (EIA)
  - Alliance of trade associations
  - Develops standards for the industry
  - Standards start with RS-# (Recommended Standard) or EIA-#
- Telecommunications Industry Association (TIA)
  - Standards, market analysis, government affairs, etc.
  - ANSI/TIA/EIA-568 - Commercial Building Telecommunications Cabling Standard
- International ISO/IEC 11801 cabling standards
  - Defines classes of networking standards

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

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


UTP
Unshielded Twisted Pair


STP
Shielded Twisted Pair

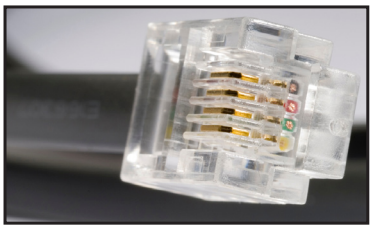


Coaxial Cable

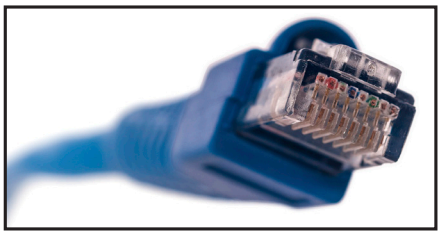
Plenum-rated cable
- Traditional cable jacket
  - Polyvinyl chloride (PVC)
- Fire-rated cable jacket
  - Fluorinated ethylene polymer (FEP) or low-smoke polyvinyl chloride (PVC)
- Plenum-rated cable may not be as flexible
  - May not have the same bend radius

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

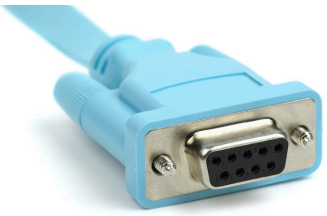
2.1 - Copper Connectors



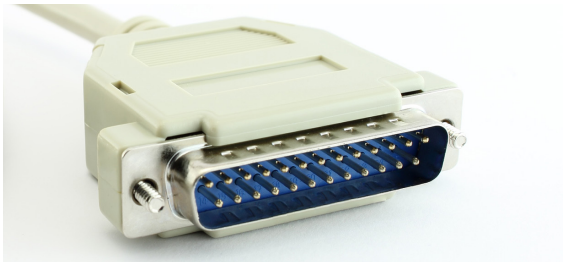
RJ-11 Connector



RJ-45 Connector



DB-9 connector



DB-25 connector

F-connector

BNC connector

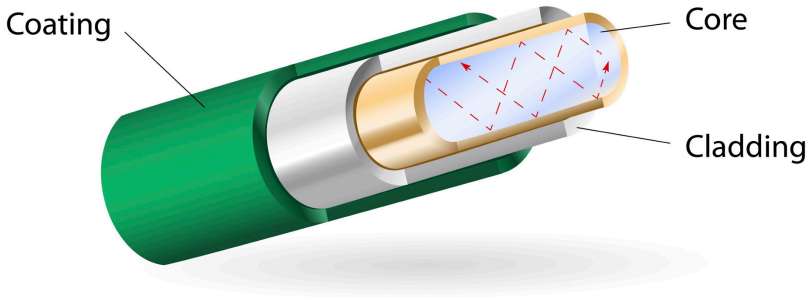
2.1 - Optical Fiber

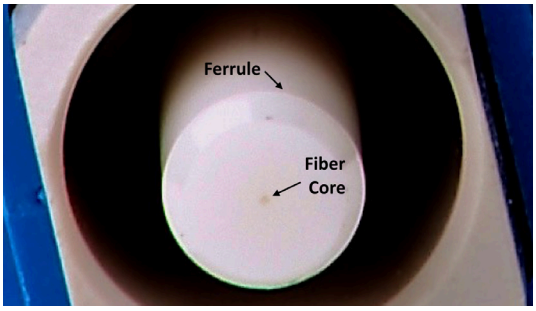
Fiber communication

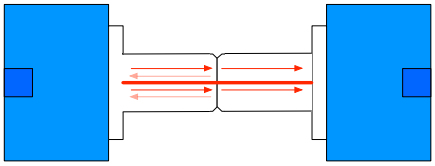
- Transmission by light
  - The visible spectrum
- No RF signal
  - Very difficult to monitor or tap
- Signal slow to degrade
  - Transmission over long distances
- Immune to radio interference - There's no RF

UPC vs. APC

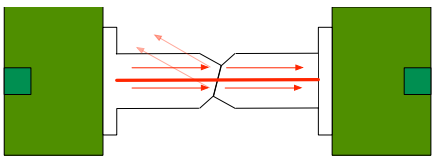
- Controlling light-Laws of physics apply
- Return loss-Light reflected back to the source
- UPC (Ultra-polished connectors)
  - Ferrule end-face radius polished at a zero degree angle
  - High return loss
- APC (Angle-polished connectors)
  - Ferrule end-face radius polished at an eight degree angle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



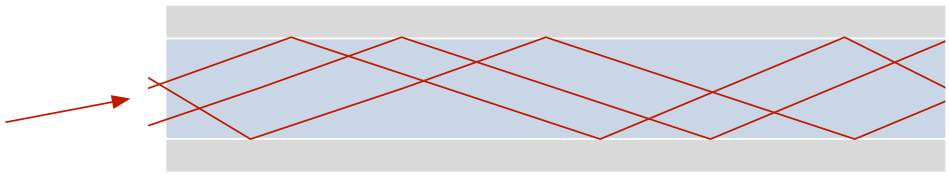




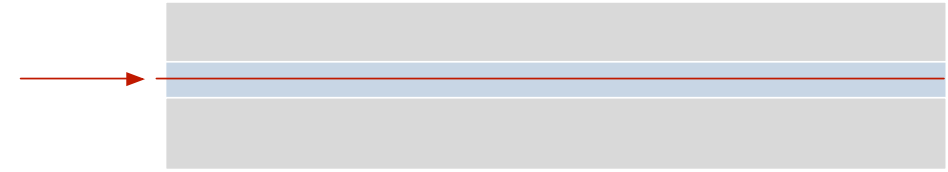
UPC - Ultra-Polished Connectors



APC - Angle-Polished Connectors

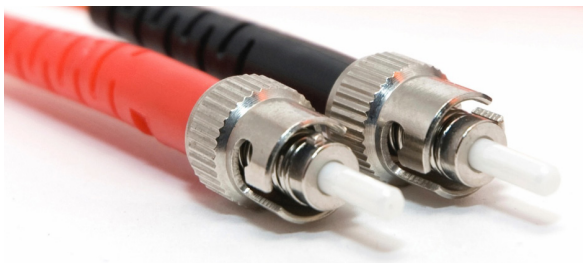


Multi-mode Fiber
Short-range communication, up to 2 km



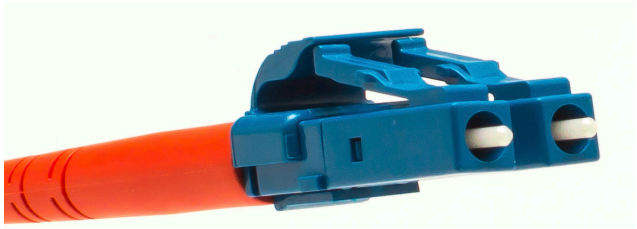
Single-mode Fiber
Long-range communication, up to 100 km

2.1 - Optical Fiber Connectors

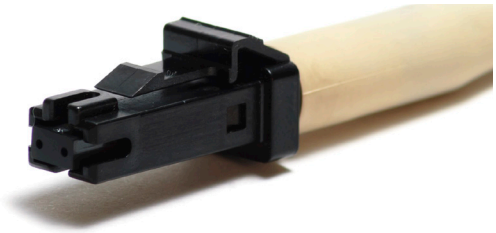


ST - Straight Tip

SC - Subscriber Connector



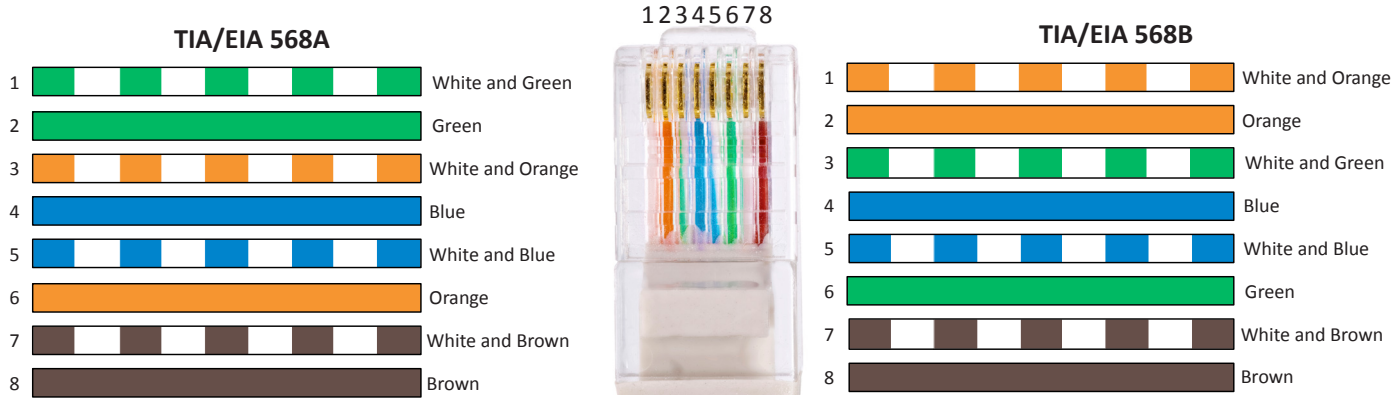
LC - Lucent Connector

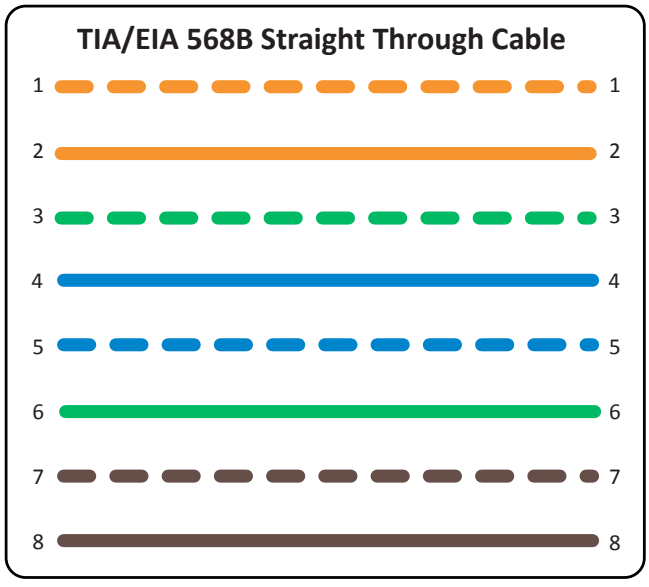


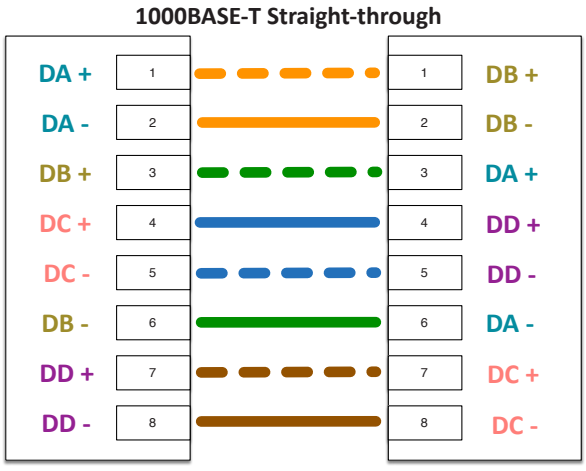
MT-RJ - Mechanical Transfer Registered Jack

2.1 - Copper Termination Standards

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



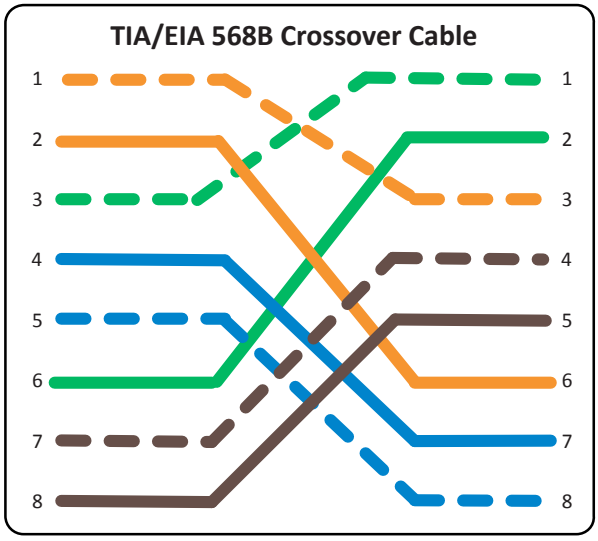


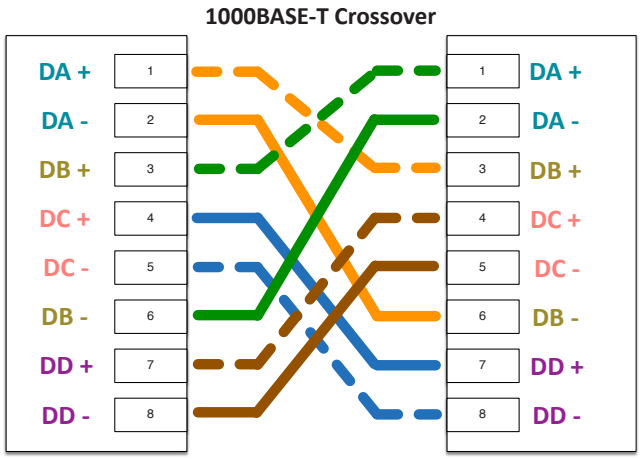


Media Dependent Interface (MDI)
Network Interface Card

Media Dependent Interface Crossover (MDI-X)
Network Switch

2.1 - Copper Termination Standards (continued)





Media Dependent Interface (MDI)
Network Interface Card

Media Dependent Interface (MDI)
Network Interface Card

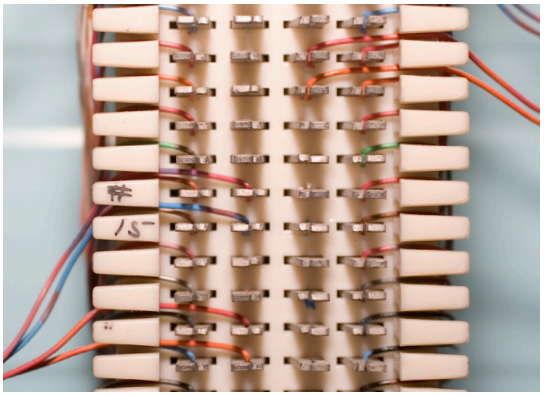
2.1 - Network Termination Points

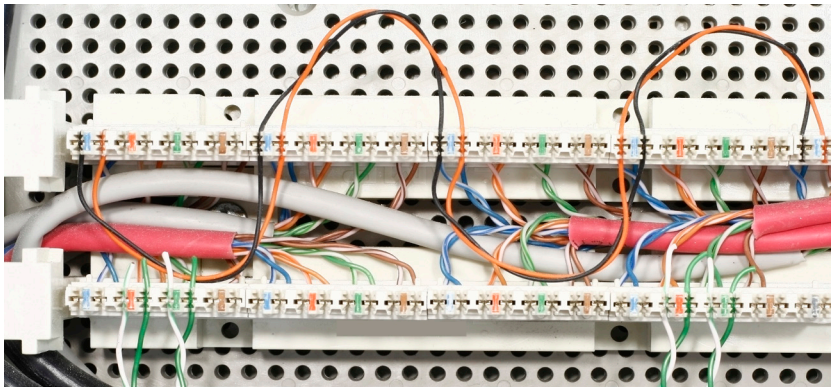
66 block

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

110 block

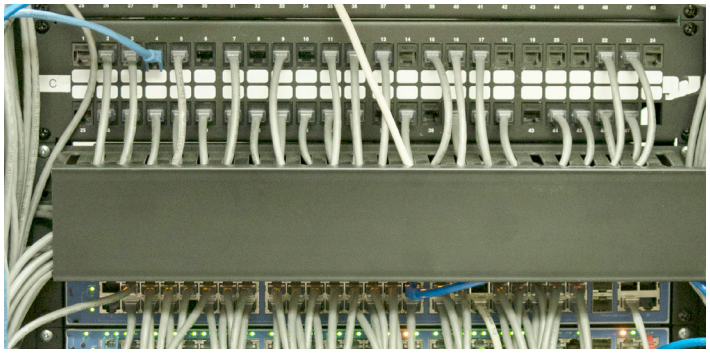
- Wire-to-wire patch panel
  - No intermediate interface required
- Replaces the 66 block
  - Patch Category 5 and Category 6 cables
- Wires are "punched" into the block
  - Connecting block is on top
- Additional wires punched into connecting block
  - Patch the top to the bottom





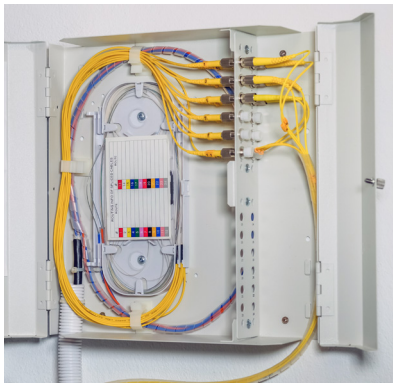
Copper patch panel

- 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



2.1 - Network Transceivers

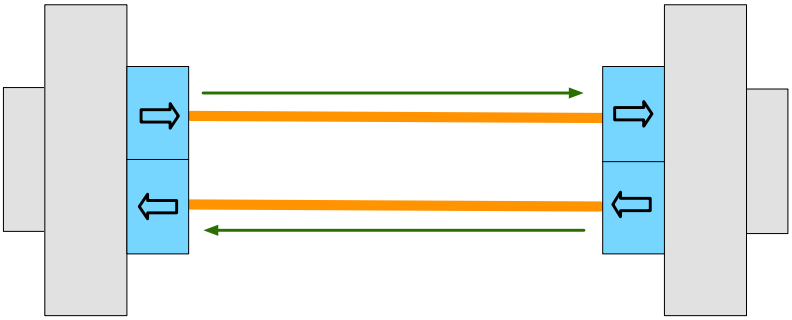
Transceiver
- Transmitter and receiver
  - Usually in a single component
- Provides a modular interface
  - Add the transceiver that matches your network

GBIC
- Gigabit Interface Converter
  - An early transceiver standard
- Common on Gigabit and fibre channel networks
  - Copper and fiber support
- Relative large, and effectively replaced by SFPs

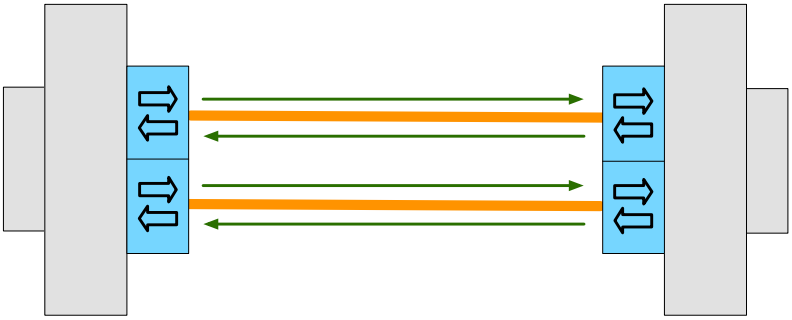
SFP and SFP+
- Small Form-factor Pluggable (SFP)
  - Commonly used to provide 1 Gbit/s fiber
  - 1 Gbit/s RJ45 SFPs also available
- Enhanced Small Form-factor Pluggable (SFP+)
  - Exactly the same size as SFPs
  - Supports data rates up to 16 Gbit/s
  - Common with 10 Gigabit Ethernet

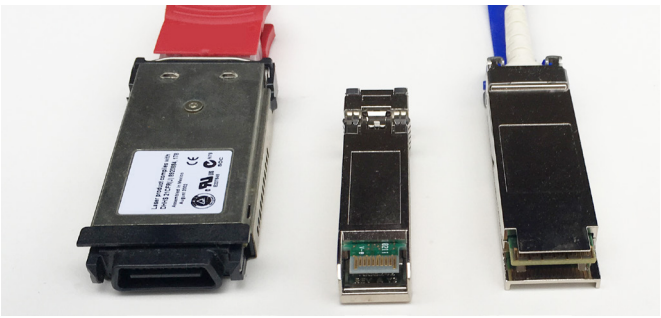
QSFP
- Quad Small Form-factor Pluggable
  - 4-channel SFP = Four 1 Gbit/s = 4 Gbit/s
  - QSFP+ is four-channel SFP+ = Four 10 Gbit/sec = 40 Gbit/sec
- Combine four SFPs into a single transceiver
  - Cost savings in fiber and equipment
- Bi-Directional (BiDi) QSFP and QSFP+
  - Additional efficiency over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

Duplex communication
- Two fibers
  - Transmit and receive



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





GBIC SFP QSFP

2.1 - Ethernet Standards

100 Mbit/s Ethernet
- 100BASE-TX
  - "Fast Ethernet"
  - Category 5 or better twisted pair copper - two pair
  - 100 meters maximum length

1000 Mbit/s (1 Gbit/s) Ethernet
- 1000BASE-T
  - Category 5 or better twisted pair copper - four pair
  - 100 meters maximum length
- 1000BASE-SX
  - Gigabit Ethernet using NIR (near infrared) light wavelength
  - Usually over multi-mode fiber
  - 220 meters to 500 meters, depending on fiber type
- 1000BASE-LX
  - Gigabit Ethernet using long wavelength laser
  - Multi-mode fiber to 550 meters
  - Single-mode fiber to 5 kilometers

10 Gbit/s Ethernet
- 10GBASE-T
  - 2006 standard
  - Frequency use of 500 MHz
    - Well above the 125 MHz for gigabit Ethernet
  - Twisted pair copper cables
    - Cat 6 – 55 meters
    - Cat 6A (augmented) – 100 meters
    - Cat 7 - 100 meters

2.2 - Networking Devices

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

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

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

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

Firewall
- Filters traffic by port number
  - OSI layer 4 (TCP/UDP)
  - Some firewalls can filter through OSI layer 7
- Can encrypt traffic into/out of the network
  - Protect your traffic between sites
- Can proxy traffic
  - A common security technique
- Most firewalls can be layer 3 devices (routers)
  - Usually sits on the ingress/egress of the network

Wireless access point (WAP)
- Not a wireless router
  - A wireless router is a router and a WAP in a single device
- WAP is a bridge
  - Extends the wired network onto the wireless network
  - WAP is an OSI layer 2 device

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

Wireless range extender
- Wireless never seems to stretch far enough
  - We can't always choose where to install an access point
- Extend the reach of a wireless network
  - A wireless repeater

VoIP endpoint
- Some people still communicate using voice
  - We now send this using VoIP
- The device can now be anything
  - Traditional phone handset, desktop application, mobile device app

2.3 - Advanced Networking Devices

Multilayer 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

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

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

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

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

Identification technologies
- Signature-based
  - Look for a perfect match
- Anomaly-based
  - Build a baseline of what's "normal"
- Behavior-based
  - Observe and report
- Heuristics
  - Use artificial intelligence to identify

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

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

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

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

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

RADIUS (Remote Authentication Dial-in User Service)
- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
- 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

2.3 - Advanced Networking Devices (continued)

UTM / All-in-one security appliance

- Unified Threat Management (UTM) / Web security gateway
- URL filter / Content inspection
- Malware inspection
- Spam filter
- CSU/DSU
- Router, Switch
- Firewall
- IDS/IPS
- Bandwidth shaper
- VPN endpoint

Next-generation Firewalls (NGFW)

- The OSI Application Layer
  - Layer 7 firewall
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection
  - Deep packet inspection
- Requires some advanced decodes
  - Every packet must be analyzed, categorized, and a security decision determined

VoIP technologies

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

Content filtering

- Control traffic based on data within the content
  - Data in the packets
- 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

2.4 - Virtual Networking

Network virtualization

- Server farm with 100 individual computers
  - 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?

The hypervisor

- Virtual Machine Manager
  - Manages the virtual platform and guest OS
- May require a CPU that supports virtualization
  - Can improve performance
- Hardware management
  - CPU, networking, security

Network requirements

- Most client-side virtual machine managers have their own virtual (internal) networks
- Shared network address
  - The virtual machine shares the same IP address as the physical host
  - Uses a private IP address internally
  - Uses NAT to convert to the physical host IP
- Bridged network address
  - The VM is a device on the physical network
- Private address
  - The VM does not communicate outside of the virtual network

2.4 - Network Storage

NAC 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

Jumbo frames

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

2.4 - Network Storage (continued)

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

Fibre Channel over the data network
- Fibre Channel over Ethernet (FCoE)
  - Use Fibre Channel over an Ethernet network
  - No special networking hardware needed
  - Usually integrates with an existing Fibre Channel infrastructure
  - Not routable
- Fibre Channel over IP (FCIP)
  - Encapsulate Fibre Channel data into IP packets
  - Fibre Channel tunneling
  - Geographically separate the servers from the storage

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

InfiniBand
- High-speed switching topology
  - Alternative to Fibre Channel
- Copper and Fiber options
  - QSFP connectors
- Popular use in research and supercomputers
  - Designed for high speeds and low latency
  - 100 Gbit/sec and 200 Gbit/sec speeds are common
  - Links can be aggregated for higher throughputs (4x, 8x, 12x links)

2.5 - WAN Services

ISDN - Integrated Services Digital Network
- BRI – Basic Rate Interface (2B+D)
  - Two 64 kbit/s bearer (B) channels
  - One 16 kbit/s signaling (D) channel
- PRI – Primary Rate Interface
  - Delivered over a T1 or E1
  - T1 – 23B + D
  - E1 – 30B + D + alarm channel
  - Commonly used as connectivity from the PSTN to large phone systems (PBX)

T1 / E1
- T-Carrier Level 1
  - Time-division multiplexing
  - North America, Japan, South Korea
  - 24 channels - 64 kbit/s per channel
  - 1.544 Mbit/s line rate
- E-Carrier Level 1
  - E is for Europe
  - 32 channels - 64 kbit/s per channel
  - 2.048 Mbit/s line rate

T3 / DS3 / E3
- T-Carrier Level 3
  - Delivered on coax (BNC connectors)
  - DS3 is the data carried on a T3
- T3
  - Twenty-eight T1 circuits - 44.736 Mbit/s
- E3
  - Sixteen E1 circuits - 34.368 Mbit/s

Network	Channels	Line Rate
T1	24 channels at 64 kbit/s each	1.544 Mbit/s
E1	32 channels at 64 kbit/s each	2.048 Mbit/s
T3	28 T1 circuits 672 channels	44.736 Mbit/s
E3	16 E1 circuits 512 channels	34.368 Mbit/s

OC (Optical Carrier)
- SONET (Synchronous Optical Networking)
- Commonly implemented by carriers on SONET rings

SONET	Line Rate
OC-3	155.52 Mbit/sec
OC-12	622.08 Mbit/sec
OC-48	2.49 Gbit/sec
OC-192	9.95 Gbit/sec

2.5 - WAN Services (continued)

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

Metro Ethernet
- Metropolitan-area network
  - A contained regional area
- Connect your sites with Ethernet
  - A common standard
  - Not your typical WAN connection
- The Ethernet is usually running over a different topology
  - Pure Ethernet
  - Ethernet over SDH, MPLS, or DWDM

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

Dialup
- Network with voice telephone lines
  - Analog lines with limited frequency response
- 56 kbit/s modems - Compression up to 320 kbit/s
- Relatively slow throughput - Difficult to scale
- Legacy systems, network utility
  - May be difficult to find a modem

2.5 - WAN Transmission Mediums

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

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

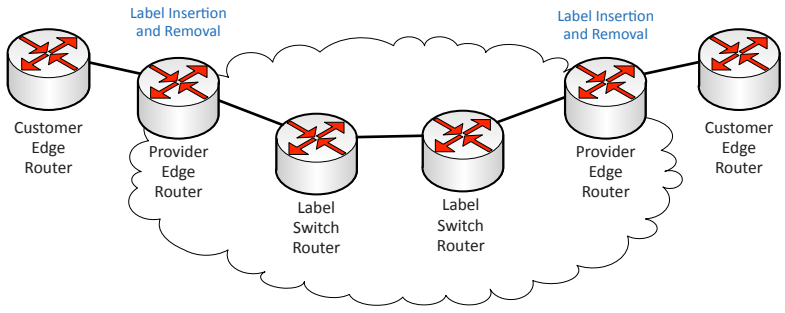
Fiber
- High speed data communication - Frequencies of light
- Higher installation cost than copper
  - Equipment is more costly and more difficult to repair
  - Communicate over long distances
- Large installation in the WAN core
  - Supports very high data rates
  - SONET, wavelength division multiplexing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

Wireless
- Use the cellular network - Wireless WAN
  - Use an external hotspot or mobile phone
- Intermittent communication
  - Security system, daily point-of-sale reporting and updates
- Roaming communication
  - Field service, travel
- Limited by coverage and speed
  - Remote areas can be a challenge

2.5 - WAN Technologies

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

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



2.5 - WAN Technologies

ATM
- Asynchronous Transfer Mode
  - A common protocol transported over SONET
- 53-byte "cells" spaced evenly apart
  - 48-byte for data, 5-byte routing header
- High throughput, real-time, low latency
  - Data, voice, and video
- Max speeds of OC-192
  - Limits based on segmentation and reassembly (SAR)

Frame relay
- One of the first cost-effective WAN types
  - Departure from circuit-switched T1s
- LAN traffic is encapsulated into frame relay frames
- Frames are passed into the "cloud"
  - Magically appear out the other side
- Usually 64 Kbits/s through DS3 speeds
- Effectively replaced by MPLS
  - And other WAN technologies

PPP (Point-to-point protocol)
- Create a network connection between two devices
  - OSI layer 2 / data link protocol
  - Communicate using many different protocols
- Works almost anywhere
  - Dial-up connections, serial links, mobile phone, DSL (PPPoE)
- Provides additional data link functionality
  - Authentication
  - Compression
  - Error detection
  - Multilink

PPPoE
- Encapsulate point-to-point protocol over Ethernet
  - The past with the present
- Common on DSL networks
  - Telephone providers know PPP
- Easy to implement
  - Support in most operating systems
  - No routing required
  - Similar to existing dialup architecture
- Allows competition
  - Once connected, data is switched to the appropriate ISP

DMVPN
- Dynamic Multipoint VPN
  - Common on Cisco routers
- Your VPN builds itself
  - Remote sites communicate to each other
- Tunnels are built dynamically, on-demand
  - A dynamic mesh

SIP trunking
- Session Initiation Protocol
  - Control protocol for VoIP
- Traditional PBX connectivity uses T1/ISDN
  - 23 voice channels, 1 signaling channel
  - When the lines are full, you get a busy signal
- SIP trunking
  - Use SIP/VoIP to communicate to an IP-PBX provider
- More efficient use of bandwidth
  - Less expensive than ISDN lines
  - More phone system options

2.5 - WAN Termination

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

CSU/DSU - Channel Service Unit / Data Service Unit
- Sits between the router and the circuit
- CSU - Connects to the network provider
- DSU - Connects to the data terminal equipment (DTE)
- Physical device - Or built-in to the router

CSU/DSU connectivity
- From the demarc
  - RJ-48c wiring
- To the router
  - Serial connection, v.35, RS-232
- May also include monitor jacks
  - Useful for diagnostic equipment

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

3.1 - Network Documentation

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

Mapping the network
- Networks are built in phases
  - Large chunks at a time
- You can't see most of it
  - Fiber and wires in the walls and ceiling
- Documentation is essential
  - Both physical and logical
- One of the best things you can do
  - Especially as the new hire

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

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

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

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

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

System labeling
- Many people will work on a single workstation or server
  - There needs to be a standard reference
- Unique system ID
  - Asset tag
  - System name
  - Serial number
- Clearly visible
  - Especially in a data center

Circuit labeling
- WAN circuits aren't a problem
  - Until they are a problem
  - It's outside your control
- All components of the WAN
  - Demarc interface
  - CSU/DSU
  - Router
- Label information
  - WAN provider Circuit ID
  - WAN provider phone number
  - Internal reference name

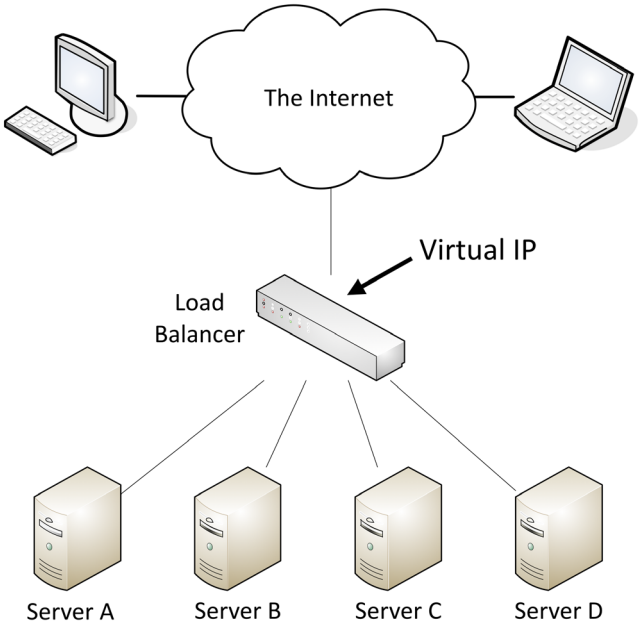
Patch panel labeling
- Not much real estate
  - Fit a lot into a small space
- Number each side of the link
  - Incremental
  - Geographically descriptive

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

3.2 - Availability Concepts

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

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



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

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

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

3.2 - Power Management

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

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

Dual-power supplies
- Redundancy
  - Internal server power supplies
  - External power circuits
- Each power supply can handle 100% of the load
  - Would normally run at 50% of the load
- Hot-swappable
  - Replace a faulty power supply without powering down

3.2 - Recovery Sites

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

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

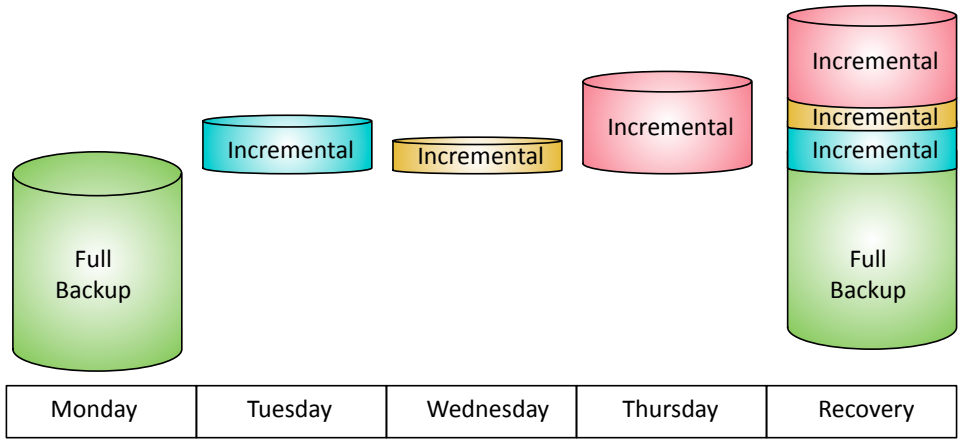
Hot site
- An exact replica
  - Duplicate everything
- Stocked with hardware
  - Constantly updated
  - You buy two of everything
- Applications and software are constantly updated
  - Automated replication
- Flip a switch and everything moves
  - This may be quite a few switches

3.2 - Backup and Recovery

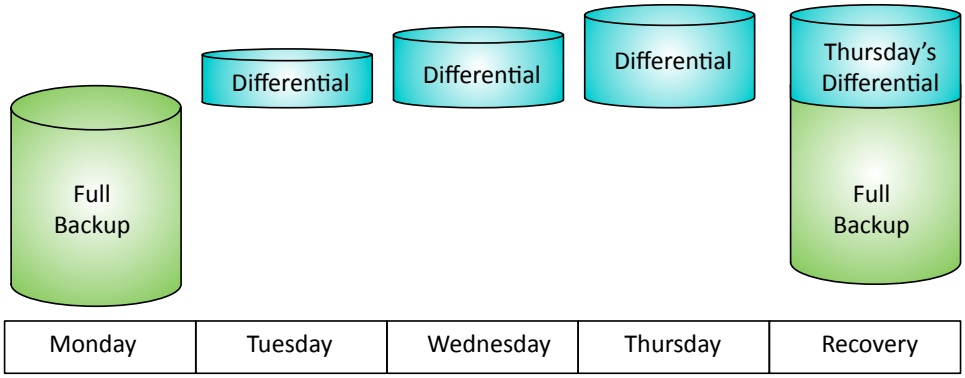
File backups
- The archive attribute
  - Set when a file is modified
- Full - Everything
  - You'll want this one first
- Incremental
  - All files changed since the last incremental backup
- Differential
  - All files changed since the last full backup

Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

Incremental Backup
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup and last incremental backup
  - These are usually smaller than the full backup
- A restoration requires the full back and all of the incremental backups



Differential Backup
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup
  - These usually grow larger as data is changed
- A restoration requires the full back and the last differential backup



3.2 - Backup and Recovery (continued)

Recovery
- Mean time to restore (MTTR)
  - Mean time to repair
- Mean time between failures (MTBF)
  - Predict the time between failures
- Recovery may have a predefined service level agreement (SLA)
  - Contractual recovery expectations
  - May include penalties for not meeting certain service levels

Taking snapshots
- The cloud is always in motion
  - Application instances are constantly built and torn down
- Snapshots can capture the current configuration and data
  - Preserve the complete state of a device, or just the configuration
- Revert to known state
  - Fall back to a previous snapshot
- Rollback to known configuration
  - Don't modify the data, but use a previous configuration
- Live boot media
  - Run the operating system from removable media - very portable!

3.3 - Process Monitoring

Log management
- Very diverse log sources
  - And quite large
- Usually sent via syslog
  - Stored in a large drive array
- Massive storage requirement
  - There's never enough
- Data rollup becomes important
  - Take samples every minute
  - Keep 5-minute samples for 30 days
  - After 30 days, rollup to 1 hour sample times

Data graphing
- Many different data sources
  - Raw logs
  - Summarized metadata
- Usually managed through a SIEM
  - Turn raw data into something visual
- Graphing can require extensive resource utilization
  - Churn through terabytes of data
- Can use built-in graphs
  - Or build custom reports

Port scanning
- 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

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

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

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

Protocol analyzers
- Solve complex application issues
  - Get into the details
- Gathers packets 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

3.3 - Event Management

Interface monitoring

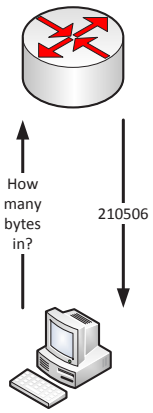
- Up or down
  - The most important statistic
  - No special rights or permissions required
  - Green is good, red is bad
- Alarming and alerting
  - Notification should an interface fail to report
  - Email, SMS
- Short-term and long-term reporting
  - View availability over time
- Not focused on additional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

SIEM

- Security Information and Event Management
  - 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

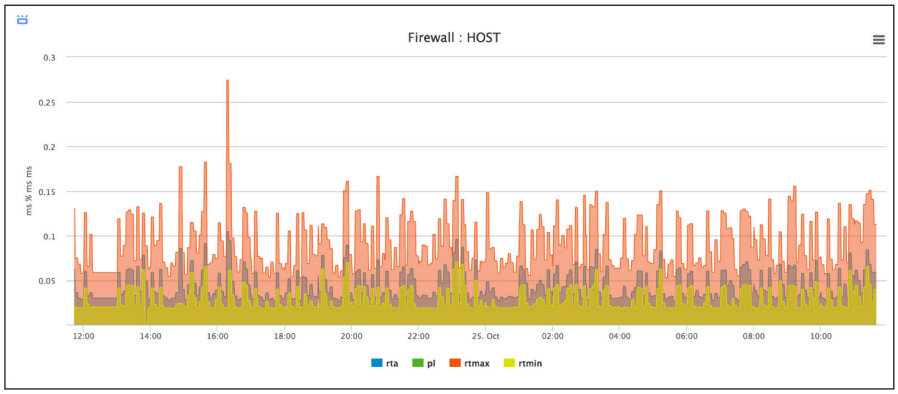
SNMP

- Simple Network Management Protocol
  - A database of data (MIB) - Management Information Base
- SNMP v1 - The original
  - Structured tables, in-the-clear
- SNMP v2 – A good step ahead
  - Data type enhancements, bulk transfers, still in-the-clear
- SNMP v3 - The new standard
  - Message integrity, authentication, encryption
- SNMP information can be very detailed
  - Access should be very limited



Syslog

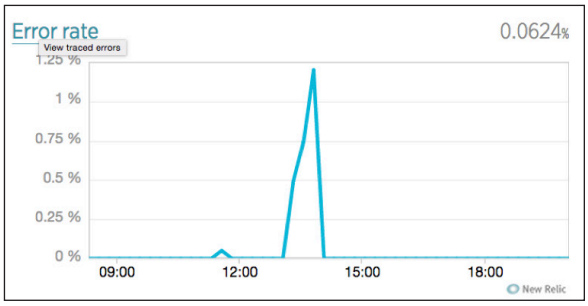
- Standard for message logging
  - Diverse systems, consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM
- You're going to need a lot of disk space



3.3 - Performance Metrics

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



Interface monitoring

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

3.4 - Remote Access

IPSec (Internet Protocol Security)

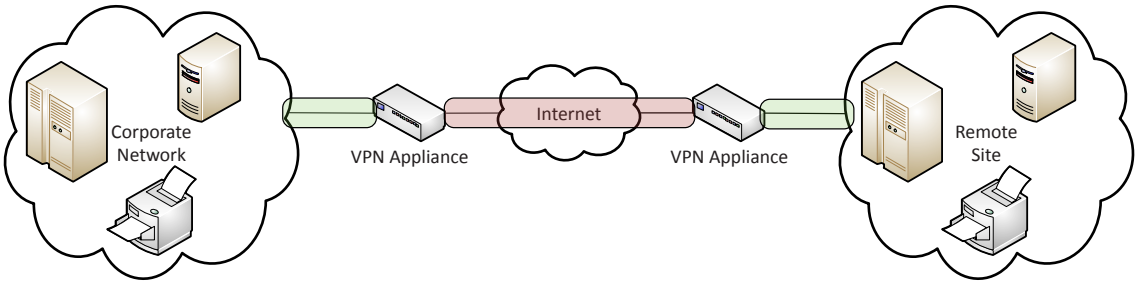
- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security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

SSL VPN (Secure Sockets Layer VPN)

- Uses common SSL/TLS protocol (tcp/443)
  - Avoids running into most firewall issues
- No big VPN clients
  - Usually remote access communication
- Authenticate users
  - No requirement for digital certificates or shared passwords (like IPSec)
- Can be run from a browser or from a light VPN client
  - Across many operating systems

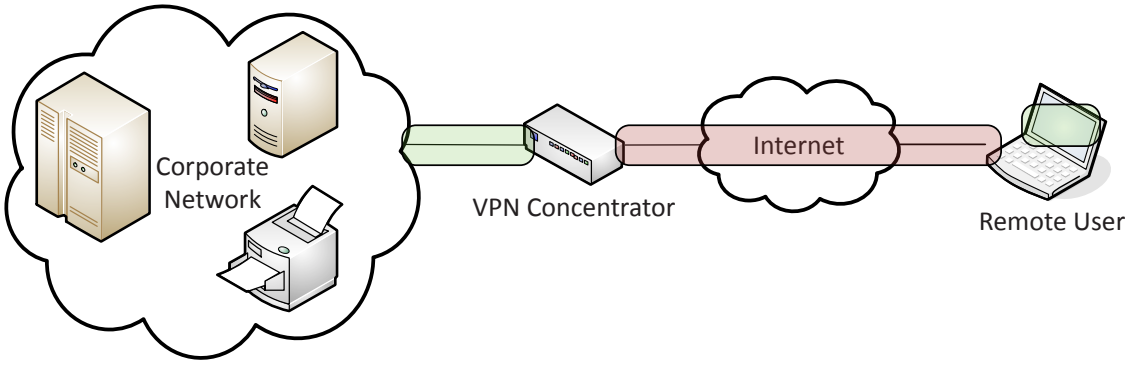
Site-to-Site VPNs

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



Host-to-Site VPNs

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



DTLS VPN

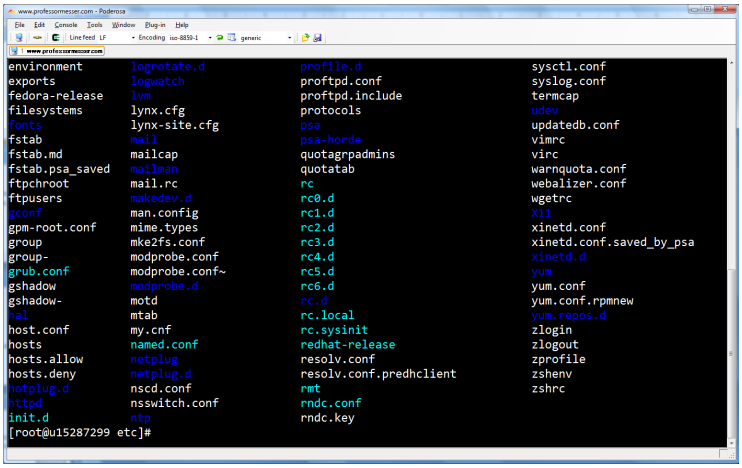
- Datagram Transport Layer Security
  - The security of SSL/TLS, the speed of datagrams
  - Transport using UDP instead of TCP
- TCP brings some great features
  - Packet reordering
  - Retransmission of lost/dropped data
- TCP sometimes gets in the way
  - Streaming, VoIP
  - When you lose a packet, it's too late to recover it

Remote desktop access

- 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
- Commonly used for technical support - and for scammers

SSH (Secure Shell)

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



3.4 - Remote Access (continued)

Web-based management console
- Your browser
  - The universal client
- Manage a device from an encrypted web-based front-end
  - Connect to the HTTPS URL and login
- The important features are in the browser
  - You may need the CLI for the detailed operations

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

Transferring files
- FTP – File Transfer Protocol
  - Transfers files between systems
  - Authenticates with a username and password
  - Full-featured functionality (list, add, delete, etc.)
- FTPS
  - FTP over SSL (FTP-SSL)
  - File Transfer Protocol Secure
  - This is not SFTP
- SFTP
  - SSH File Transfer Protocol
  - Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal
- TFTP – Trivial File Transfer Protocol
  - Very simple file transfer application
  - Read files and write files
  - No authentication
  - May be used to download configurations
  - VoIP phones

3.5 - Policies and Best Practices

Privileged user agreement
- Network/system administrators have access to almost everything
  - With great power comes great responsibility
- Expectations
  - Use other non-privileged methods when appropriate
- Limitations
  - Use privileged access only for assigned job duties
- Signed agreement
  - Everyone understands the policies

Password policies
- Written policy
  - All passwords should expire every 30 days, 60 days, 90 days, etc.
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

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

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

Licensing restrictions
- So many licenses
  - Operating systems, applications, hardware appliances
  - And they all use different methods to apply the license
- Availability
  - Everything works great when the license is valid
  - Meeting the expiration date may cause problems
  - Application may stop working completely
- Integrity
  - Data and applications must be accurate and complete
  - A missing/bad license may cause problems with data integrity

International export controls
- Equipment, information, data
  - Country-specific laws controlling export
- Not only shipment of physical items
  - Includes the transfer of software or information
  - Protect PII
- Dual-use software can be controlled
  - Dual-use for both civilian and military use
  - Security software, malware, hacking tools
- Check with legal team - don't ship unless you're sure

3.5 - Policies and Best Practices (continued)

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

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

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

Incident response policies
- How is an incident identified?
  - Automated monitoring, personal account
- How is the incident categorized?
  - Email issue, brute force attack, DDoS, etc.
- Who responds to an incident?
  - Large list of predefined contacts
- What process is followed?
  - Formal process needs to be created prior to the incident

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

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

Non-disclosure agreement
- NDA (Non-disclosure agreement)
  - Confidentiality agreement / Legal contract
  - Prevents the use and dissemination of confidential information
- Internal
  - Protect the organization's private and confidential information
  - Part of employee security policies
- External
  - Two parties can't disclose private information or company secrets about the other party

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

Physical destruction
- Shredder / pulverizer
  - Heavy machinery - complete destruction
- Drill / Hammer
  - Quick and easy - platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and the electronics
- Incineration

Safety procedures and policies
- Equipment safety
  - Electrical safety policies
- Personal safety
  - Jewelry policy, lifting techniques, fire safety, cable management, safety goggles, etc.
- Handling of toxic waste
  - Batteries, toner
  - Refer to the MSDS (Material Safety Data Sheet)
- Local government regulations
  - Safety laws, building codes, environmental regulations

4.1 - Physical Security

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

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

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

Identification badges
- ID badge
  - Picture, name, other details
  - Must be worn at all times
- May be integrated with door access or a smart card
  - It's more than just a visual identification
- Standardized format
  - Train all employees to look for ID and ask questions if they don't see one

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

Tokens and cards
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token
  - Certificate is on the USB device
- Hardware or software tokens / key fobs
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

Door access controls
- Conventional
  - Lock and key
- Deadbolt
  - Physical bolt
- Electronic
  - Keyless
- Token-based
  - Magnetic swipe card or proximity reader
- Multi-factor
  - Smart card and PIN

4.2 - Authorization, Authentication, and Accounting

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

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

4.2 - Authorization, Authentication, and Accounting (continued)

TACACS
- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

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

SSO with Kerberos
- Authenticate one time
  - Lots of backend ticketing, uses cryptographic tickets
- No constant username and password input! - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly

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

Local authentication
- Credentials are stored on the local device
  - Does not use a centralized database
- Most devices include an initial local account
  - Good devices will force a password change
- Difficult to scale local accounts
  - No centralized administration
  - Must be added or changed on all devices
- Sometimes useful as a backup
  - The AAA server might not be available

Certificate-based authentication
- Smart card - Private key is on the card
- PIV (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- CAC (Common Access Card)
  - US Department of Defense smart card
  - Picture and identification
- IEEE 802.1X
  - Gain access to the network using a certificate
  - On device storage or separate physical device

Auditing
- Log all access details
  - Automate the log parsing
  - OS logins, VPN, device access
- Usage auditing
  - How are your resources used?
  - Are your systems and applications secure?
- Time-of-day restrictions
  - Nobody needs to access the lab at 3 AM

4.2 - Multi-factor Authentication

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

Something you know
- Password
  - Secret word/phrase, string of characters
  - Very common authentication factor
- PIN
  - Personal identification number
  - Not typically contained anywhere on a smart card or ATM card
- Pattern
  - Complete a series of patterns
  - Only you know the right format

4.2 - Multi-factor Authentication (continued)

Something you have
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone - SMS a code to your phone

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

Somewhere you are
- Provide a factor based on your location
  - The transaction only completes if you are in a particular geography
- IP address
  - Not perfect, but can help provide more info
  - Works with IPv4, not so much with IPv6
- Mobile device location services
  - Geolocation to a very specific area
  - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
  - Still not a perfect identifier of location

Something you do
- A personal way of doing things - You're special
- Handwriting analysis
  - Signature comparison or writing technique
- Typing technique - Delays between keystrokes
- Very similar to biometrics - Close to something you are

4.2 - Access Control

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

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

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

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

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

Access Control Lists (ACLs)
- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?

4.3 - Wireless Encryption

Wireless encryption
- All wireless computers are radio transmitters and receivers - anyone can listen in
- Solution: Encrypt the data
  - Everyone gets the password
  - Or their own password
- Only people with the password can transmit and listen
  - WPA and WPA2

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

Temporal Key Integrity Protocol
- Mixed the keys
  - Combines the secret root key with the IV
- Adds sequence counter - prevents replay attacks
- Implements a 64-bit Message Integrity Check
  - Protects against tampering
- TKIP has it's own set of vulnerabilities
  - Deprecated in the 802.11-2012 standard

WPA2 and CCMP
- WPA2 certification began in 2004
  - AES (Advanced Encryption Standard) replaced RC4
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
- CCMP block cipher mode
  - Uses AES for data confidentiality
  - 128-bit key and a 128-bit block size
  - Requires additional computing resources
- CCMP security services
  - Data confidentiality (AES), authentication, and access control

4.3 - Wireless Authentication and Security

EAP
- EAP - Extensible Authentication Protocol
- An authentication framework
- Many different ways to authenticate based on RFC standards
- WPA and WPA2 use five EAP types as authentication mechanisms

EAP types
- EAP-FAST
  - EAP Flexible Authentication via Secure Tunneling
  - Cisco's proposal to replace LEAP (Lightweight EAP - previously used with WEP)
  - Lightweight and secure
- EAP-TLS (EAP Transport Layer Security)
  - Strong security, wide adoption
  - Support from most of the industry
- EAP-TTLS (EAP Tunneled Transport Layer Security)
  - Support other authentication protocols in a TLS tunnel
  - Use any authentication you can support, maintain security with TLS

PEAP
- Protected Extensible Authentication Protocol
  - Protected EAP
- Created by Cisco, Microsoft, and RSA Security
- Encapsulates EAP in a TLS tunnel, one certificate on the server
  - Combined a secure channel and EAP
- Commonly implemented as PEAPv0/EAP-MSCHAPv2
  - Authenticates to Microsoft's MS-CHAPv2 databases

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

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 (not actual security)

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

4.4 - 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

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 bad guys 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 amplification

- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common 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

Example of a DNS record used in DDoS amplification attack

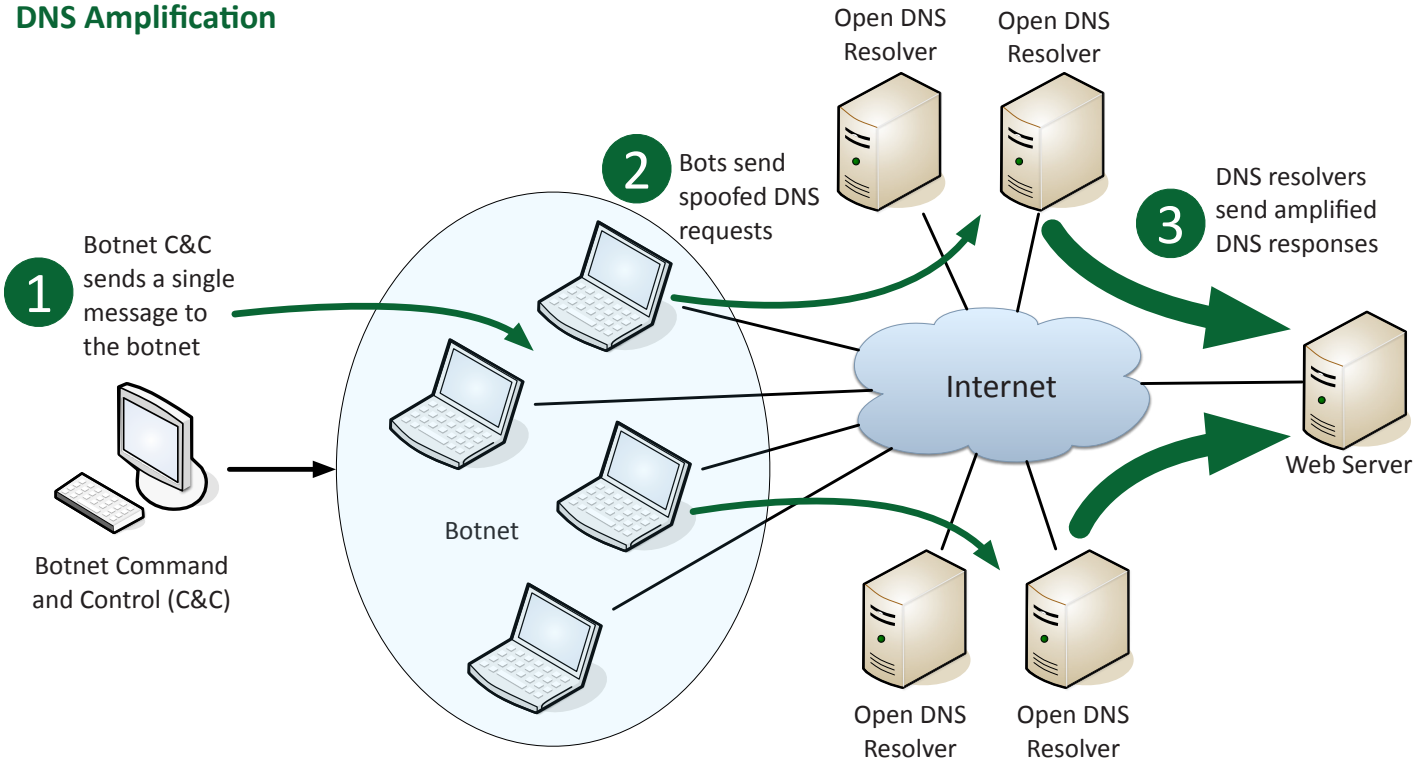
```
$ dig ANY isc.org @75.75.75.75
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.8.3-P1 <<>> ANY isc.org @75.75.75.75
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27443
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;isc.org.                       IN      ANY

;; ANSWER SECTION:
isc.org.            1712       IN      DNSKEY    257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr hhCeFvAZih7yJHf8ZGfW6hd38hXG/
xylYCO6Krpbdojwx8YMXLA5/kA+ u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPClw+vT+U8eXEJmO20jISlULgqy3 47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz
Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3oA8lVUgEf/rzeC/bB yBNsO70aEFTd
isc.org.            1712       IN      DNSKEY    256 3 5 AwEAAbDs5ksq3roEgvfiN+HHzPqErVe5lOpQ6bNjRDH/BSUisBM8gvgd ZGIdctVRYl8vgAJcpc//
YE4vpNrDsfgGfiyz+Fd2pCJTXGm6mDoAAMLJ FrG64gYVdby2AnI7sonZlT5PHjS0dKBhhf0Pd/+SgKNIf25wh1UzFRCp CXznWdER
isc.org.            1712       IN      RRSIG     DNSKEY 5 2 7200 20170712230419 20170612230419 12892 isc.
org. MZ8PU+4k/wwHDw3jdyzUpm74MFhbFvCemlJ61ho0gkDGNhEqn8/yC1Fs oaT7PK9U8hknlrppp/os08yUifegPsvO1mhezTfIEHTP+JPJS6VO0G5A
a9QHQtVO2FOPuR7HW2AQysldFL9pfvwOlKkzm4yuuhrM2BqhMeSZimo6 VvolWqHyE58dOHoyeylmcvmNb45qoR4spKZR9A1hdxesYgI1tosw9tTd
PswnkyO3rizmFjABzcXDUeKSlodPRr1hZd6rNRRacIeiskPxw8E6WTnT 0RzOM7nFBDIKeTixA59xlPpIN2t+xh1zu8tQ5NsMF2CJK+b5LZTjovEg 9ho9NA==
isc.org.            1712       IN      RRSIG     DNSKEY 5 2 7200 20170712230419 20170612230419 60321 isc.org.
```

DNS Amplification



4.4 - Social Engineering

Effective social engineering

- Constantly changing - You never know what's next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or associate

Social engineering principles

- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / Social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week
- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity - Act quickly, don't think
- Familiarity / Liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

How I Lost My $50,000 Twitter Username

- Naoki Hiroshima - @N
  - https://medium.com/cyber-security/24eb09e026dd
- Bad guy calls PayPal and uses social engineering to get the last four digits of the credit card on file
- Bad guy calls GoDaddy and tells them he lost the card, so he can't properly validate. But he has the last four, does that help?
  - GoDaddy let the bad guy guess the first two digits of the card
  - He was allowed to keep guessing until he got it right
  - Social engineering done really, really well
- Bad guy is now in control of every domain name
  - And there were some good ones
- Bad guy extorts a swap
  - Domain control for @N, owner agrees
- Twitter reviewed the case for a month
  - Eventually restored access to @N

4.4 - Insider Threats

Insider threats

- We give people tons of access
  - Least privilege, anyone?
- You have more access than others just by entering the building
  - Lock away your documents
  - Some organizations have very specific procedures
- Significant security issues
  - Harms reputation
  - Critical system disruption
  - Loss of confidential or proprietary information
- Innocent employees - Phishing scams, hacking scams
- Careless employees - Using a laptop for personal use
- Disgruntled employees - Someone is out to get you
- Defense in depth - Cover all possible scenarios

Insider threat research

- Computer Emergency Response Team
- Insider threat research
  - 2017 U.S. State of Cybercrime Survey
  - http://www.cert.org/insider_threat/
- 20% of attacks caused by insiders
  - 43% said that damage from insider attack was more damaging than an outsider attack
- 76% of insider incidents handled without legal action
  - We never really hear about these

4.4 - Logic Bombs

Logic Bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Time bomb
  - Time or date
- User event
  - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Real-world logic Bombs

- March 19, 2013, South Korea
  - Email with malicious attachment sent to South Korean organizations
  - Posed as a bank email
  - Trojan installs malware
- March 20, 2013, 2 p.m. local time
  - Malware logic-bomb activates
  - Storage and master boot record deleted, system reboots
- Boot device not found
  Please install an operating system on your hard disk.

4.4 - Logic Bombs (continued)

Real-world logic Bombs

- December 17, 2016, 11:53 p.m.
- Kiev, Ukraine, high-voltage substation
- Logic bomb begins disabling electrical circuits
  - Malware mapped out the control network
- Began disabling power at a predetermined time
- Customized for SCADA networks
  - Supervisory Control and Data Acquisition

Preventing a logic bomb

- Difficult to recognize - Each is unique
  - No predefined signatures
- Process and procedures - Formal change control
- Electronic monitoring
  - Alert on changes
  - Host-based intrusion detection, Tripwire, etc.
- Constant auditing
  - An administrator can circumvent existing systems

4.4 - Rogue Access Points

Rogue access points

- A significant potential backdoor
  - Huge security concerns
- 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 connection type
  - Enable port security, limit MAC addresses per port

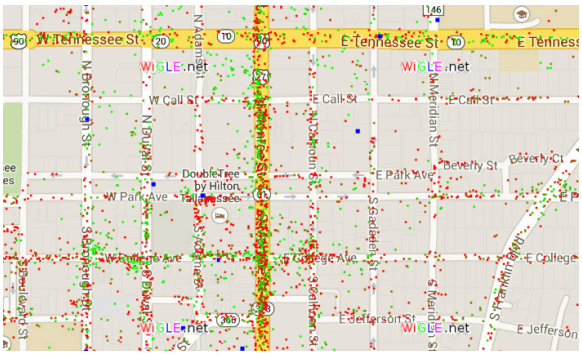
Wireless evil twins

- Buy a wireless access point
  - Less than $100 US
- Configure it exactly the same way as an existing network
  - Same SSID and security settings
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPN

4.4 - Wardriving

Wardriving

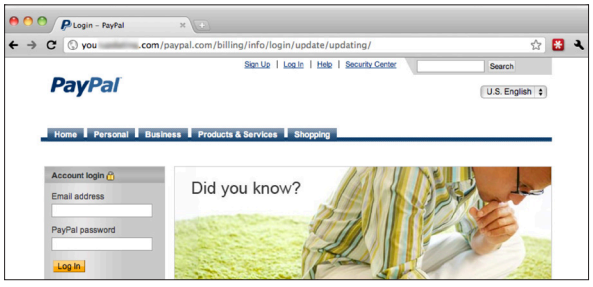
- Combine WiFi monitoring and a GPS
  - Hop in your car and go!
- Huge amount of intel in a short period of time
  - And often some surprising results
- All of this is free
  - Kismet, inSSIDer
  - Wireless Geographic Logging Engine - http://wigle.net
- Always an alternative
  - Warflying, warbiking



4.4 - Phishing

Phishing

- Social engineering with a touch of spoofing
  - Often delivered by spam, IM, etc.
  - Very remarkable when well done
- Don't be fooled - Check the URL
- Usually there's something not quite right
  - Spelling, fonts, graphics
- Vishing is done over the phone
  - Fake security checks or bank updates



Spear phishing

- Phishing with inside information
  - Makes the attack more believable
  - Spear phishing the CEO is "whaling"
- April 2011 - Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operations staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 - Oak Ridge National Laboratory
  - Email from the "Human Resources Department"
  - 530 employees targeted, 57 people clicked, 2 were infected
  - Data downloaded, servers infected with malware

4.4 - Ransomware

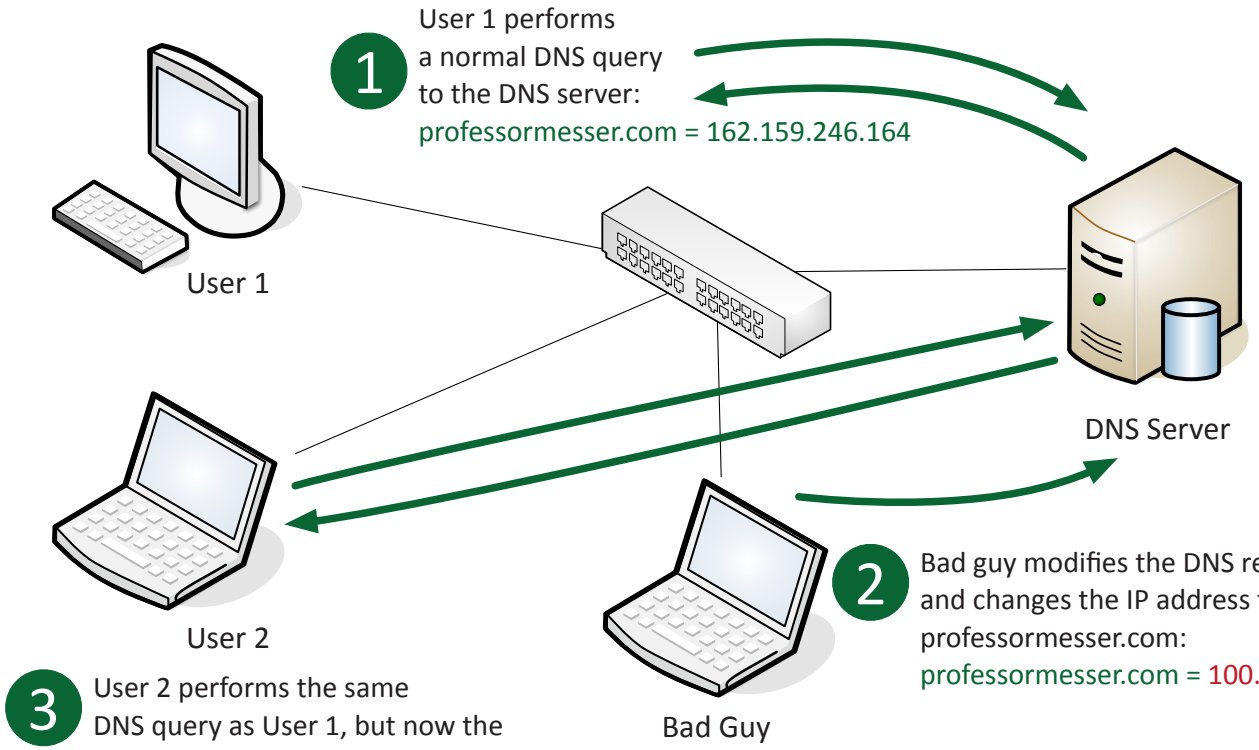
Your data is valuable
- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth?
  - There's a number

Ransomware
- The bad guys want your money
  - They'll take your computer in the meantime
- May be a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

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

Protecting against ransomware
- Always have a backup
  - An offline backup, ideally
- Keep your operating system up to date
  - Patch those vulnerabilities
- Keep your applications up to date - security patches
- Keep your anti-virus/anti-malware signatures up to date
  - New attacks every hour
- Keep everything up to date

4.4 - DNS Poisoning



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

4.4 - Spoofing

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

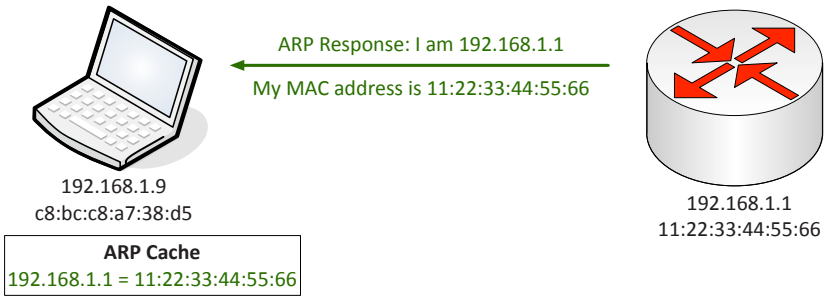
MAC spoofing
- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate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

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

1

A legitimate response to an ARP request is received from the default gateway.

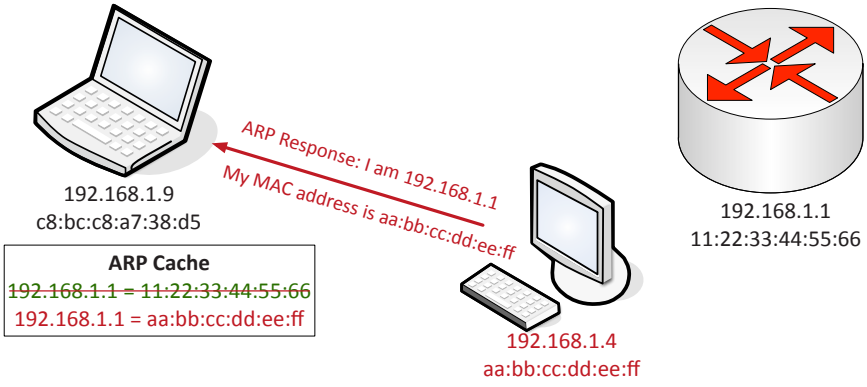
The ARP response is cached on the local device.



2

An attacker sends an ARP response that spoofs the IP address of the router and includes the attacker's MAC address.

The malicious ARP information replaces the cached record, completing the ARP poisoning.



4.4 - Wireless Deauthentication

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

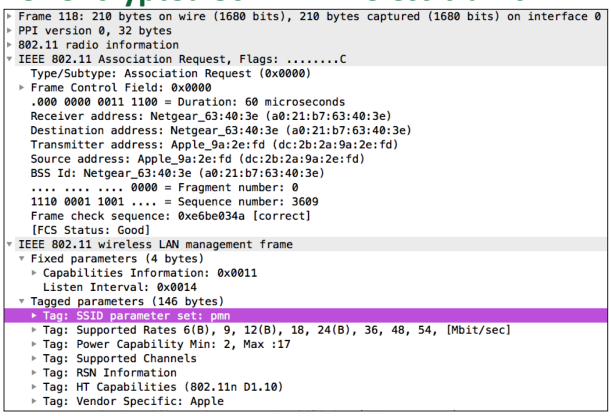
802.11 management frames
- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/ disassociate with an access point, etc.
- Original wireless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

4.4 - Wireless Deauthentication (continued)

Protecting against disassociation

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

Unencrypted 802.11 wireless traffic



4.4 - Brute Force Attacks

Brute force

- The password is the key
  - Secret phrase, stored hash
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

Dictionary attacks

- People use common words as passwords
  - You can find them in the dictionary
- If you're using brute force, you should start with the easy ones
  - password, ninja, football
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- This will catch the low-hanging fruit
  - You'll need some smarter attacks for the smarter people

4.4 - VLAN Hopping

VLAN hopping

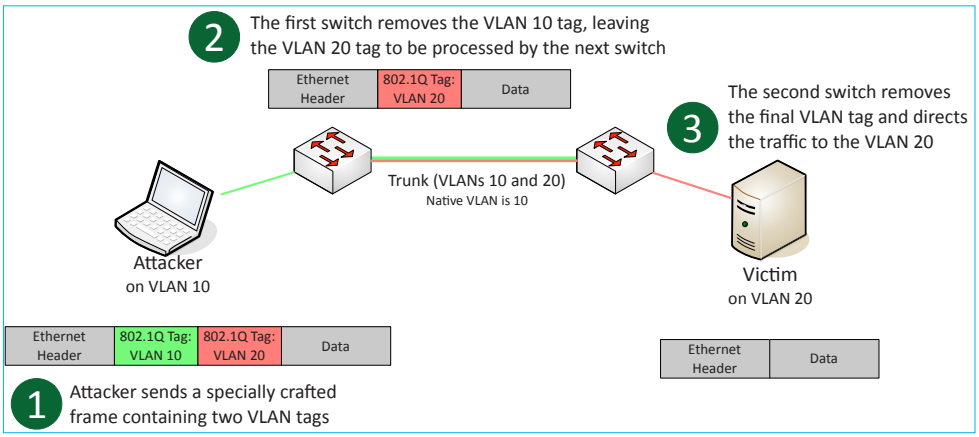
- Define different VLANs
- You only have access to your VLAN
  - Good security best practice
- "Hop" to another VLAN - this shouldn't happen
- Two primary methods
  - Switch spoofing and double tagging

Switch spoofing

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

Double tagging

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



4.4 - Man-in-the-Middle

Man -in- the-middle

- How can a bad guy watch without you knowing?
  - Man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security

Man-in-the-browser

- What if the middleman was on the same computer as the victim?
  - The calls are coming from inside the browser!
  - Malware/Trojan does all of the proxy work
- Huge advantages for the bad guys
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The man-in-the-browser waits for you to login to your bank
  - And cleans you out

4.4 - Vulnerabilities and Exploits

Vulnerabilities and exploits

- Vulnerability
  - 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
- Exploit
  - Take advantage of a vulnerability
  - Gain control of a system
  - Modify data
  - Disable a service

Zero-day attacks

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

4.5 - Device Hardening

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 WAP or router
  - http://www.routerpasswords.com

Avoid common passwords

- People use common words as passwords
  - You can find them in the dictionary
- Brute force attackers start with the easy ones
  - password, ninja, football
- Many common wordlists are available
  - Some are customized by language or line of work

Upgrading firmware

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

File hashing

- Hashing represents data as a short string of text
  - A message digest
- Unique value
  - A hash is unique to a particular data structure
  - The hash will be different if the data changes
- Verify a downloaded file (integrity)
  - Hashes may be provided on the download site
  - Compare the downloaded file hash with the posted hash value

Disabling unnecessary services

- Every service has the potential for trouble
  - The worst vulnerabilities are 0-day
- "Unnecessary" isn't always obvious
  - Windows 7 includes over 130 services by default
  - Windows 10 has over 240
- This may require a lot of research
  - Many different sources
  - Don't rely on the manufacturer
- Trial and error may be necessary
  - Testing and monitoring

Watching the network

- There's a wealth of information in the packets
  - Some of it is very sensitive information
- It's exceptionally easy to pull this out of the air
  - Your coffee break could cost you
- Use encrypted protocols and technologies
  - Browser, email, terminal, file transfer, encrypted tunnels

4.5 - Device Hardening (continued)

Secure protocols
- SSH - Secure Shell
  - Terminal sessions; use instead of Telnet
- SFTP - Secure (SSH) File Transfer Protocol
  - File transfer using SSH instead of FTP
- SNMPv3 - Simple Network Management Protocol
  - Version 3 added encrypted communication instead of SNMPv1 and v2
- TLS/SSL - Transport Layer Security / Secure Sockets Layer
  - HTTP inside of TLS is HTTPS
- IPsec - Internet Protocol Security
  - Encrypt at the IP packet level

Generating new keys
- We communicate to network devices over encrypted channels
  - HTTPS, SSH
- Encryption keys are usually managed on the device
  - SSL/TLS keys for HTTPS, SSH keys
- Anyone with the key can potentially decrypt administrative sessions
  - Or gain access to the device
- Update or change the keys during the installation
  - Have a formal policy to outline processes and procedures

Disabling unused TCP and UDP ports
- Control traffic based on data within the content
  - Data in the packets
- Use a firewall to allow or restrict port numbers
  - TCP and UDP filtering
- Firewall location
  - Personal/Software firewall
  - Network-based firewall

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

4.6 - Mitigation Techniques

IPS signature management
- You determine what happens when unwanted traffic appears
  - Block, allow, send an alert, etc.
- Thousands of rules - Or more
- Rules can be customized by group
  - Or as individual rules
- This can take time to find the right balance
  - Security / alert "noise" / false positives

Device hardening
- No system is secure with the default configurations
  - You need some guidelines to keep everything safe
- Hardening guides are specific to the software or platform
  - Get feedback from the manufacturer or Internet interest group
- Other general-purpose guides are available online

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
  - Non-trunked frames
- Native VLAN defaults to VLAN 1
  - But some Cisco management protocols use VLAN 1
- Change the native VLAN number (e.g., VLAN 999)
  - Management protocols will continue to use VLAN 1 (even if it's not formally configured on the trunk)
  - Non-trunked traffic will use the native VLAN number (VLAN 999)

Privileged accounts
- Elevated access to one or more systems
  - Administrator, Root
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes
- User accounts should have limited control
  - Role separation with different access rights
  - More difficult for a single limited account to breach security

FIM (File Integrity Monitoring)
- Some files change all the time
  - Some files should NEVER change
- Monitor important operating system & application files
  - Identify when changes occur
- Windows - SFC (System File Checker)
- Linux - Tripwire
- Many host-based IPS options

4.6 - Mitigation Techniques (continued)

Restricting access via ACLs
- Use device ACLs to limit access to important infrastructure devices
  - Only admins should be able to login
- Drop all other traffic
  - Define the subnets for the technology teams
- This is a bit different than setting an application ACL
  - You're dropping traffic for non-authorized users
  - Used mostly for access to management interfaces

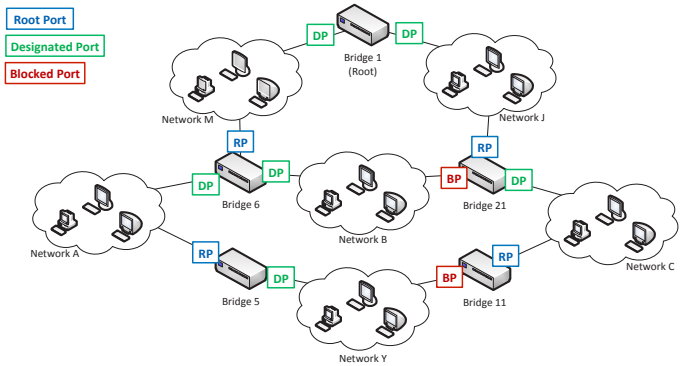
Honeypots
- Attract the bad guys - and trap them there
- The bad guys are probably a machine
  - Makes for interesting recon
- Honeypots / Honeynet - a network of honeypots
- Many different options
  - http://www.projecthoneypot.org/, honeyd
- Constant battle to discern the real from the fake

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

4.6 - Switch Port Protection

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)
  - Created by Radia Perlman
  - Used practically everywhere

BPDU guard
- Spanning tree takes time to determine if a switch port should forward frames
  - Bypass the listening and learning states
  - Cisco calls this PortFast
- BPDU (Bridge Protocol Data Unit)
  - The spanning tree control protocol
- If a BPDU frame is seen on a PortFast configured interface (i.e., a workstation), shut down the interface
  - This shouldn't happen - Workstations don't send BPDUs



Root guard
- Spanning tree determines the root bridge
  - You can set the root bridge priority to 0, but that doesn't always guarantee the root
- Root guard allows you to pick the root
  - Cisco feature
  - Prevents a rogue root bridge
- If your root bridge receives a superior STP BPDU on a root guard port, root guard changes the interface status to "root-inconsistent" (listening)
  - This effectively disables the interface to the rogue root

Flood guard
- 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
  - Interface is usually disabled by default

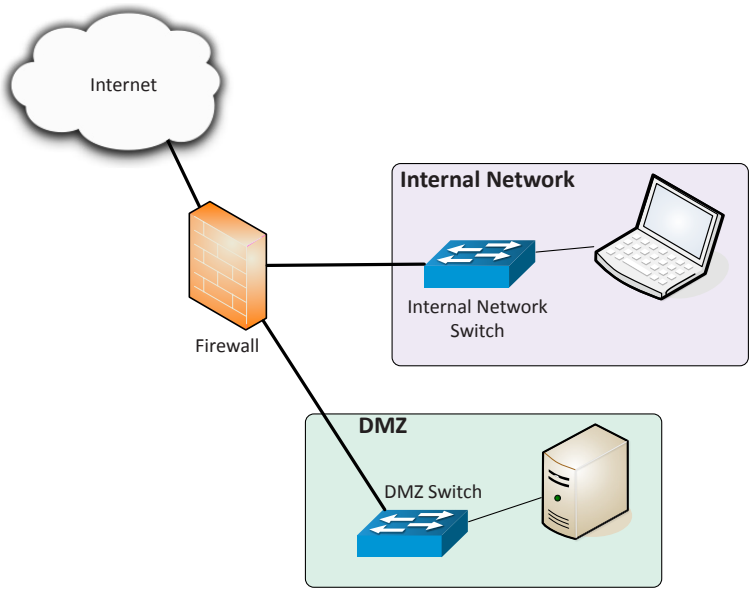
DHCP snooping
- IP tracking on a layer 2 device (switch)
  - The switch is a DHCP firewall
  - Trusted: Routers, switches, DHCP servers
  - Untrusted: Other computers, unofficial DHCP servers
- Switch watches for DHCP conversations
  - Adds a list of untrusted devices to a table
- Filters invalid IP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

4.6 - Network Segmentation

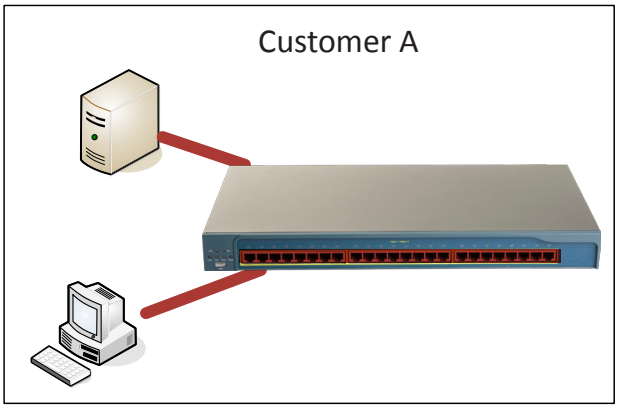
Segmenting the network
- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation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

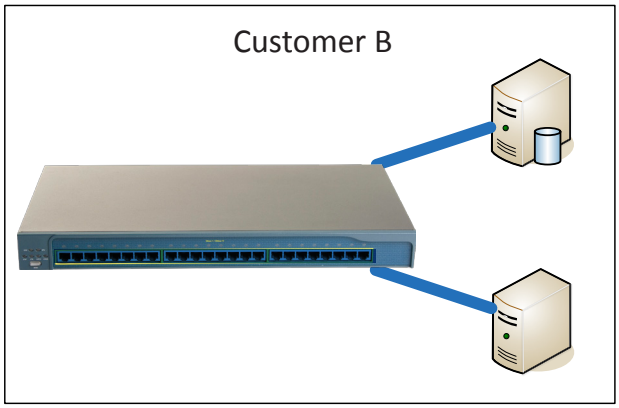
Physical segmentation
- Devices are physically separate
  - Switch A and Switch B
- Must be connected to provide communication
  - Direct connect, or another switch or router
- Web servers in one rack
  - Database servers on another
- Customer A on one switch, customer B on another
  - No opportunity for mixing data
- Separate devices
  - Multiple units, separate infrastructure

DMZ
- Demilitarized zone
  - An additional layer of security between the Internet and you
  - Public access to public resources

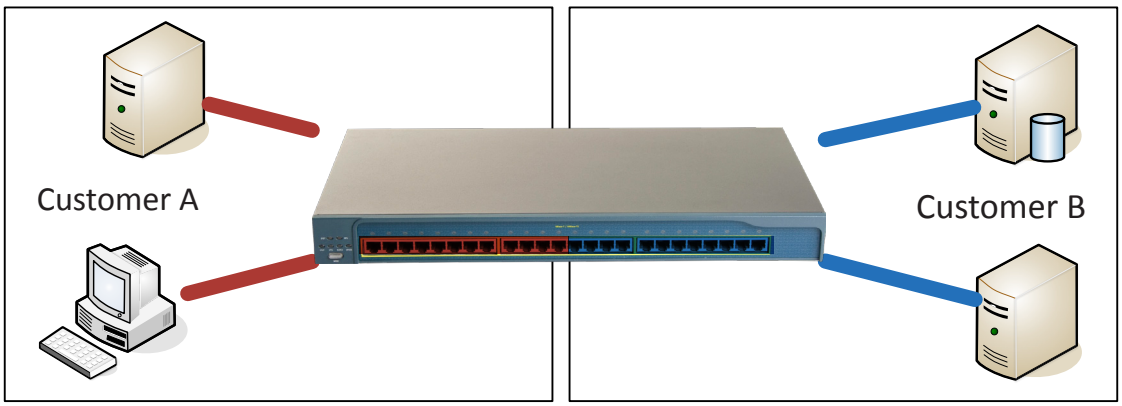


Physical segmentation
- Separate Device
  - Multiple units, separate infrastructure

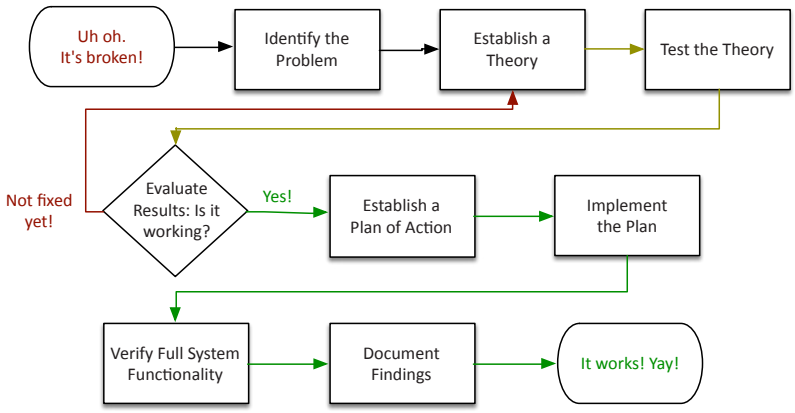




Logical segmentation with VLANs
- Virtual Local Area Networks (VLANs)
  - Separated logically instead of physically - Cannot communicate between VLANs without a Layer 3 device / router



5.1 - Network Troubleshooting Methodology

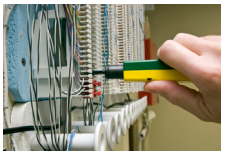


- Identify the problem
  - Information gathering, identify symptoms, question users
- Establish a theory of probable cause
- Test the theory to determine cause
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify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

5.2 - Hardware Tools

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

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

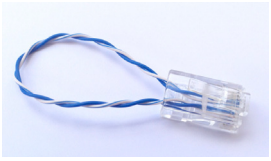


Punch-down Tool
- Forces wire into a wiring block
- Trims the wires and breaks the insulation

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

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

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

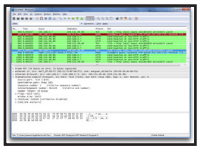


Loopback plug
- Useful for testing physical ports
- Serial, Ethernet, T1, fiber
- These are not crossover cables

Multimeter
- AC/DC voltages
- Continuity, wire mapping

Spectrum analyzer
- View the frequency spectrum
- Identify frequency conflicts

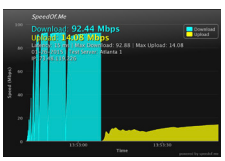
5.2 - Software Tools



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

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

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



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

5.2 - Command Line Tools

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

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>`

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

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

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

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

pathping - Combination of ping and traceroute
- `pathping <ip address>`

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

route - View the device's routing table
- `route print` - View the Windows routing table

arp - Address resolution protocol information
- `arp -a` - View the local ARP table

5.3 - Wired Network Troubleshooting

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

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

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

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

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

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

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

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

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

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

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

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

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

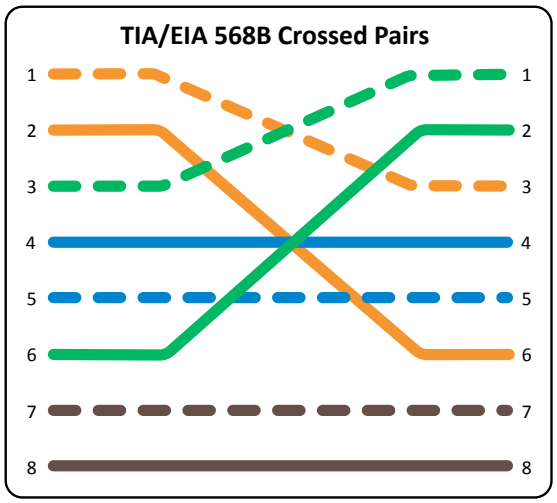
Incorrect cable type
- Excessive physical errors, CRC errors
  - Check your layer 1 first
- Check the outside of the cable
  - Usually printed on the outside
  - May also have length marks printed
- Confirm the cable specifications with a TDR
  - Advanced cable tester can identify damaged cables

Incorrect cable type

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

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

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



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

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

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

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

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

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

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

5.4 - Wireless Network Troubleshooting

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

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

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

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

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

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

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

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

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

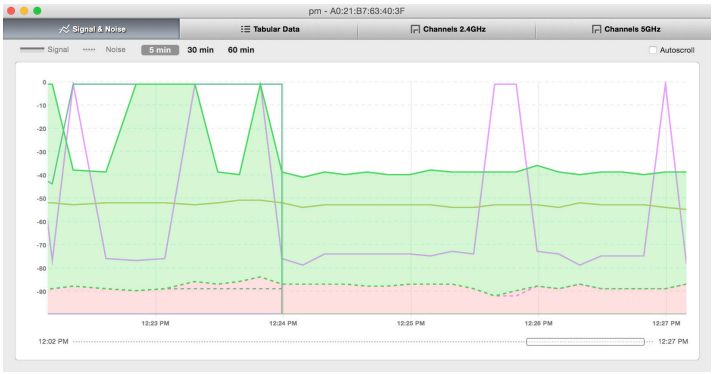
Frequency mismatch
- Devices have to match the access point
  - 2.4 GHz, 5 GHz
- Verify the client is communicating over the correct channel
  - This is normally done automatically
  - May not operate correctly if manually configured
- Older standards may slow down the newer network
  - 802.11b compatibility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

5.4 - Wireless Network Troubleshooting (continued)

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

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

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



5.5 - Network Service Troubleshooting

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

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

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

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

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?

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

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

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

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

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

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

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

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

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

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

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


Professor
Messer