Chapter 1 – Network Models

- Two Methods of Understanding Networks
  - OSI – Open System Interconnection
    - Seven Layer Model
  - Transmission Control Protocol/Internet Protocol
    - TCP/IP
  - Understand at what layer a problem may occur and provides a common language
- The OSI Seven Layer Model in Action
    - each level has distinct protocols and encourages modular network design
  - L7 – Application
  - L6 – Presentation
  - L5 – Session
  - L4 – Transport
  - L3 – Network
  - L2 – Data Link
  - L1 – Physical
- Network Hardware and Layers 1 + 2
    - physical channel through which data moves (unshielded twisted pair – UTP) connected to a central box
  - L1 – defines method of moving data between computers, the physical channels, equipment, infrastructure
    - Network Interface Card (NIC) – provide interface between cables/boxes and pc
  - L2 – The NIC – provides each system with a unique identifier – burned-in firmware with 48-bit MAC address
      - designated via IEEE
    - first six digits represent NIC manufacturer (OUI), last six are manufacturers
      - unique serial # for NIC
        - device ID
      - check with ipconfig /all
    - IEEE forms MACs from MAC-48/EUI-48
  - How is a MAC used in NICs?
    - send/receive binary data via electrical impulses
      - broken into frames – Frames are sent only to the interface associated with the destination MAC address
    - Receiver MAC + Sender MAC + Type + Data + FCS Framecheck Sequence
      - uses cyclic redundancy check to verify data is intact
    - Different networks use different frames and frame sizes ~ 1500 bytes
      - this then goes to Central Box
        - initially a hub – repeater – dumb – broadcasts to all ports
      - Even through every frame went to every NIC – only the NIC with the correct MAC address would decipher and process
    - This was replaced with a Switch – filters traffic actively via MAC address
  - FCS – 4-bytes – binary arithmetic – product divided by a key factor and remainder is the FCS
  - Frames are all used to control traffic – limiting how much space a single NIC uses – allowing for other NICs on the network to talk
  - An NIC will first send a broadcast (FF-FF-FF-FF) on L2 broadcast address – requests MAC addresses or IPs in search of correct recipient
    - Data → NIC → Frame → add FCS → Send Along Network → Central Box → Unicast and broadcast frames → Recipient NIC → Processed
  - Any device dealing with MAC addresses is port of OSI L2 – Data Link Layer
    - Jobs of an NIC

- Logical Link Control – talks to OS via device drivers
- Media Access Control – creates and addresses frames – sent along network

- Network Software – Layers 3 – 7
  - Large networks require logical addressing, breaking the internet up into subnets
    - Switching from MACs to logical addressing requires a network protocol which exists in every OS
      - rules for communication
      - creates unique system IDs
        - TCP/IP
          - protocol suite
  - Internet Protocol – IP – OSI L3 – Network Layer
    - packets are created
    - IP is primary logical addressing tool via IP addresses using dotted decimal notation
    - a router connects each subnet using IP address which is stored in system software unlike burned-in MACs
    - In a TCP/IP network is a packet within the frame
      - Destination IP Address + Source IP Address + DATA
        - then sent by NIC
      - Frame Header + Packet Header + DATA + FCS
    - Each router the frame travels along removes frame header, checks packet for IP matching, and re-frames if no match to move on to next router
      - once at correct router, frame is re-fitted with appropriate MAC frame and sent to device
  - Segmentation and Reassembly * OSI L4 – Transport Layer
    - Segmentation – data is cut, framed, and organized so receiver can process data
    - Transport Protocol breaks data up into segments/datagrams with sequence numbers
  - Talking on a Network – Layer 5 – The Session Layer
    - Session Software – connects application to applications and networks
  - Translation – OSI L6 – Presentation Layer
    - translates data from lower layers into format usable by application layer
  - Network Applications – OSI L7 – Application Layer
    - Software apps using the network
    - the code built in to all OS that enables network-aware applications
      - all Oss have Application Programming Interfaces used to make programs network aware
  - Encapsulation and De-Encapsulation
    - preparing data to go onto a network and reverse occurs at receiver
- The TCP/IP Model
  - Four Layers – Application, Transports, Internet, Link/Network Interace
  - The Link Layer – OSI L1+2
    - Physical and Data Link
    - cabling, physical addresses, NICs, Switches
    - Complete frames
  - The Internet Layer
    - pure IP packets and related protocols
    - routers, IP addressing
  - The Transport Layer
    - OSI Transport and Session Layers
    - segmentation, reassembly
    - connection and connectionless communication
      - Connection – IMAP, verify good connection – TCP

        - Connectionless – VoIP – does not first verify good connection – UDP
    - IP Packet + IP Address = TCP segment
        - Destination Port + Source Port + Sequence Number + Checksum + Flags + Acknowledgement + DATA
        - port – logical values assigned numbers between 1-65,536
        - applications first look for destination then source port
    - UDP Datagram
        - Destination Port + Source Port + Length + Checksum + DATA
            - less complex due to indifference about connection
            - session are easy to see under this model via netstat -n
- The Application Layer
    - L5,6,7 – Application, Presentation, Session
        - standard formats are an inherent part of TCP/IP
- Frames, Packets, Segments/Datagrams
    - application creates data
    - Transport – data broken down in TCP or UDP segments
    - Internet – adds ID addressing, creates IP packets
    - Link – wraps IP packet into a frame with MAC + FCS
- Both models are essential for primary diagnosis

Chapter 2 – Cabling and Topology

- Network Topologies
    - ways of connecting computers together
- Bus and Ring
    - Bus – connected all computers inline with one cable
        - required terminators to prevent reflection
    - Ring – network connected all computers with a ring of cable
    - entire network stop if cable was damaged
- Star
    - central connection box offered fault tolerance but faced difficult transition
- Hybrid
    - ring was shrunk into a small box with all computers to box
    - physical and logical topologies combined
- Mesh
    - wireless devices with devices connection to two or more other devices
    - partially meshed – at least two machines have redundancies
    - fully meshed – all devices interconnected
- Cabling and Connectors
- Copper Cabling and Connectors
        - twisted and coaxial
    - coaxial - central wire, insulated, and wrapped in braided metal shield
        - shielded against EMI
        - originally used BNC bayonet style connectors
        - F-connectors screw on and are used for modern connections
            - RG-59
            - RG-6
    - Twisted Pair
        - common in networks, more twists = less crosstalk
            - twisted in either shielded or unshielded (STP vs UTP)
                - STP – six different types
                - UTP – no shield, plastic wrapped, vulnerable to EMI

- CAT ratings dependent on MHz frequency maximums
- Modern networks can be more efficient, pumping more data through less
- originally used RJ-11 for two pairs, now uses 8-position/8-contact (8P8C)
    - not RJ-45s
- Fiber Optic Cabling and Connectors
    - transmits light rather than electricity – good for long distance and EMI areas
        - glass core, cladding, buffer material, and insulating jacket
        - measured via core and cladding ratings
    - structured in pairs of senders and receivers (duplex)
    - use LEDs – multimode fiber (MMF)
    - use Lasers – singlemode fiber (SMF) – avoids modal distortion
        - wavelength light is also measured in nanometers (nm)
            - four main connectors
                - ST SC – unique ends
                - LC, MT-RJ – duplex
- Other Cables
    - Classical Serial
        - since 1969 – 9-pin, male-D (DB-9)
            - point-to-point, low bandwidth
    - Parallel – point-to-point, low bw, 25-pin, female-D (DB-25)

- Fire Ratings
    - PVC has no fire protection
    - Plenum-rated – much less smoke, fumes, 3-5x more expensive
        - Plenum is the space between the tile and concrete ceilings
    - Riser – vertical cables between floors have a separate fire rating
- Network Industry Standards – IEEE
    - 802 working group – networking standards
        - subcommitties

Chapter 3 – Ethernet Basics

- Ethernet
    - bus topology – 1973 – Xerox
    - IEEE 802.3 Ethernet Committee
        - open standard
- 802.3 Standards
    - wired standards that shared some basic frame type and network access method
        - 802.3i – 10Mbps – Twisted Pair
        - 802.3ab – 1 Gbps – twisted Pair
        - 802.3by – 25 Gbps – Ethernet over Fiber
    - frames remain the same despite different components
        - Ethernet II – Modern
    - Data frames with MAC address to ID networked computers and use CSMA/CD to determine which machined gained access
- Ethernet Frames
    - data broken down into frames
        - prevent machine network monopoly of bus cable
        - retransmitting lost data becomes more efficient
    - Using small frames enables computers to share a cable easily as each computer listens to the segment

        - detect if other computers are transmitting
        - if corrupted data requires transmission, small chunks limit file resend size
    - Basic Ethernet Frames contain Five Fields
        - Destination MAC Address
        - Data Type
        - Data
        - Source MAC
        - Frame Check Sequence
            - transmission begins with preamble (which can include pad filler)
    - Preamble
        - 7-byte series of alternating binary with a 1-byte frame delimiter
            - always precedes frame
        - gives receiving NIC time to prep for incoming frame
    - MAC Address
        - ID NICs on a network
        - destination address enables NICs to examine each frame and only process frames intended for them
        - source address enables accurate recipient response
    - Type
        - helps receiving computer interpret frame contents (if frame has IPv4 vs IPv6 data)
        - does not tell if frame has higher-level data (emails, webpage)
    - DATA
        - contains payload
    - Pad
        - Filler to bring packet up to 64bit minimum
    - Frame Check Sequence
        - recognize corruption of data via special code called cyclic redundancy check (CRC) and attaches frame check sequences (result) to frame
            - confirmed by answer comparison
    - Early Ethernet Standards
        - Bus Ethernet
            - every computer originally connected to some hybrid star topology used since 1990s
                - center hub – electronic repeater
        - 10BaseT
            - two or more computers connected to hub via IEEE committee (10Mbps) baseband (cable carries on signal type)
            - T = twisted pair
        - UTP
            - requires CAT3 or higher UTP pair, one pair sends the other receives
            - 8P8C – RJ45 connector (pins 1-8) 1+2 send, 3+6 receive
                - hub connector cannot simultaneously send and receive
            - NIC communicates in one direction (half-duplex) originally
                - now full-duplex
            - RJ45 connection – crimp (installed via crimping) with a crimper with color coded wires (solid/stripe pair)
            - Industry Standard – TIA/EIA 568 A+B
        - 10BaseT Limits and Specifications
            - cable distribution and number of computers (1024)
            - distribute between hub and computer (100 meters)
        - 10BaseFL

- Fiber Optic Version
    - max cable length – 2KM
    - immune to EMI
    - harder to tap into
  - multimode via SC or ST connector
  - One Sender, one receiver
    - 10 Mbps; Baseband;2000m between hub and node;1024 nodes;starbus; physical star, logical bus; multimode + ST/SC
- Interconnecting versions of Ethernet via media connector

- CSMA/CD
  - Carrier Sense Multiple Access/Collision Detector
    - determine which computer should use a shared cable at a given moment
      - Carrier Sense – node examines cable pre-frame send and waits several milliseconds between tests
      - Multiple Access – equal wire access, first come
    - if collision occurs, data is lost
      - sensed by NICs which generates RNG number that determines how long to wait
        - one is always sooner than the other
        - collision domains are rare in modern equipment
- Enhancing and Extending Ethernet Networks
    - Trouble with Hubs
      - one message on wire at a time, busy network = slow networks due to collisions
  - Switches
    - takes advantage of MAC addresses to create P2P connections
      - gives every conversation full bandwidth
    - table of MAC addresses – Source Address Table (SAT)
      - allows accurate forwarding, handle bandwidth resources better
    - Ports are collision domains, switch buffers incoming frames to avoid collisions
    - Unicast Messages – go to target
    - Broadcasting – all ports
- Connecting Ethernet Segments
    - additional switches – limits single point of failure exposure and increase node availability
  - Uplink Ports
    - connect two switches via using a straight-through cable
    - modern switches do not need dedicated uplink ports due to auto-sense
  - Crossover Cables
    - special twisted-pair cables
      - reverse send/receive pairs on one end
        - one wired via TIA/EIA 568A, the other 568B
    - allows switches to hear one another via regular port
  - Spanning Tree Protocol
    - creation of redundant network connections called bridging/switches loops
    - spanning tree protocol avoids crashes due to packets
      - switches detect loops before they occur via special frames (Bridge Protect Data Units)
    - Topology established via BPDUs with one switch elected root bridge (acts as center of STP)
    - Root Bridge

        - reference point to maintain loop free topology
            - If links go down, STP uses Topology Change Notification (TCN) BPDU to enable switch network around failed device
            - STPs cannot be switches directory connected to PCs via PortFast setting (creates unnecessary TCN issuance)
        - If ports configured with PortFast receive BPDUs, can cause loop
            - Root Guard helps to move ports to root-inconsistent (forwarding state) to help define locations where root bridge should NOT be located
        - STP has been replaced by Rapid Spanning Tree Protocol (RSTP)
            - faster convergence time following network change
- Troubleshooting Switches
    - physical damage or dead parts → replace switch or cable with known good device

---

Chapter 4 – Modern Ethernet

- 100-Megabit Ethernet
    - Frame Size and Elements, CSMA – stay same between 100Mgbt to 1000Mgbt
    - standardization = communication and scalability
- 100baseT
    - 100Mbps;Baseband;100m hub/node dist; 1024 nodes; star bus, physical star and logical bus; Cat5 or better UTP/STP cabling with RJ45/8P8C
    - cabling had to be replaced and NICs changed when going from 10BaseT to 100BaseT as well as halo/switch
        - costly
    - circumnavigate cost with multispeed, autosensing NICs, hubs/switches which worked with lowest BaseT
    - Checks OS or physical card for indicators
    - All modern NICs are multispeed, autosensing (“10/100/1000”)
- 100BaseFX
    - good for long distance, shielded against EMI, hard to tap into
    - 100Mbps;Baseband;2Km hub/node distance; 1024; star bus topology; multimode fiber-optic with ST or SC connectors
- Full-Duplex Ethernet
    - most 100BaseT NICs can do full duplex by late 90s, doubling bandwidth but not speed
    - autoconfigures between NIC and Switch
        - can be manually forced
    - fast Ethernet – good for LANs, simple device networks, but no longer the newest standard
- Gigabit Ethernet
    - common modern NICs
        - IEEE 802.3ab (1000BaseT) – four UTP/STP pairs, 100m
        - IEEE 802.3z (1000BaseX) – SX+LX
    - 1000BaseSX
        - multimode FOC, 220-500m; LC connectors
    - 1000BaseLX
        - lasers for long distance; 5km; (70km with repeaters)
    - SFF Fiber Connectors
        - ST connectors require twisting and are small
        - SC connectors snap-in but are large
        - SFF = Small Form Factor – Mechanical Transfer Registered Jack (MT-RJ) common
            - LC Type – common in US

- Mechanical Connection Variation
    - standard connection type is called physical contact (PC) connector
        - two fiber pieces touch
        - replace flat surface connectors
    - PC has ultra-physical contact (UPC) – significant reduction in signal loss
    - Angled Physical Contact (APC) add 8 degree curve angle, further lowering signal loss
- Implementing Multiple Types of Gigabit Ethernet
    - frames don't vary among ethernet flavors
    - dedicated media convertors
        - SMF – UTP/STP
        - MMF – UTP/STP
        - Fiber/Coax
        - SMF/MMf
    - modular parts – Gigabit Interface Converter (GBic) can accept any ethernet jack
    - switches and other equipment use smaller small-form factor pluggables (SFPs)
- Ethernet Evolutions
    - 10 Gigabit Ethernet
        - 10 Gbps, FOC + Copper
        - Fiber-based 10 Gbe
            - data integrity and transfer speed
            - standards created to use either/or synchronous optical network (SONET) as well as LAN physical layer mechanisms
                - many different 10 Gbe standards
                - defined by fiber-type, wavelength, and physical layer signaling type, maximum signal dist
            - "10 GBase" + Fiber Type signififer + Physical Layer Signal Standard Signifier
                - R = LAN; W=SONET/WAN
                - S = short wavelength; 85nm – max fiber length = 300m
                - L = long wavelength; 1310nm – max fiber length = 10km
                - E = extra long wavelength; 1550nm – max fiber length = 40km
    - Other 10 Gbe Fiber Standards
        - 10GBaseL4 = 4 lasers;1300nm;legacy fiber; 300m multimode; 10km single
        - 10GBaseLRM = 10GBaseLR over legacy multimode fiber – 220m
        - 10GBaseZR = 1550nm;single mode;80km – LAN/WAN-SONET
    - Copper-Based 10GbE – Twisted pair – Cat6 = 55m;Cat6a = 100m
    - 10GbE Physical Connections
        - multisource agreements to make interoperable devices and standards
        - MSA-transceivers make media conversion by connecting with proper transceiver
            - XENPAK
            - SFF+
    - Characteristics of Fiber Transceivers
        - standard duplex pair format
        - Wave Division Mulitplexing (WDM) differentiates wave signals on a single fiber – Single Strand Fiber Transmission
        - Bidirectional (BiDi) Transceivers have single optical port designed to send on one wavelength and receive on another
            - require corresponding receiver on other end to work
        - cost effective, similar performance
        - less wiring or double current wiring
        - Gigabit = SFP;10GBase=SPF+;40GBase=QSFP
- Backbones

    - speed vs cost
    - multispeed ethernet
        - high speed switches with no computer connection besides server
            - sub-sets of switches that service specific areas
- IEEE 802.3ba
    - 40 + 100 Gbit Ethernet
        - 40 GbE/100GbE

Chapter 5 – Installing a Physical Network

- Understanding Structured Cabling * TIA/EIA Standards * 586+
    - Cable Basics + Physical Star Network + BICSI
        - safety, changeability, organization
    - Structured Cable – Network Components
        - telecom room + horizontal cabling + work area
    - Horizontal Cabling
        - typically SE or better UTP
        - Solid Core vs Stranded Core
            - solid – better conductor but stiffer and brittle
            - standard – weaker conductor but more robust
        - Horizontal Cable – Solid Core
            - highest CAT rating possible – four pair assumed (typically CAT5e or CAT6; CAT6a for 10GBaseT)
    - The Telecommunications Room
        - Intermediate Distribution Frame (IDF)
            - must impose organization to prevent mess over time
        - Equipment Racks
            - 19in wide with varying heights; free standing or bolted
            - network hardware components are mountable, rack mounted switches, servers, UPSs
                - height measured = unit = U = 1.75in
                - (most devices 1U, 2U, or 4U)
            - two post, four post, or rail rack
                - depends what devices are to be used
            - REMEMBER PROPER AIR FLOW
            - REMEMBER TO SECURE AND LOCK
        - Patch Panels and Cables
            - box with female ports in front and permanent connectors in the back which connect to the horizontal cables to prevent moving
                - most common type – 110 block
                - uses a punch down tool
            - punchdown block has groups for individual wires (be sure to align properly at both ends to avoid TX/RX reversed)
            - 66 blocks are still commonly found for telecoms
            - varying configurations for UTP, STP, fiber ports and different numbers
                - patch panels come with CAT ratings
                    - higher the better
                - once patch panel is installed, connect ports to switch with patch cables
                    - stranded core, can be color coded

        - reinforced (booted) connectors
    - The Work Area
        - wall outlet termination point for horizontal network cables
        - convenient PC/Telephone connection point
        - PC connects to wall with patch cable
        - female jacks are CAT-rated
            - label and document
        - first place to check for network troubleshooting
- Structured Cable – Beyond the Star
        - typical building wide network consists of high-speed backbone running vertically through building and connects to multispeed switches on each floor
            - mirrored by telephone connections
            - typically one or more 25-pair UTP running to 66 block per floor
- Demarc – Demarcation Point
    - physical location of connection from outside world and marks division of network responsibility
        - internal vs upstream
    - DSL/modem supplied by ISP = Network Interface Unit = Demarc for Private Networks
        - smart jacks allow ISP to determine if customer is cut off from NIU
            - allows for loopback address, remote for testing
- Connections Inside the Demarc
    - After Demarc – Network/Tele connections go to customer box for primary distribution
        - customer premises equipment (CPE)
            - NIU → CPE = Demarc Extension
        - Telecomms also use VCCs (Vertical cross connect)
    - Demarcs, Tele-crossconnects, LAN cross-connects all go to main distribution frame (MDF) which connections to floor-specifics IDFs
    - Multiple NIUs can exist within one building, some with Demarcs, IDFs, and MDFs
- Installing Structured Cabling
        - assessment and planning
            - floor plans, access, standards, routing
    - Gathering a Floor Plan
        - key to proper planning – first major step, DIY
    - Mapping the Runs
        - survey work areas both existing and planned
            - determine cable drops
        - inside or outside wall runs – external raceways
    - Determining the Location of the Telecommunications Room
        - Distance 90m max
        - Power and Dedicated Circuit
        - Humidity and Air Conditioning
        - Cooling and Low Temperature Maintenance
        - Access and Prevention of Unauthorized Access
        - Expandability and Scalability
    - Pulling Cable
        - start in telecommunications room and work out to drops via hooks/cable trays
            - telescoping poles, special nylon pull ropes
        - local codes, TIA/EIA, National Electrical Code
        - vertical drops post cut-in for mount brackets, faceplates, etc
        - organize and consolidate cables for connections
    - Making Connections
        - proper jacks and cable run tests, document/label

- Connecting the Work Areas
- Rolling Patch Cables
    - stranded core UTP cables that match CAT level of horizontal cabling
        - crimps are solid/stranded specific
        - RJ45 crimper with stripper and snips
        - first cut cable square
        - strip off ½ inch of plastic jacket
        - insert individual wires into correct location via TIA/EIA 568A or B
            - limit unraveling
        - insert crimp into crimper and press
    - Good patch cables should have boots, slid on before crimping both ends
    - Test
- Connecting Patch Panels
    - cable management via proper management hardware
    - organize patch to mirror network layout either physically or logically
    - document everything
- Testing the Cable Runs
    - Copper Challenges
        - length – too long degrades signal
        - broken/open, bent pins
        - shorts
        - breaks and locating breaks
        - correct vs incorrect termination
        - EMI/RSI – UTP is susceptible
        - signal from one pair interfering with another pair
    - Verify terminated ends and cables are correct with cable tester
        - continuity testers
        - wiremap test
        - time domain reflectometer (TDR)
            - near end crosstalk detection (NEXT)
            - far end crosstalk detection (FEXT)
                - weaker signal due to attenuation
- Measuring Signal Loss
    - dB – decibal
        - process of verification perform with cable certifiers
- Fiber Challenges
    - dB, various standards and causes
    - Signal Loss/Degradation
        - Damaged Open Connections
            - check small form factor pluggables (SFPs) or gigabit interface converters (GBic)
        - dirty connectors, mismatch
        - attenuation and dispersion, bend radius
    - Physical or Signal Mismatch
        - few connectors
        - even if physical connection possible, signal may not be compatible (transceiver mismatch)
        - cable/fiber mismatch – incorrect cable type
            - different wavelengths
        - Fiber Tools

        - ST, SC, LC connections
        - Optical Time Domain Reflectometer (OTDR)
            - determine continuity errors
        - Complex TIA/EIA requirements – Fiber Certifiers
    - Biggest Issues
        - attenuation
        - light leakage
        - modal distortion
- NICs
    - final part – recognize various NICs by sight
    - all UTP Ethernet NICs uses RJ45 – cable runs from NIC to switch
    - Fiber-optic NICs come in a wide variety with connectors being used for multiple standards
        - check documentation
- Buying NICs
    - brand names, multispeed, maintain model uniformity
- Physical Connections
    - PCI – Peripheral Component Interconnect
    - PCIe
- Drivers
    - Windows – Device Manager
    - Linux – Network Applet
    - MacOS – Network Utility
- Bonding
    - multiple NICs for a single machine
        - bonding/link aggregation
        - increases speed between machine and switch
    - use Identical NICs and Switches
        - Link Aggregation Control Protocol (LACP)
- Link Lights
    - state of the link
        - confirms connection to switch, which also has lights for connectivity
            - steady on = good
    - Activity Light – Active Traffic, good for verifying connection
    - Collision Lights = older
    - Fiber Optics NICs typically do not have lights but issues are often related to NIC connection
        - connectors are first place to check
- Diagnostics and Repair of Physical Cabling
    - Diagnosing Physical Problems
        - eliminate potential software errors
        - check if other networked devices are discoverable
        - process of elimination
    - Check Lights
        - Both NIC and Switch
        - Notification Area Symbols
        - Check shared resource access from multiple locations (server)
        - continuity tests, swapping patch cables and connections
    - Check the NIC
        - OS utility, NIC-based diagnostic via Loopback Plug
        - female connection point common source of failure
    - Cable Testing
        - majority of issues occur at work area

        - horizontal cable test with midrange tester with TDR
            - test with workspace loopback plug and microscanner in telecom room
            - test patch cable or horizontal issue
            - check couplers
- Problems in the Telecommunications Room
    - patch panel runs
    - power and environment
        - UPS
            - power monitoring
        - generator
    - check frequency of UPS usage = voltage event recorder
    - temperature monitors with rack monitoring system
        - environmental monitors = humidity
- Toners
    - generator and probe and butt set (optional)
        - assist with cable trace

Chapter 6 – TCP/IP Basics

- The TCP/IP Protocol Suite
        - Link Layer relies on technologies outside the TCP/IP protocol suite to get IP pakcets from one system to another
    - Top Three Layers
        - Internet, Transport, Application
    - Certain parts of IP Packets fit perfectly within TCP/IP model layers
        - the header for a higher layer is data for a lower layer
- Internet Layer Protocols
    - Internet Protocol (IP) works at Internet Layer
        - takes data chunks from Transport Layer, adds addressing, and creates final IP Packet
        - IP then gives packet to Layer 2 for Frame Encapsulation
            - certain applications use ICMP to confirm IP address pairing
        - ICMP is typically used automatically by applications as needed without user action
            - ping utility
    - Internet Layer Common Three Protocol
        - Version + 32bits + DSCP + TTL + TCP = IP header
        - full IP packet headers have 14 different fields
            - Dest/Src IP addresses
            - DSCP for VoIP
            - Version
            - TTL
            - Header Length
            - Protocol
- Transport Layer Protocols
        - Determine connection/connectionless communication
            - TCP – connection-oriented ensures data arrives in good shape
            - UDP – connectionless is used when data integrity is not a major concern
- TCP – Transmission Control Protocol
    - most commonly used, transfer is reliable and complete

        - requires communication rules → acknowledge sender/receiver and readiness to send/receive
        - Three-Way Handshake – SYN → SYN-ACK → ACK
    - TCP segments data, giving each piece sequence number and verifies all segments are received
        - SRC PORT + DEST PORT + SEQUENCE # + ACK = TCP Header
    - Port numbered from 1-65,535 determines what application needs requested data
        - applications are assigned specific numbers
            - web servers – 80 HTTP, 443 HTTPS
            - email – 143 IMAP4
    - Headers also contain
        - Seq + Ack #s
        - Flags
        - Checksums
- UDP – User Datagram Protocol
        - doesn't possess extras seen in TCP
        - best for mass data transfer where perfection isn't needed, or systems are so close data loss changes are low
    - Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) use UDP
        - SRC PORT + DEST PORT + LENGTH + Checksum = UDP Header
        - UDPs do not get segmented
- Application Layer Protocol
    - IP and Ethernet
        - TCP/IP – simplified and complex network support (LANs and WANs)
    - LANs
        - every host runs TCP/IP software over Ethernet hardware
            - creates two addresses (IP and MAC) per host
        - to send IP packet, sender inserts IP packet into an Ethernet frame
    - IP Packet
        - Dest MAC + Src MAC + Type + Dest IP + Src IP + Data + FCS = Ethernet Frame
    - For sender to get receiver MAC, it sends ARP (FF:FF:FF:FF:FF:FF) broadcast
        - receiver sends ARP reply by providing MAC attached to specified IP
            - allows sender to transmit unicast Ethernet frames to receiver
            - test with arp -a
        - IP addresses allow unique ID of machines on a given network and allow distinguishment between LANs
            - also allows computers to communicate between LANs in a WAN
- IP Address
    - IPv4 – common – 32bit value, broken into four groups of eight
        - each 8 piece section translates in dotted decimal notation
            - 00000000 = 0; 11111111 = 255
        - no two computers on the same network can have the same IP
        - every OS comes with utility that displays IP/MAC in CLI (ipconfig, ifconfig, ip a)
- IP Address in Action
    - create network IDs so each LAN has unique ID
    - Interconnect LANs via routers, routers use Network ID
    - Subnet Mask gives computers on the network a way to recognize if a packet is for the LAN or a computer on the WAN
- Network IDs
    - each LAN within a WAN needs on
        - each computer within a LAN share similar but not exact IPs
    - The network ID is the section of the IP address that is shared by all devices in a LAN

        - non-shared port is host ID
- Interconnecting LANs
    - TCP/IP LANs must have a router connection to connect to other TCP/IP LANs
        - as a result, every router needs an IP address for every LAN it connects to, to route packets to correct LAN
    - Router Interface that connects a LAN to the router is the default gateway
        - the interface must have an address in the LANs network ID
            - typically the lowest = 1
        - Network IDs are used to determine network traffic
        - Built within the router is a routing table, the instruction that tell the router what to do with incoming packets and where to send them
    - Network IDs are flexible, can be changed as long as no other Network IDs match within connected networks (WAN)
        - allocation is governed to prevent this
        - by having more zeroes in an address for Network ID, more total addresses can be used
    - Network IDs enable multiple LANs into a WAN, with everything connected together via routers and their tables
- Subnet Mask
    - tool that tells a sending computer whether the destination IP is local or long distance
    - comprised of a string of ones followed by a number of zeroes, all equaling a total of 32 bits
        - IP section that aligns with subnet mask = network ID
            - zeroes section = host ID
    - A sender will compare destination IP with own IP via subnet mask
        - if there is a match for the first three sections = local
            - no match = long distance
        - if local → sender issues ARP to determine receiver MAC
        - if not → sender sends message to default gateway via ARP for Default Gateway MAC
            - message then sent to default gateway
- Class IDs
    - Internet Assigned Numbers Authority (IANA) formed to track and disperse IP addresses
        - Five Regional Internet Registries (RIRs)
            - parse out IPs to ISPs and Corporations
            - these blocks are called network blocks
    - Classes
        - A – 1-126 – 1.0.0.0 – 126.255.255.255
        - B – 128-191 – 128.0.0.0 – 191.255.255.255
        - C – 192-223 – 192.0.0.0 – 223.255.255.255
        - D – 224-239 – 224.0.0.0 – 239.255.255.255
        - E – 240-254 – 240.0.0.0 – 254.255.255.255
    - Multicast – routers talking to one another
    - IANA structure ran out of room, efficiency, and scalability quickly
- CIDR – Classless Inter-Domain Routing and Subnetting
    - taking a single-class of IP addresses and further dividing into smaller groups
    - subnetting – done by organizations
    - CIDR – done by an ISP
- Subnetting
    - more efficient than class blocks
        - allows creation network for security (air gap between public and private computers)
        - Bandwidth control (separation of LANs by traffic usage)
    - cornerstone is subnet mask
        - never try to subnet without first converting to binary

- Making a Subnet
  - begins with single network ID
  - separate into however many subnets are needed
- Calculating Subnets
  - start with beginning subnet mask, extend subnet extension until you have number of subnets needed
    - 2^y
      - y = number of bits added to subnet
    - the size of the subnets can be varied through Variable Length Subnet Masking (VLSM)
  - Manual Dotted Decimal to Binary Conversion
- CIDR – Subnetting in the Real World
  - competency standard
- IP Address Assignment
  - two ways to give a host an IP address, subnet mask and default gateway
    - static addressing – manually
    - dynamic addressing – server input
- Static IP Addresses
  - manual entering IP info
  - each node on a network must have an IP address, subnet mask, and default gateway
    - decide network ID
    - IP Address Sequentially After
    - Separate Servers from Clients
    - Document Assignments
  - Windows → IPv4 Properties
  - MacOS → Network Utility in System Preferences
  - Unix/Linux → # ip addr add "ip" dev eth1
    - or ifconfig
  - static IP addresses done with ip command will be lost on reboot
    - Permanent → Network Configuration GUI
  - Verify with ping command
    - troubleshoot as necessary
- Dynamic IP Addressing
  - Dynamic Host Configuration Protocol
    - autoassigns IP addresses when a host connects to a network
    - DHCP Server and Clients
      - router for SOHO, server for Enterprise
      - client requests IP info, DHCP server responds
- How DHCP Works
  - Client sends out initial DHCP Discover Message on Broadcast
    - DHCP server responds with DHCP Offer
      - IP Addresses, subnet mask, gateway
    - Client Responds with DHCP Request
      - verifies offer is valid, accepting offer
      - DHCP server responds with DHCP Acknowledgement and lists MAC and IP info provided to client in a database
  - DHCP Handshake
    - client gets DHCP Lease after which a request is sent from client to server again
      - server provides IP info from MAC address
- Configuring DHCP
  - UDP Port 67/68
    - clients and servers

    - Clients – most hosts configured as a client by default via OS
    - Servers
        - hands on configuration
        - pool of legit IP addresses
        - knowledge of network subnet mask
        - knowledge of IP of default gateway
    - Pool of IPs = DHCP Scope
        - Scope Options
            - default gateway, network time server, DNS server, etc.
    - Router Assumes it is DG typically and self-assigns initial IP
- DHCP Relays
    - relies on broadcasting to work
        - DOR – on broadcast
        - A – unicast
    - within a domain, broadcast works but routers block broadcast traffic
        - but for enterprises it is impractical to apply DHCP servers for every LAN
    - DHCP Relays (built into most routers) accepts DHCP broadcasts from clients and sends, via unicast, addresses directly to DHCP server
        - must give relay IP of real DHCP Server; IP helper address
- DHCP Reservation
    - file servers, printers, cameras, multi-purpose devices and other hosts should never use DHCP
        - need fixed, permanent, statically assigned IPs
        - setting an IP exclusion will prevent DHCP from assigning an IP to a client
- MAC Reservations
    - assign a server a DHCP-assigned address via MAC reservation
        - assigns a specific IP to a specific MAC
- Living with DHCP
    - No DHCP Server
        - client cannot get address
        - Automatic Private IP Addressing (APIPA)
        - generated automatically if no response from DHCP
            - allows clients on some NetID to communicate but no Default Gateway
        - check IP – if APIPA, DHCP problem
            - try to establish IP manually → windows = ipconfig /renew
                - MacOS → Network Utility → Renew Lease
            - force lease renew → W → ipconfig /release → ipconfig /renew
                - MacOS → sudo ifconfig eth0 down → sudo ifconfig eth0 up
                - Linux → sudo dhclient -r → sudo dhclient
- Multiple DHCP Servers
    - Single DHCP Server → Single Point of Failure
    - Multiple DHCP Servers → assign different scopes with some subnet mask, DG, etc.
    - DHCP failover → two servers work together to provide DHCP to network
        - primary and secondary with a single scope
            - common in large networks
- Rogue DHCP Server
    - Easy to add DHCP server to network → assign wrong IPs
    - Rogue DHCP Server
        - unintentional → easy to detect, same clients can access internet and some cannot
            - ipconfig
                - DHCP clients with incorrect network IDs
        - intentional → hard to detect, IPs in same scope as legitimate DHCP server

        - change DG, enabling intercept/capture of incoming/outgoing traffic
- Special IP Addresses
    - loopback address
    - private IP addresses
        - never used on internet and blocked by routers
            - 10.0.0.0-10.255.255.255 Class A
            - 172.16.0.0-172.31.255.255 Class B
            - 192.168.0.0-192.168.255.255 Class C
        - all others are public

Chapter 7 – Routing

- Power of TCP/IP protocols in routing
    - allows interconnection of individual LANs into WANs
    - routers inspect incoming packets and forward them toward their eventual LAN destination
        - typically just require initial configuration
- How Routers Work
        - any piece of hardware or software that forwards packets based on their destination IP address
        - work at the network layer of the OSI model and at Internet Layer of TCP/IP model
        - typical routers can last for many years with software upgrades
    - typical home routers combine switches, routers, firewalls, DHCP servers
        - Boxes connect two networks
            - the home router connects directly to a built in switch
- Routing Tables
        - process begins with packets entering router for handling
        - router strips off Layer 2 info and drops resulting IP packets into a queue
            - router inspects IP packet destination address and sends packet to correct port
                - this inspection is performed via routing table
                - this table is key to understanding and controlling the process of forwarding packets to their proper destination
        - Destination LAN IP – a defined network ID – Every network ID directly connected to one of the routers ports is always listed here
        - Subnet Mask – to define a network ID, need a subnet mask
    - Routers use combinations of Destination LAN IP and subnet mask to see if a packet matches that route
        - Gateway – The IP address for the next hop router; where the packet should go
            - If the network ID is directly connected to the router, then a gateway is not needed
        - Interface tells the router which port to use, different routers use different descriptions
    - A router will check the entire table before sending the packet, choosing the better path if a packet works for more than one route
        - zeroes in a routing table means anything
    - Default Router tells router exactly what to do with every incoming packet unless another line in the routing table gives another router
        - Isolated and Tier One Backbones do not have default routes
    - Every node on a network has a routing table
        - a metric is a relative value that defines the cost of using that route – useful when directly connected to other NetIDs
        - Routing allows packets the option of taking more than one route, in case one route fails
        - Different routes require assignment of different metrics
            - automatic with Dynamic Routing

        - lowest always wins
    - Routers communicate and detect when routes are down
- Freedom From Layer 2
    - Routers enable connection to different network technologies
        - routers can connect to anything that stores IP packets
    - industry routers enable interface addition
- Network Address Translation
    - routers running NAT hide IP addresses on LAN computers while enabling communications with Internet
        - extended IPv4 addressing life
- The Setup
    - NAT replaces source IP addresses of a computer with the source IP address from the outside router interface on outgoing packets
        - performed by NAT capable routers
- Port Address Translation
    - Internal networks use a block of private IP addresses for hosts inside network
        - connect to Internet through one or more public IP addresses
    - most common NAT form is one-to-many
        - Port Address Translation (PAT)
        - PAT uses port numbers to map traffic from specific machines in the network
    - Src and Dst IP addresses and port numbers for TCP/UDP segment are recorded in NAT table
        - private IP addresses are swapped for public IP addresses on each packet
        - port number is also translated into a unique port number
        - when receiving system sends packet back, it reverses the IP addresses and ports and is compared to entries in NAT translation table
- Port Forwarding
    - PAT is not great for incoming communications. Tech traffic originating outside a network accessing an internal machine, another tech is required
    - Static NAT maps a single non-private IP address to a single machine
    - Port Forwarding can designate a specific local IP address for various network services
        - external computers can request a service using public IP and port number of desired service
    - Port Forwarding can hide a service hosted inside your network by changing the default port number for that service
        - to access such an internal site, the URL would have to be changed to specify the port request number
- Dynamic NAT
    - many computers share a pool of routable IP addresses that number fewer than the computers
    - an X amount of IP addresses can be served to a Y amount of computers for external access
        - if uses exceeds availability, issues arise
- Configuring NAT
    - Gateway = NAT On
    - Router = NAT Off
- Dynamic Routing
    - routers have the capability to update their routes dynamically, with dynamic routing protocols
- Routing Metrics
    - it is the role of the metric setting for the router to decide which route to use
    - Common Criteria
        - hop count, bandwidth, delay/latency, cost, MTU
    - Different dynamic routing protocols use one or more of these routing metrics to calculate their own routing machine
- Distance Vector and Path Vector

- DV – first to appear – total cost – hop sum, speed
  - compare total cost to get to a particular network ID within total cost to get to all the other routers for some network ID
  - entire routing table is transferred to other routers in WAN
  - Distance routers share tables, update, and pass along until a path is completed
    - compare paths to assign metric values
  - once a path is decided, routers continue to send their tables to one another
    - convergence/steady state as all updates are completed
    - convergence takes time and does not scale well with large numbers of routers
  - Two Different DV Protocols
    - RIPv1 – Routing Information Protocol – max hop of 15
      - updates every 30 seconds, cause overloads
      - didn't use variable-length subnet masking or authentication
    - RIPv2 – Current Version – VLSM + authentication added
      - obsolete for small WANs due to convergence time
      - easy setup is good for small WANs
    - Path Vector Routing Protocol
      - BGP
        - Autonomous Systems
          - one or more networks governed by a single dynamic routing protocol
        - AS's communicate via Autonomous System Numbers (ASNs) assigned by IANA
        - AS's use a generic External Gateway Protocol (EGP) to communicate with one another
        - AS internal communications use generic Interior Gateway Protocols (IGP)
      - BGP protocol is the Border Gateway Protocol
        - glue of the internet
        - path vector
          - advertising info passed to them from different AS's edge routers (AS to AS) which are forwarded to include ASN
        - ignores bad routes and policies for controlling how other routers reach ISPs
          - implements route aggregation
            - simplify routing tables by tracking routers that connect to subset location

- Link State
  - announce and forward individual route changes as they appeared, as opposed to forwarding entire tables
  - Two Link-State Protocols
    - OSPF – Open Shortest Path First – most commonly used IGP
      - designed to work with simple AS
      - faster convergence
        - connect to other OSPFs via Hello Packers
          - establish neighborship and exchange info via Link-State advertisements LSA packets
          - flood OSPF areas
      - Best routes are established and replacements if necessary
      - Cost Metric
        - bandwidth:bandwidth type

        - scales well, prevents loops, supports authentication
            - did not originally support IPv6
        - IS-Is – Intermediate System to Intermediate System
            - similar to OSPF but native support for IPv6
            - de facto standard for ISPs
    - ELGRP – Enhanced Interior Gateway Routing Protocol
        - CISCO Proprietary
        - hybrid between distance vector and link state
            - advanced DV protocol
    - Dynamic Routing Makes the Internet
        - essential
            - RIPv1, RIPv2
            - BGP
            - OSPF, IS-IS
            - EIGRP
    - Route Redistribution
        - routers cannot use different routing protocols to communicate, but can speak different protocols simultaneously
            - can announce routes from one protocol onto another via route redistribution
- Working with Routers
    - Connecting to Routers
        - special serial connectors – CISCO-specific
            - rollover/yost cable
            - managed devices
        - Plug into console port and serial port on PC or use a USB-to-serial Adapter
        - Use a terminal emulation program to talk to router
            - PuTTY, HyperTerminal
            - Basic Settings – 9600 band, 8 data bits, no parity
        - CISCO IOS
    - Web Access
        - router must have been built-in IP address or give the router an IP address
        - never plug new address into an existing network
            - always fully configure before placing online
            - laptop and crossover cable
    - Network Management Interface
        - NMS knows how to talk to software, routers, switches, computers, etc to give an overall view of network
        - OEM or third-party
    - Other Connection Methods
        - USB, Telnet, SSH – use network as opposed to cable
- Basic Router Configuration
        - must have a minimum of two connections
        - must configure every port on router to talk to network, ID and routing table function properly
    - Setup WAN side
        - know Network IDs for each side of router
        - DHCP
    - Setup LAN side
        - choose Network ID
    - Establish Routes
        - usually automatic
    - Configure Dynamic Protocol

        - tied to individual NICs that are configured to use Dynamic Protocol
    - Document and Backup
- Router Problems
    - routing tables
        - static routes
        - wrong netmasks
        - missing routes
    - typically manual input error
        - convergence issues
    - use traceroute and mtr
        - tracert (w)
        - traceroute (m + L)
    - mtr – dynamic, continually update route
        - mtr is linux – continuous
        - pathping is for windows – set time

Chapter 8 – TCP/IP Applications

- Transport Layer and Network Layer Protocols
    - TCP/IP → TCP over IP – HTTP,DHCP,POP,UDP,ICMP
        - TCP/IP Suite
            - Big Three – TCP, UDP, ICMP
- How People Communicate
    - only single communication between a computer and another computer is called a session
        - sessions are connectionless or connection-oriented
- TCP * Transmission Control Protocol
    - connection oriented communication
    - most common type
        - SYN – SYNACK – ACK
        - Threeway Handshale
            - session closes with FIN – ACK FIN – ACK
        - connection-oriented is designed to check for errors and asks for repeats as needed
- UDP * User Datagram Protocol
    - good for sessions that don't require overhead of connection-oriented
- DHCP * Dynamic Host Configuration Protocol
    - uses UDP
        - sends information for each step without confirmation as client wont have an IP address to begin 3-way handshake
    - Uses two port numbers
        - clients use port 67 to send/receive data
        - servers use 68 to send/receive data
- NTP/SNTP * Network Time Protocol/Simple NTP
    - both use UDP
    - synch clocks of devices on a network
        - via port 123
- TFTP * Trivial File Transfer Protocol
    - uses UDP to move files across machines within the same LAN
        - port 69
- ICMP * Internet Control Message Protocol

    - works at L3 to deliver connectionless packets and handles mundane issues such as host unreachable messages (like ping)
        - sends ICMP “echo” request to which TCP/IP computers respond with “echo reply”
- IGMP * Internet Group Messaging Protocol
    - enables routers to communicate with hosts to determine a group membership
        - IGMP Group is assigned to an address in the Class D range
        - Those who wish to receive the multicast must tell their upstream router or switch that they wish to receive it
            - joining the IGMP Group
- The Power of Port Numbers
    - TCP/IP port numbers between 0 and 1023 are the most well-known
    - clearly defined port numbers exist for well-known TCP/IP applications
    - 16-bit value between 0 and 65,535
        - web servers – port 80
    - web client source port number is generated pseudo-randomly by web-client computer
        - generally 1024-5000 – ephemeral port numbers
        - 49152-65535 – dynamically/private port numbers
    - ephemeral port numbers are used as the destination port to get the info back to the web client running on the client computer
- Registered Ports
    - 1024-49151 – registered ports
        - anyone can use these port numbers for their servers or for ephemeral numbers on clients
        - most Oss opt to use dynamic/private port numbers for ephemeral ports
    - Computers keep track of status of communication (Storing IP addresses and Port numbers in RAM) in a socket or endpoint
        - socket pairs or endpoints
    - show list with netstat -n
        - a single webpage may have multiple connects to a clients computer
            - TCPView – OpenSource and Free, netstat but actively update
            - NetActivity Viewer
- Connection Status
    - open/listening port is any socket that is prepared to respond to any IP packets destined for that sockets port number
        - netstat -an, -ano, -b
        - ps
        - Task Manager, Process Explorer
- Common TCP/IP Applications
    - The World Wide Web
        - the web is composed of servers that store specifically formatted documents using language such as HTTP or HTML, XML
        - all web servers have a default web page unless otherwise specified
- HTTP
    - runs on port 80
    - ID how messages are formatted and transmitted, requests and responses
    - HTTP is relatively simple, requiring Java/Ajax, server-side scripting, and cookies for smart website creation
- Publishing a Website
    - most ISPs offer web servers, though individual hosting is possible
        - price varies
    - upload HTML pages to a webhost, upload to a web server
- Web Servers and Web Clients

- servers deliver/serve up web pages
    - listen on port 80 and fetch requested HTML pages
- Any computer can be a server through software
    - Microsoft IIS
        - set max connection limit depending on available bandwidth/memory
            - protection against DoS
    - Unix/Linux Apache HTTP Server
            - popular, can run on Windows, free
        - executed with text files
            - GUI webadmin, webmin
            - nginx, GWS

- SSL/TLS and HTTPS
    - for security, require authentication, encryption, and nonrepudiation
- Secure Sockets Layer
- Transport Layer Security
    - latest version of SSL
        - uses encryption
- HTTPS uses port 443

- Telnet and SSH
- Telnet Protocol (unsafe) allows remote access of a computer via command line
    - port 23 – TCP
- remotely administrate a server and communicate with other servers on a network
- no encryption
    - use SSH instead

- Telnet/SSH Servers and Clients
- freeSSHd
- PuTTY

- Configuring a Telnet/SSH Client
- provide hostname, login name, password

- SSH and the Death of Telnet
- SSH does what Telnet can but securely encrypted
    - SSH – TCP – port 22

- Email
- email programs use a number of application level protocols to send and receive information
    - SMTP – Simple Mail Transfer Protocol – to send
        - port 25 – TCP
    - POP3 – Post Office Protocol version 3 – receive
        - port 110 – TCP
    - IMAPv4 – Internet Message Access Protocol version 4
        - port 143 – TCP
        - preferred over POP3
        - enables device synch, folders
- also web-based (gmail, outlook, yahoo!)
    - proprietary

- Email Servers
- Exim – 50% of market share
- PostFix

- Email Client
    - Outlook, Thunderbird
- Configuration
    - enter POP3/IMAPv4 domain name and SMTP server domain name to email client

        - password, username
- FTP * File Transfer Protocol
    - old active FTP used TCP ports 20 + 21
    - passive FTP uses port 21
    - FTP sites are usually anon or secure sites
- FTP Servers and Clients
    - servers store files, accept connections, verify usernames/passwords, file transfers
        - client logs in and downloads files
    - FileZilla Servers
        - not secure by default without login credentials
        - check client support numbers
    - CyberDuck FTP Client
- Active and Passive FTP
    - active works unless client uses NAT
    - passive uses port 21 for requests and replies with random port number
        - client initiates all conversations allowing NAT greenlight

---

Chapter 9 – Network Naming

- All TCP/IP networks, including the internet, use a name resolution protocol called Domain Name System (DNS)
- Before DNS
    - two continue to work in modern systems: NetBIOS and Hosts
- NetBIOS
    - used broadcasts for name resolution. A computer would broadcast name and MAC upon boot up
    - all receiving systems would store info in a cache, whenever a system was missing a NetBIOS name, the broadcast would start again
    - only suitable for small networks – 40 hosts max
        - no logical addressing like IP addresses, each system had to remember the NetBIOS name and the MAC
            - without logical addressing, routing cannot be supported
        - widespread broadcasting made it unacceptable for large networks
    - NetBIOS over TCP/IP (NetBT) runs NetBIOS on top of TCP/IP
        - a name resolution protocol that had nothing to do with DNS
        - ports 137, 139 (TCP)
        - ports 137, 138 (UDP)
    - NetBIOS only handles host names, but did not do resource sharing (Server Message Block) TCP 445
- Hosts
    - original TCP/IP specification implemented name resolution using a special text file called hosts
    - the host file contained a list of IP addresses for every computer on the internet
        - this file still exists in every computer but is not relied on, OS hosts did not scale with growth of the internet
        - same users place shortcut names in a host file to avoid typing long names in certain TCP/IP applications
            - AV/AM uses this to block malicious sites
- DNS
    - How DNS Works
        - delegation through hierarchical DNS servers
        - DNS servers primarily use UDP port 53

        - DNS root consists of 13 DNS server clusters
            - delegate name resolution to other servers
        - Top Level Domain Servers
            - handle TLD names (.com, .org, .net, .edu, .gov, .mil, .int) and country codes
        - Second Level Domain Servers
            - handle millions of names created within each top-level domain
            - support individual computers
        - ICANN created additional TLDs (.biz, .info, .pro)
        - DNS names have a max of 255 characters
    - Name Spaces
        - DNs hierarchical name space is an imaginary tree structure of all possible names that could be used within a single system
        - host files use a flat name space
            - individual, no grouping
            - require all names be unique
        - DNS namespace is a hierarchy of DNS domains organized into a DNS tree
                - domains = folders, separated within a period
            - Top of DNS tree is root
                - host names fit into domains
        - Private TCP/IP networks require at least one DNS server as the root of the intranet
            - DNS naming convention works in reverse of a typical file path
                - fully qualified domain name (FQDN) written with root on far right, followed by the names of the domains added to the left, and host name on far left
                - always have period on the end to signify the root
            - Private networks don't need TLDs
    - Name Servers
        - DNs Server – computer running DNS server software
        - Zone – container for a single domain that gets filled with records
        - Record – a line in the zone data that maps an FQDN to an IP address
        - DNS servers store DNS info
            - system requires IP address for an FQDN via DNS query
            - a single DNs server is an authoritative name server if it lists all names on the domain and corresponding IP address
        - A single domain can use more than one DNS server – large scale domains start with a primary DNS server and one or more secondary DNS servers (master and slaves)
            - all servers know one another to communicate frequently
                - maintain updates
        - DNS root servers know where to send requests
        - Domain Names must be registered for Internet use with ICANN
    - Name Resolution
        - Since routers do not forward broadcasts, another method must be used
        - modern hosts automatically map the hosts file to the hosts DNS resolver cache
            - contains recently resolved addresses
        - When a name is entered, a host contacts its DNS server and requests IP addresses
            - PC must know IP of its DNS server as DNS server data is part of the critical basic IP information such as IP address, subnet mask, and default gateway
        - DNs is configured via IPv4 Properties dialogue box (Windows); Network Config Utility (Linux),
            - verify with ipconfig, and "cat /etc/resolve.conf (Linux/Unix)

        - DNs Server first checks resolver cache, if not, checks root server that handles a given name operator (like .com) which shares IP address at a .com server
            - which shares IP address of website DNS server
                - which shares IP address of website
            - once discovered, it is stored in resolved cache and allows HTTP requests to begin
- DNS Servers
    - Microsoft Server and Unix/Linux come with DNS Server software
        - every DNS server keeps a list of cached lookups (all resolved) – which has a size limit – divided into subfolders that share SLD
        - Choose authoritative or cache-only server
            - authoritative share IP addresses and FQDNs
            - cache-only are never authoritative, only used to communicate with other DNS servers to resolve IP addresses
    - IP addresses and FQDNs for computers in a domain are stored in forward lookup zones – important
- DNS Record Types
    - A record – workhorse
    - SOA, NS, CNAME, AAAA, MX, SRV, TXT
        - SOA – start of authority – defines primary name server in charge of forward lookup zone
        - NS – shows primary server name for a domain
        - MX – mail servers, SMTP server to determine where to send mail
        - TXT – freeform record type, any text can be added to a forward lookup zone
        - CNAME – Canonical name record acts as an alias – querying this will often return host name
        - AAAA – equivalent to A records but reserved for IPv6
        - SRV – generic record that supports any type of server
- Primary and Secondary Zones
    - Primary Zones – act as primary name server for that zone
    - Secondary Zone – created on other DNS servers to act as backups to the primary zone
    - Typical to have a minimum of Two DNS servers for any forward lookup zone, both authoritative
    - Reverse Lookup Zones enable a system to determine an FQDN by knowing the IP address
        - take a network ID and reverse it, creating a PTR pointer record
        - Low-level (like mail) functions use reverse lookup zones
    - For A Records to be added automatically, Windows uses NetBIOS to name the DNS name and making SMB protocol run directly on TCP/IP without NetBT
        - SMB and NetBIOS over TCP ports – UDP 137,138; TCP 137,139
        - SMB without NetBIOS – TCP ports 445
        - Linux uses Samba
- Living with SMB
        - uses dual name resolution scheme
            - local – SMB
            - Internet – DNS
        - a Windows domain must have a true DNS name
    - Active Directory – a super domain is an organization of related computers that share one or more Windows domains
        - windows domain controllers are also DNS servers
            - all domain controllers are equal partners
- Active Directory – Integrated Zones
        - nothing can be updated if a primary server goes down
            - unless using an Active Directory Integrated Zone
                - eliminating the need for zone transfers

- Placing DNS Servers
    - Do individual hosts need DNS to resolve hosts on the local network>
        - small LANs can use SMB
        - organizations use DNS
            - Local DNS for Intranet
    - Do individual hosts need DNS to resolve Internet names?
        - always yes if connected to internet
            - Internet DNS
- Local DNS
    - internal DNS server
        - contains forward lookup zone for in-house domain
            - both primary and secondary
    - can also handle internet naming needs via DNS forwarding any DNs requests for which the local server is not authoritative
        - small networks use gateway routers that contain rudimentary DNS for forwarding and caching
        - DNS Server without forwarding and no root hints in a cache-only server
- Private and Public DNS
    - Internal → Private/Invisible – Server behind firewall
    - Public → Never behind firewall
    - Public DNS servers handle FQDN equally, rarely go down, with faster resolution speeds and avoid DNS reflections
        - Level 3 – Cloudflare, DNS Witch, OpenDNS, SafeDNS
- External DNS Servers
    - not internal to an organization
    - external DNS servers (except for root) must connect to other DNS servers that are always external to an organization
        - third party DNS servers offer both public and private services or cloud-based (Azure, AWS)
- Dynamic DNS
    - manual uploading of DNS records is common for web and email servers
    - Dynamic DNS (DDNS-1997) enabled DNS servers to get automatic updates of IP addresses of computers in their forward lookup zones via DHCP Server
        - Windows uses DDNS to talk with DHCP for updates to records (A Records)
- DNS Security Extensions
    - DNS Security Extensions (DNSSEC)
        - authorization and integrity protocol preventing impersonation of legitimate DNS servers
    - Implemented via Extension Mechanisms for DNS (EDNS)
    - DDNS on the Internet
- IPAM * IP Address Management
    - software including DHCP and DNS servers specifically designed to work together to administer IP addresses for a network
- Troubleshooting DNS
    - servers rarely go down and have backups
    - Server Not Found Error
        - Test
            - eliminate DNS caches on local system with /flushdns
            - Run ping to test
                - OK is msg “request timed out”
                - If can ping IP but not name, check DNS
            - Ensure correct server entry

        - ipconfig /all
    - If all info matches, nslookup to query DNS server
        - if error, primary server is down or incorrect server settings
- Diagnosing TCP/IP Networks
    - improper Configuration
        - Diagnose NIC
        - Check NIC Driver
        - Diagnose Locally
        - Check IP address and subnet mask
        - Run netstat
            - statistics to help diagnose problems
        - Diagnose to the Gateway
            - ping router
        - Router Status by Ping, before, at or after
        - Traceroute addresses on internet to check path

Chapter 10 – Securing TCP/IP

- Making TCP/IP Secure
    - Five Areas of TCP/IP Security
        - Encryption, Integrity, Nonrepudiation, Authentication, and Authorization
- Encryption
    - all data starts as plaintext → key + alg → ciphertext
    - Substitution
        - earliest forms of cryptography
        - broken with patterns, frequency analysis, BF
    - XOR
        - Binary Exclusive OR
        - uses a third key value as parts of the alg
        - need to know alg + key to decrypt
    - Symmetric/Public + Asymmetric/Private
- Symmetric Key Encryption
    - most algs use block ciphers to decrypt chunks
        - good when data comes in chunks (like IP packets over wired networks)
    - DES – oldest, 64bit block, 56bit key (Vulnerable to BF)
    - Alternative to Block Cipher is Stream Cipher
        - single bits, popular when long data streams are used
        - RC4 – popular, but legacy and vulnerable
    - AES is commonly used now for symmetric
        - 128bit block with 128, 192, 256 bit key sizes
        - very secure
- Asymmetric Key Cryptography
    - allows sender to transmit key with increased safety via two separate keys
    - RSA
- Encryption and the OSI Model
    - L1 – no common encryption, large WANs use SONET
    - L2 – no common encryption
    - L3 – IPsec only via software
    - L4 – no common encryption due to TCP/UDP

- L5, 6, 7 – SSL/TLS
- Integrity
  - Hash
    - value of fixed length (checksum, message digest)
      - 100-500 bits
        - one-way function, irreversible and unique output per input stram
    - file hashing allows for comparison
    - passwords are hashed for mass storage, also compared
      - MD5 – common – 128 bit
      - SHA1-3
  - Encryption and authentication schemes use hashes
    - SMTP → CRAM-MD5 → Server Authentication
- Non-Repudiation
  - Digital Signatures
    - hash of public key encrypted by private key for comparison
  - PKI
    - certificates are standardized files with a public key and a digital signature + digital signature of a trusted third party company
    - Checked via certificate Authorities
      - Tree of Certifications
    - PKIs aren't mandatory to use certificates
      - certs and asymmetric cryptography operate hand-in-hand
- Authentication
  - local authentication (logins)
  - Multi-factor (Something you know, have, are, do)
- Authorization
  - Access Control List
    - Network Access Controls (NAC)
    - Permissions
    - Models
      - Mandatory (MAC) – every resource is assigned a label that defines its security level
      - Discretionary (DAC) – resource owners assign access to a resource at their discretion
      - Role-Based (RBAC) – popular in file sharing – defines user access to a resource based on roles the user plays in the network environment
        - leads to group creation
- TCP/IP Security Standards
  - Point-to-Point Protocol (PPP)
    - enables two p2p devices to connect, authenticate with username and password and negotiate network protocol the two devices will use – typically TCP/IP
      - Password Authentication Protocol (PAP) – unsafe cleartext transfer of login
      - Challenge Handshake Authentication Protocol (CHAP) – provides more secure routine with hashing
        - repeats intermittently to prevent MitM
  - AAA – Standard to follow when overseeing central databases
    - Authentication, authorization, and Accounting
      - port authentication
    - Authentication – credentials for network access
    - Authorization – capability determination

            - Accounting – Auditing
        - RADIUS and TACACS+
    - RADIUS – Remote Authentication Dial-In User Services
        - support ISP connections to a single database
            - RADIUS Server – supports PAP, CHAP, MS-CHAP
            - Network Access Servers (NACs)
            - Groups of connected systems
        - Microsoft Internet Authentication Service (IAS)
        - Unix/Linux – FreeRADIUS
        - Pulse Secure Steel-Belted RADIUS
        - UDP port 1812, 1813
        - UDP ports 1645, 1646
    - TACACS+ - Terminal Access Controller Access Control System Plus
        - single server storing the ACL for all devices in the network
        - Cisco support of AAA in large complex networks
            - TCP port 49
                - separates AAA into different ports
            - PAP, CHAP, MD5, Kerberos
    - Kerberos
        - no connection to PPP
        - many TCP/IP networks all connected to a single authenticating server
        - adopted as authentication protocol for all Windows networks using a domain controller
            - windows domain is a group of computers that defers all authentication to a domain controller
            - domain controller stores a list of all user names and passwords
                - login occurs on domain controller
        - Kerberos uses Key Distribution Center (KDC) on domain controller
                - Authentication Server (AS)
                - Ticket-Granting Service (TGS) and Ticket (TGT)
            - Login sends a request with hashed login info to AS, AS compares hash and responds with TGT and timestamp → authenticated, but not authorized
                - 10 hour lifespan
            - Client sends timestamped TGT to TGS for authorization
                - TGS sends a timestamped service ticket (token) back to client
            - token is used to access domain resources
                - contains security identifier (SID) of user account and SIDs of groups user is a part of
                    - allows for single sign-on without reauthentication
        - Kerberos forces 8-hr timestamps
        - Kerberos has weaknesses
            - KDC goes down – no access
                - requires backup KDC
            - Timestamp requires clock sync
                - easy on wired networks, difficult for dispersed networks
- Encryption Standards
    - SSH
        - servers use PKI in the form of an RSA key and asymmetry
        - AES encryption
        - Logins are used for identification or public keys (PuTTYgen for RSA/DSA keys)
            - can be turned off for hardening
        - also acts as a tunnel

    - Tunneling
        - encrypted link between two programs
        - SSH tunnels are popular and easy
- Combining Authentication and Encryption
    - SSL/TLS
        - requires server with certificate, checks copy of cert against CA root cert list
        - TLS is an upgrade to SSL – more flexible in application
    - IPSec
        - authentication and encryption protocol suite that works at the Internet/Network Layer and will grow with IPv6
        - Transport Mode – only actual payload of IP packet is encrypted; dest/src IP address and header info visible
        - Tunnel Mode – entire packet is encrypted and placed into IPsec endpoint where it is encapsulated inside another IP packet
- Secure TCP/IP Applications
    - HTTPS
        - SSL/TLS
            - if certs expire, tread carefully
            - if certs are on revocation list, avoid
    - SCP
        - Secure Copy Protocol
            - replaced by SFTP
    - SFTP
        - SSH File Transfer Protocol
            - replaced SCP and FTP
            - TCP port 22
    - SNMP
        - Simple Network Management Protocol
            - query state of SNMP capable devices
            - agents collect network info from management information base (MIB) server
                - SNMP3 is current/safe for network admins
    - LDAP
        - Lightweight Directory Access Protocol
            - query and change database used by the network
                - Windows Active Directory
                    - Windows Domain Controllers, every backup must have a copy and be able to take control/update
            - LDAP used when a computer needs to access another database for info/make an update
                - used automatically via Domain Controllers TCP/UDP port 389
    - NTP
        - Network Time Protocol
            - gives current time, important when using Kerberos
                - UDP port 123

Chapter 11 – Advanced Networking Devices

- Virtual Private Networks
        - an encrypted tunnel requires endpoints
        - VPNs are usually either software on dedicated boxes

        - computer must be on same network with uniform network ID or share software
        - VPN creates virtual NIC on device to create endpoint 1, which connected to endpoint 2
            - creating a tunnel
    - PPTP VPNS
        - Point to Point Tunneling Protocol
            - advanced PPP with endpoints placed on client and server
                - server endpoint – routing and remote access service (RRAS)
                - client endpoint – control panel VPN, Virtual NICE DHCP query
            - once connected to RRAS server, PPTP creates a secure tunnel
                - client takes on IP address of target network
                - host-to-site connection
    - L2TP VPN
        - Layer 2 Tunneling Protocol
        - PPTP + Cisco Layer 2 Forwarding (L2F) with support for any connection type
        - Local LAN endpoint connected to VPN concentrator (router)
            - site-to-site connection possible
        - No authentication/encryption (as PPTP has), using IPsec
    - SSL VPNs
        - don't require client software, connecting via web browser with the traffic secured using TLS
            - SSL Partial VPNs – secure webpage
            - SSL Tunnel VPNs – active control, greater access
    - DTLS VPNs
        - Datagram TLS
            - optimize connections for delay-sensitive applications (voice/video) using UDP datagrams
                - CISCO AnyConnect
    - DMVPN
        - Dynamic Multipoint VPN
            - enables direct VPN connects between multiple locations directly without need for central connection
            - employs IPsec
    - Alternative VPNs
        - OpenVPN, SSH, Generic Routing Encapsulation Protocol (GRE)
        - pure IPsec solutions
- Switch Management
    - Managed switches have programming and logic to handle switching, security, etc
        - requires configuration via
            - direct plugin to serial interface using veritual terminal and CLI
            - switch onto network, virtual terminal over SSH and CLI
            - Get switch onto network and use switch built-in GUI
    - Many managed switches have a special serial port called a console port
        - plugin via laptop, use PuTTY
            - common for initial config
    - Switch needs IP address, will have default IP, login, and settings that will require change
        - DNS, Default Gateway, etc.
        - for maintenance
    - To reduce exposure, it is common to dedicate one port on every managed device as a management port
        - interface configuration can only be done on that port

- Then plug all management ports into a switch that is totally separate from the rest of the network
  - this prevents unauthorized access to said ports
    - out of band management
- Switches often have an HTTPS/management URL
  - in-band management

- Virtual LANs
  - enables segmentation of a physical network into multiple discreet networks without adding hardware
    - take single broadcast domain, with one or more switches, and divide into multiple broadcast domains
      - via assigning each port to a specific VLAN
    - managed switches can handle any number of VLANs
- Trunking
  - process of transferring VLAN traffic between two or more switches
    - configure a port on each switch as a trunk port – carry all traffic between all switches in a LAN
      - Ethernet Switch – IEEE 802.11Q
- Configuring a VLAN-capable Switch
  - SSH – CLI
  - Web Browser GUI
    - CISCO Network Assistant
  - aassign ports – VLAN assignment
- Tagging
  - access ports, tag traffic with appropriate VLAN when frames enter the switch
    - access ports connect to workstations
  - Tagging and Untagging ports on VLAN switches, changing native VLAN to mitigate double-tagging attacks
    - native VLAN is set to unused VLAN and trunk port tags native VLAN traffic
- VLAN Trunking Protocol
  - Cisco VLAN Trunking Protocol (VTP) automates the updates of multiple VLAN switches
    - switches enter one of three states
      - server – master
      - client – updates with server
      - transparent – manual settings with no updates
- InterVLAN Routing
  - each VLAN has own broadcast domain – no way for data to get from one VLAN to another without router or multilayer switch
    - InterVLAN Routing
      - router-on-stick configuration
        - single router interface to connect to multiple VLANs on a switch
    - Many VLAN-capable switches also do routing
- DHCP and VLANs
  - DHCP requests cannot go through a router, single subnet only
    - a DHCP relay agent (enabled/configured on router) will pass DHCP requests along across router interfaces
      - Cisco IP helper command
  - DHCP relay support (ports 67, 68); TFTP (port 69); NTP (port 123); TACACS+ (port 99); DNS (port 53); NetBIOS (port 137); and NetBIOS Datagram (port 138)

- Troubleshooting VLANs
  - typically port assignment

- Multilayer Switches
  - L2 + L3 switch
    - L2 switch – forwards traffic via MAC
    - L3 switch – forward traffic via IP
      - a hardware version of a software L3 router
      - Router ports require IP address
  - Switch port and Router port
    - good for load balancing, quality of service, port bonding, and network protection
- Load Balancing
    - a single IP address divided over multiple servers
      - creates a server cluster
        - balance demands amongst servers
  - Methods
    - DNS Load Balancing
      - public IP, multiple A records, same FQDN
        - A Records accessed in round robin fashion as requests arrive
    - Content Switch
      - L7 – read HTTP(S) requests (handle SSLs, cookies) and lightens server workload
    - QoS and Traffic Shaping
      - prioritize traffic based on certain roles (bandwidth for clients)
        - traffic shaping controls flow of packets into/out of network
- Port Bonding
  - joining two or more ports logically in a switch so that the resulting bandwidth is treated as a single connection and the throughput is multiplied by the number of linked connectors
    - increase speed of links without upgrading infrastructure
    - NIC teaming, port aggregation
      - Port aggregation Protocol (PAgP)
      - Link Aggregation Control Protocol (LACP)
        - IEEE 802.1AX-2014
- Network Protection
    - IDS/IPS, Proxy Servers, Port Mirroring, AAA
  - IDS/IPS
    - dedicated software separate from a firewall, functioning within the network
    - network-based or host-based
      - network – NIDS is placed around network at multiple points
      - host – runs on individual systems
    - Both check definition files for signatures to compare against
    - IPS sits directly in the traffic
      - can stop attack but causes latency issues and can be a SPoF
  - Port Mirroring
    - copy data from any or all ports on a switch to a single physical port
    - allows admin to inspect packets to/from certain computers
      - local – onto same switch, connect to that switch
      - remote – does not require direct plugin for review
  - Proxy Server
    - redirects client requests to a proxy server, avoid usual DNS resolution
      - HTTP(S) goes to proxy, then to web server
        - benefitted by caching
    - A forward proxy server acts on behalf of clients

        - a reverse proxy server acts on behalf of servers
        - any TCP application can take advantage of proxy servers
            - Squid
    - AAA
        - supports port authentication
        - RADIUS + 802.1X port authentication, TACACS+
        - very difficult to configure
            - locate and read errors

Chapter 12 – IPv6

- IET – IPv6
    - 128bit addressing space = 2^128 addresses
        - IPsec standard protocol support for every IPv6 stack
        - More efficient routing scheme using a smaller routing table footprint via aggregation
- IPv6 Basics
    - always uses link-local addressing for communications with local network
- IPv6 Addressing Notation
    - octets are gone, use colons over period with quartets/hextets between 0000 and ffff
        - two 64bit sections
            - network prefix – first 64 bits – for routing
            - interface ID – second 64bits – broken down into global routing prefix and subnet ID
    - Eight groups of four hexadecimal characters
        - leading 0's can be dropped, strings of 0's can be replaced with :: - only one per address
    - Still uses /x convention (like CIDR)
        - signifying bit length of network prefix
        - unspecified addresses (all 0's or all 1's, cannot be used)
- Link-Local Addresses
    - host no longer has a single IP address unless network is not connected to a router
    - Upon first boot, a link-local address is self-assigned to the computer
        - always begins with fe80:
    - The Interface ID is generated one of two ways
        - old 0's used to MAC to create 64-bit Extended Unique Identifier (EUI)
            - no longer used
    - Current OS's generate a random 64-bit #
    - Link-local performs all necessary work when Internet is not connected
- IPv6 Prefix Length
    - used to determine whether to send packets to a local MAC address to default gateway to send out packets to internet
        - last 64bits are generated by NIC
        - RIRs pass out /48 prefixes to ISPs plus 16 bits for subnetting
            - then provide 64bit interface IDs to users
- The End of Broadcast
    - Link-local IPv6 address is unicast to that system
        - no broadcast is used
            - replaced with multicast
    - IPv6 multicast functions similarly to IPv4 multicast but with additional functions
        - only routers read messages
        - encapsulated Ethernet Frames use 33-33-xx-xx-xx-xx for IPv6

        - computers not specifically setup to process said frame will drop it at L2
            - a computer must be configured as a member of a particular group to read a particular multicast
                - ff02::1 – all nodes addr
                - ff02::2 – all routers addr
                - ff02::1:ff:xx:xxxx – solicited node addr
        - IPv6 also uses anycast
            - gives a number of computers or clusters the same IP address
                - routers then use BGP to determine which computer in the cluster is closest
                    - packets are sent to closest root DNS server
            - anycast addresses are unicast addresses, but this is only known by the top-tier router that sends packet to closest root server
- Global Unicast Address
    - second IPv6 address for computer
        - commonly derived from default gateway
            - router determines prefix computer generates last 64-bits
            - true internet address
                - prefix delegation from upstream ISP
- Aggregation
        - routers underneath another router use a subset of that routers existing routes
        - gives detailed geographic picture of router organization
    - IPv6 network is capable of changing constantly to maintain aggregation
- Regional Internet Registries
    - ARIN, RIPE NCC, APNIC, LACNIC, AfriNIC
- Using IPv6
    - rarely need static IPs, DHCP almost non-existent
    - uses Neighbor Discovery Protocol
        - five packet types
            - Neighbor – solicitation, advertisement
                - search for computers in broadcast domain, only head by IPv6 machines
            - Router – solicitation, advertisement, redirect
                - attain network IDs rather than through NAT and private network IDs
- Is IPv6 Working
    - ipconfig (windows)
    - ip addr (linux)
    - ifconfig (mac)
- DHCPv6
    - gives better control over LAN in certain situations
    - DHCPv6 Server must first be configured
        - complete IP info – stateful – similar to DHCP for IPv4
            - Stateless – gives partial IP info, relying on router advertisements
- DNS in IPv6
    - uses AAAA records
- Getting Past the IPv4 – IPv6 Gap
    - transition mechanisms
        - 4 to 6
            - encapsulated data type into another. IPv4 encapsulated into IPv6 tunnel to get to IPv6 router
            - needs tunneling client
        - 6 to 4

        - one of two tunneling protocols that get IPv6 through IPv4 NAT
- ISATAP
    - Intra-Site Automatic Tunneling Addressing Protocol
        - works within IPv4 network by adding address to an IPv6 prefix for endpoint address
- Tunnel Brokers
    - create actual tunnel and offer custom-made endpoints client for use, to avoid manual connection
        - usually use Tunnel Setup Protocol (TSP) or Tunnel Information and Control Protocol (TIC)
- Overlay Tunnels
    - enables two IPv6 networks to connect over an existing IPv4 infrastructure
        - run dual stack
    - local net traffic encaps in IPv4 packets, router strips away IPv4 packet and forwards inner IPv6 packet
    - manual tunnels can be set for point-to-point secure IPv6 connections with IPsec
- NAT64
    - NAT from IPv4 not needed in IPv6
    - NAT64 is a transition mechanism that embeds IPv4 into IPv6 for Network traversal with a NAT64 gateway handling traffic between IPv4 and IPv6 segments

---

Chapter 13 – Remote Connectivity

- Telephony and Beyond
    - The vast majority of the long distance connections that make up the internet use a unique type of signal called SONET
        - Most high-speed internet connections still use tech designed to handle phone calls
- The Dawn of Long Distance
    - Analog signals – degraded over long distance
        - Many individual wires – solved with multiplexers which combined circuits – split with demultiplexer
        - Uses modulation technology
            - Served local exchanges all over country – houses in central offices
            - Analog eventually moved to digital
        - Calls kept separate via frequency multipliers, assigning individual frequency ranges in the frequency division multiplexing (FDM) process
    - Digital is better over long distance (via repeaters)
        - Trunk lines are analog but connections between central offices and homes are converted into digital
- Digital Telephony
    - It all starts with DS0
        - Analog converted into 8-bits 8000xsec = 64kbps DS0 digital signal rate, connected at central office
    - Copper Carriers: T1 and T3
        - First digital trunk carriers – “T-carriers”
            - T1 – most common/basic, at either end (termination) is a channel service unit/digital service unit (CSU/DSU) – point-to-point (no more than two CSU/DSUs on a single T1 line)
            - User digital signal 1 (DS1) – primitive frames of 25 pieces (frame bit and 24 channels) with each channel holding single 8-bit DS0 data sample
                - 193 bit/frame x 8000/sec = 1.54Mbps

        - T3 Lines support 45 MBps – 672 individual DS0 channels – DS3 lines (E3 in Europe – 34 Mbps)
            - E1 and SONET use derivative of HDLC protocol
        - CSU/DSU have two connectors (at least) – one goes to Demarc, and another goes to router
            - Performs line encoding and conditioning, has a loppback function (built in to newer routers)
        - CSU protects against interference/lightning, stores statistics
        - DSU provides timing to user ports, framing, and formatting
    - Fiber Carriers: SONET/SDH and OC
        - SONET remains primary standard for long-distance, high-speed, fiber-optic transmission systems
            - Defines interface standards at Physical and Data Link Layers
        - Most long distance pipes use rings-topo for fault tolerance
            - Rings can combine DS1, DS3, E1 signals into singular massive frames
        - Optical Carrier (OC) standards denote optical data-carrying capacity of fiber-optic cables in networking using SONET
            - OC speeds from 51.8 Mbps (OC-1) → 39.8 Gbps (OC-768)
            - Wavelength Division Multiplexing (Dense WDM enables single-mode fibers to carry signals with wavelength via laser light colors = 7.6 Gbps (off a 51.8 Mbps OC-1)
                - Coarse WDM is simpler, but limited to 60Km – 10 GBase – LX4 nets
        - SONET uses STS Signal Method – two parts: payload and overhead
            - Payload = data, overhead = signal and protocol info
                - STS – 1, 3, 17, 24, 48, 192, 256, 768
- Packet Switching
    - Enables interconnecting of multiple T1, T3, OCs rather than just P2P – (First Gen called X.25 Packet Switching Protocol)
        - WAN connections use either Frame Relay or ATM
    - Frame Relay
        - T-carrier lines, on-again-off-again LAN traffic L1 + L2 OSI (frames, not packets)
        - Switches frames quickly, no integrity guarantee
            - High-level protocols do integrity checks
    - ATM
        - Asynchronous Transfer Mode – voice, video, data in one via short, fixed length “cell” frames (53 bytes) – 152.52-622.08 Mbps
    - MPLS
        - Multiprotocol Label Switching
            - Replace Frame Relay and ATM
            - MPLS Label sits between L2 header and L3 info
                - Label:A – unique ID used by MPLS routers
                - Exp: Relative value that determines importance
                - S: single bit value, single packet with many labels
                - TTL: Determines hop #
            - Allows routers to avoid running IP packets through full tables, relying on headers = faster
                - FEC – set of packets that can be sent to the same place – single broadcast domain
                - LSR – looks for and forwards packets based on MPLS label
                - LER – MPLS router that adds MPLS labels to incoming packets without one and stripping off ones that do

        - LDP – LSRs and LERs use LDP to communicate dynamic state info
    - LERs determine routers (entrances and exits for MPLS network) and add labels to packets as they leave FECs
        - LSRs strip away labels and add their own, progressing until packets leave opposing LER
    - MPLS are good for end user VPNs
        - Permanent virtual circuits (PVCs), popular for connecting separate customer locations
- Real-World LAN
    - ISP/Telephone company runs T-carrier line to Demarc, installs CSU/DSU on other side, and connects to router
    - Bit Error Rate Test (BERT) verifies T-carrier connection from end-to-end
- Alternative to Telephony WAN
    - T1, T3, OC-x replaced with 10Gbps, 40Gbps, or 100Gbps Ethernet on single-mode fiber and connected to DWDM capable switches
        - Metropolitan Area Network (MAN)
    - Good for dedicated connections
- The Last Mile
        - Solutions: dial-up, DSL, Broadband cable, Satellite, Fiber
    - Dial-up
        - Dedicated or dial up
        - Public Switched Telephone Network
            - Oldest/slowest – regular telephone line from LEC local office
                - Band rate of 2400 – RJ45 jack
            - Modem jacked in goes to either NIC or Demarc
                - Parallel data converted to serial digital then converted to analog
            - Modem and Universal Asynchronous Receiver/Transmitter (UART)
    - Bit Rate vs Band Rate
        - To get modems past the 2400-band limit, modems modulated 2400-band single multiple times a second
    - V Standards
        - Modems query each other to determine fastest transfer rate
            - Standards established by CCITT – V-Standards
                - V.22 – 1200bps – V.32 – 9600bps – V.34 – 28kbps
                - V.22bis – 2400bps – V.32bis – 14,400bps – V.90 – 57,6kbps
                - V.92 – 57.6kbps (current standard)
                - V.42 – error checking, V.42bis – data compression, V.44 – data compression
                - MNP5 – error check and data compression
    - ISDN * Integrated Services Digital Network
        - Two types of channels – bearer channels carry data and voice information via DS0
            - Delta channel – carry setup info and configuration info @ 16kbps
        - Common setup is 2B/ID – Basic Rate Interface (BRI) setup
            - Primary Rate Interface (PRI) = T1 = 23 billion channels
        - Physical connections similar to PSTN
            - Jack → Demarc → ISP
                - 18k feet within central office
        - Configure ISDN phone number and Service Profile ID
    - DSL * Digital Subscriber Line
        - Fully digital, dedicated – same physical devices as PTSN
            - Symmetric DSL (SDSL) – equal upload/download speeds

        - Asymmetric DSL (ADSL) – different upload/download speeds (faster download)
    - DSL Features
        - Data/voice simultaneous transit, same distance restrictions as ISDN (18kft) to central office, which has a DSL Access Multiplexer (DSLAM)
    - Installing DSL
        - Pre-existing telephone lines, requires DSL filter on each POTS line
        - DSL modem → jack → NIC/computer → gateway router (Cat5/6 patch) → switch
        - 1st Gen – Bridged Connection – DSL pluggeddirect into NIC
            - PPPoE then used for stronger control over DSL connection
                - Requires account and password
- Broadband Cable
    - Phenomenal top speed – 5-200Mbps
        - Cable modem, coax cable → headend → cable company
        - Data over cable service interface specification (DOCSIS) – currently v3.1
            - F-coax connection + RJ45
- Satellite
    - One-way – download only, PSTN/dial-up for uploads
    - Two-ways – both upload/download
        - Computer → satellite mod → satellite dish
- Fiber
    - Passive Optical Network – single fiber to neighborhood switch
        - WDM – multiple signals on same fiber

- Which Connection?
    - Availability, bandwidth
- Using Remote Access
    - Use WAN + LAN
        - Dial up to internet, VPN, Remote Terminal, Private Dial-up, Dedicated Connection, VoIP
- Dial-Up Internet
    - Old, rare, cheap – good backup
        - Modem, ISP #, username/password, PPP connection type, IP info (DHCP)
- Private Dial-Up
    - Private network – no internet – requires two systems – one is a remote access server (RAS), the other is the client with a connection tool
        - Window RRAS – authenticate, file, print access dial-up modem
    - Must setup a server in LAN as RAS
- VPNs
- Dedicated Connection
    - Remote connections, server disconnected
        - Still need DHCP + DNS – dedicated between two locations (two locations and T1 line)
            - Dedicated to the internet
                - DSL + cable – PPPoE info ADSL
        - Cable splitting degrades signal logarithmically
            - Limit cable modem splits to no more than one
- Remote Terminal
    - Telnet
    - WinFrame/MetaFrame/XenApp
        - Windows Terminal Services
            - Remote Desktop Protocol, VNC + SSH

        - Remote Desktop Connection
    - VoIP
        - IP network
        - RTP * Real-Time Transport Protocol – majority standard
        - SIP + H.323 – Session Initiation Protocol – run on top of RTP
            - (SIP) port TCP 5060, 5061; H.323 port 1720
    - Skype * Peer-to-Peer – Incompatible with other VoIPs
        - Real-Time Streaming Protocol – on top of RTP for video streaming
- WAN Troubleshooting Scenarios
    - Loss of Internet Connectivity
        - Proper configuration
            - Tools such as ping, ipconfig, netstat, nslookup
    - Interface Errors
        - Local Ethernet Interface/LAN Interfaces
            - Make sure all LAN connections are goo
            - Modem Checks
                - LAN → WAN
                    - Two interfaces
    - DNS Issues
        - Choosing DNS server to use
            - Sometimes DNS servers fail or use helpers
                - Use a fast public DNS IP address (like Google) and load onto secondary DNS server as backup
    - Interference
        - CPE can cause problems (EMI), shielded cables vs unshielded
        - Modem can fail too, splitters/splices
        - Every form of remote connection has very clear fault tolerances
            - Verify during installation or system changes

Chapter 14 – Wireless Networking

- Uses RF waves to enable communication
    - unbound media
- share same OSI layers (except first two) and same protocols
    - type of media and protocols for transmitting/receiving data
- IEEE 802.11 Wireless Standard – WiFi
- WiFi Standards
    - 1990s – 802.11 standard
    - 802.11
        - defines how to communicate and how to secure
        - 802.11 – 1997 – defined certain features
            - wireless network cards
            - special configuration software
            - capability to run in multiple styles of networks
            - how transmissions work
    - Hardware
        - Wireless Ethernet NICs
            - take data from upper OSI layers
            - encapsulate into frames – not the same as 802.3

        - send out in streams and receive frames as radio waves
    - Wireless PCIe Ethernet Cards
        - or wireless USB network adapters (USB NICs)
            - have "placeable" benefit for strongest signal
    - Wireless Access Point (WAP)
        - Interconnect wireless network nodes with wired networks
        - operates like a hub, works at OSI Layer 1
        - often combined with built-in switch and/or router
- Software
    - every wireless network adapter needs a device driver and a configuration utility
    - configuration utility determines
        - link state connection
        - signal strength
        - mode, security encryption, power saving
- Wireless Networking Modes
    - uncommon ad hoc mode
        - direct connection
    - common infrastructure mode
        - uses WAP
    - AD HOC MODE
        - peer-to-peer, decentralized FFA
        - mesh topo, forming on Independent Basic Service Set (IBSS)
            - basic unit or organization
            - good for < 12 computers
    - INFRASTRUCTURE MODE
        - one or more WAPs, star topo
        - WLAN, connects wireless to wired
            - single WAP → Basic Service Set (BSS)
            - more WAPs → Extended Service Set (ESS)
- Range
    - theoretical maximum
        - practical is roughly 50% of listed
- BSSID, SSID, ESSID
    - Basic Service Set ID – basic infrastructure mode
        - one WAP and one or more wireless clients
        - same as MAC
            - Ad hocs use random 48bit string that functions like a MAC, going in every frame
    - Service Set ID – applied to BSS/IBSS to help connection occur
        - network name – 32bit ID in header of frames
        - Devices must share same SSID, found via SSID broadcast
    - Extended Service Set ID – SSID applied to ESS
        - single broadcast domain via connection to central switch (one with the strongest signal)
        - connections change via roaming
- Broadcasting Frequency
    - interference, avoided with specific frequencies
    - originally 2.4 or 5.0 GHz
- Broadcasting Methods

        - original 802.11 – spread spectrum – small chunks over different frequencies within a range
            - three different spread-spectrums
                - Direct-Sequence Spread Spectrum (DSSS)
                    - uses all frequencies, more bandwidth, greater throughput but sensitive to interference
                - Frequency-Hoping Spread Spectrum (FHSS)
                    - one frequency at a time
                - Orthogonal Frequency Division Multiplexing (OFDM)
    - Channels
        - portion of available spectrums
            - 2.4 Ghz → 14 channels, 20 Mhz bandwidth
                - 1, 6, 11 are non overlapping – default choices
            - 5.0 Ghz → 40 channels
    - CSMA/CA
        - wired networks use CSMA/CD
        - wireless networks use CSMA/CA
            - both access network media without frame collision
        - Modern wired networks use full-duplex, no need for CSMA, wireless does not have benefit of full-duplex
            - CD uses back-off between collided nodes to randomly pick when to resend attempted packet transmission
        - wireless devices cannot detect collisions
            - radio is half-duplex
            - cant hear C source when A and B sources are talking
        - CA takes steps to avoid collisions preemptively
            - 802.11 standard – two methods for CA
                - Distributed Coordination Function (DCF)
                - Point Coordination Function (PCF)
            - Only DCF currently implemented
                - Back-off function + IFG
                - receiver nodes must reply with ACK per frame
                    - ACK tell other nodes to wait before attempting
        - wireless networking has overhead and latency, causing stalls and timeouts
            - throughput reduced, only "goodput" carries data
        - 802.11 | 2.4 | DSSS | 2Mbps | ~300' | 802.11 compatible
        - 802.11b | 2.4 | DSSS | 11Mbps | ~300' | not compatible
        - 802.11a | 5.0 | OFDM | 54Mbps | ~150' | not compatible
        - 802.11g | 2.4 | OFDM | 54Mbps | ~300' | 802.11b compatible
        - 802.11n | 2.4 | OFDM (QAM) | 100Mbps | ~300' | 802.11b/g compatible
        - 802.11ac | 5.0 | OFDM (QAM) | 1Gbps| ~300' | 802.11a compatible
- WPS
    - WiFi Protected Setup
        - push notification or PIN
            - easily hacked
- WiFi Security
        - no default security
        - 802.11 uses MAC address filtering, authentication, and data encryption
    - MAC Address Filtering
        - accepted user lists (like ACLs) – white or blacklist
            - can be countered with Spoofing

- Wireless Authentication
  - 802.11i uses IEEE 802.1x → RADIUS + EAP
    - client supplicant → WAP Network Access Server → RADIUS → [Accept-Accept Authenticator] → user
  - PPP protects supplicant-NAS connection
  - IPsec protects NAS-RADIUS connection
    - both EAP encrypted
- EAP
    - PPP wrapper that EAP-compliant applications use to accept different forms of authentication, to allow two devices to authenticate
  - EAP-PSK – most popular, pre-shared key, uses AES
  - EAP-TLS – defines RADIUS use and mutual authentication
    - client-side certificate request
    - most secure
  - EAP-TTLS
    - Tunnel TLS
    - single server-side certificate
    - common for more secure networks
  - EAP-MS-CHAPv2
    - Protected EAP (PEAP)
    - password function
    - most common implementation
  - EAP-MD5
    - weak, least common
  - LEAP
    - Lightweight EAP
    - Cisco Specific
    - MS-CHAP authentication with RADIUS
  - EAP-FAST
    - Flexible Auth via Secure Tunneling
    - Cisco replacement for LEAP
- 802.1x
  - wired form of EAP
    - PPP replaced with Ethernet Frame
  - port-based authentication network access control mechanism for networks
    - devices go through full AAA process
  - combines RADIUS AAA with EAP
    - only wireless broadly adopted 802.1x
- Data Encryption
  - Data Encryption using WEP
    - 64 or 128 bit encryption
    - subject to WEP attacks
      - IV leaves key short
      - key is both static and shared
    - no user authentication
  - Data Encryption using WPA
    - 802.11i intermediate fix
    - dynamic encryption key generation (per user/per session)
      - uses TKIP-RC4
        - hackable

        - Data Encryption using WPA2
            - IEEE 802.11i
                - TKIP-RC4 replaced with CCMP-AES
                    - counter mode cipher blocking chaining message authentication code protocol)
                - common to use PSK
                    - no authentication unless using Enterprise version
                - use long complex passphrases for protection
    - Enterprise Wireless
            - robust construction, centralized management, VLAN pooling, Power over Ethernet, Personal into Enterprise
        - Robust Device Construction
            - better materials
            - more configurable
            - upgradeable
        - Enterprise Wireless Administration
            - wireless controllers
            - Direct WAP – thick client
            - WAP through Wireless Controller – thin client
        - Lightweight Access Point Protocol (LWAPP) – for interoperability
    - VLAN Pooling
        - pool of VLANs for single SSID and assign clients randomly
    - Power over Ethernet
        - IEEE 802.3af
            - power over ethernet – 14.4 watts
                - PoE+ - 25.5 watts
- Implementing WiFi
        - site survey
        - install Aps
        - configure Aps and Clients
        - test network
    - Performing a Site Survey
        - floor plan
        - site survey tool
            - NETSCOUT AirMagnet Survey Pro
            - discover other wireless networks
        - What If Wireless is Already There?
            - set SSID and channel to avoid overlap
                - use wireless analyzer
                - Acrylic WiFi
            - WAPs use algorithms to configure to least-congested channels
                - issue with high density environments
                - heat map
        - Interference Sources
            - objects, structures, appliances
                - require 802.11n/802.11ac with 3-4 antennas or multiple WAPs
    - Installing the Client
        - wireless NIC for desktops, most mobile devices have wireless clients
            - PCIe or USB
- Setting up an Ad Hoc Network
        - rare but still possible

- Configuring NICs requires four things after setting NIC
    - SSID – same network to Ad Hoc
    - IP Addresses – no two devices can have same
    - Channel
    - Sharing
- Ensure File and Printer Sharing running on all nodes

- Setting Up an Infrastructure Network
    - Placing the Aps/Antennas
        - Three Types
            - omnidirectional
            - unidirectional
            - patch
        - Omnidirectional
            - dipole – straight antennas, two radiating in opposite directions
                - good for outdoors or single floor
                - subject to a lot of bleed out
                - can require a signal booster
                - obstacles create deadspots
                - antennas needed to strengthen RF output (measured in dB)
                    - variable sizes
        - Unidirectional
            - use one or more directional antennas that focus signal into a beam
            - unidirectional came in several shapes
                - parabolic – dish
                - yagi – beam, narrow and focused
        - Patch
            - generate half-sphere beam
            - always placed on walls
            - fill room without broadcast to room behind patch
    - Optimal Antenna Placement
        - will vary depending on site survey, space, and security concerns
    - Configuring the AP
        - browser-based setup utility
            - enter local IP and configure WAP
        - Configuring SSID and Beacon
            - make sure it is unique
            - Beacon Traffic is a major portion of wireless traffic
                - broadcasted every 100ms
        - Configuring MAC Address Filtering
            - build a whitelist or blacklist
        - Configuring Encryption
            - generate unique security key
                - WPA2 – both NIC and WAPS
                - bit size and passphrase
        - Configuring Channel and Frequency
            - in environments with overlapping networks
            - 802.11n either 2.4 Ghz or 5.0 Ghz
    - Configuring the Client
        - infrastructure mode – some SSID on all nodes and Aps
- Extending the Network
        - add one or more WAPs to create an Extended Service Set

        - use a wireless bridge
        - wireless range extenders
    - Adding A WAP
        - cable from a switch
    - Wireless Bridges
        - connect two wired networks together or wired and wireless
        - point-to-point – two max
        - point-to-multipoint
- Verifying the Installation
    - move traffic between nodes
- Troubleshooting WiFi
        - cant get on
        - slow connection
        - weird connection
    - No Connection
        - Channel Problems
            - channel overlap
                - stick to 1, 6, 11
            - frequency mismatch
                - correct SSID but different channel
                - set to autochannel selection
            - security type mismatch
                - manually set encryption type is wrong
                - wrong passphrase
            - signal/power levels
                - distance limitations and signal attenuation
                - get closer, avoid deadspots, increase WAP power, better antenna, upgrade to newer 802.11ac
        - Slow Connection
            - Overworked WAPs
                - device saturation
                    - overcapacity
                - jitter
                    - latency
                - bandwidth saturation
            - physical issues
                - absorption
                - reflection
                - refraction
            - dealing with physical issues
                - multipath
            - captive portal
                - can slow due to it being an extra step in the login process
                    - web browser requiring accepting EULA
            - interference
                - RF interference
                    - non-wifi and wifi sources
                - shutdown or remove devices
                    - scan for with RF scanner
                    - signal-to-noise ration
        - Weird Connection

- Open Networks
    - non-encrypted
        - avoid logging in with SSID used in another location
        - provide security when you do
    - wrong SSID
        - Rogue Aps
        - misclicks
    - Untested Updates/Incompatabilities
        - research and test updates
        - determine backwards compatibility
    - Rogue Aps
        - evil twin attacks
    - War Driving and War Chalking
        - marking physical addresses with open networks with chalk
            - rare

Chapter 15 – Virtualization and Cloud Computing

- Meet the Hypervisor
        - programming that helps handle vritualization
        - handle same input/output OS requests of hardware normally
            - virtualized BIOS and System Setup
        - host allocates actual RAM and CPU power
    - Emulation versus Virtualization
        - Virtualization takes hardware of host system
            - can only act exactly like host system
        - Emulation connects commands to/from host machine into a different platform
    - Desktop Virtualization
        - New → OS Type → Config RAM, Memory → OSD/ISO file → Virtual Desktop
    - Virtualization Benefits
        - power saving, hardware, consolidation, system recovery, system duplication, research potential
    - Virtualization in Modern Networks
        - servers, especially web/email are usually virtualized
        - bare-metal hypervisors (Type 1) vs software-based (Type 2)
            - VMware ESX, can be kept in thumb drives that loads basic interface
    - Hypervisors
        - bare-metal → VMware ESX, Microsoft Hyper-V, Citrix XenServer (open source, popular with cloud)
            - also Linux KVM
    - Administering a Hypervisor
        - ESX, Hyper-V not administered directly at the box
            - VMware vSphere Client
            - Microsoft Hyper-V Manager
- ScalingVirtualization
    - Data Storage
        - SAN
            - Storage Area Network
                - takes a pool of hard disks and present them over the network as any number of logical disks

        - allows read/write blocks over network
        - various mapping options, and avoid performance cost of implementing a file system
    - uses Fiber Channel, Internet Smaller Computer System Interface, and InfiniBand infrastructure
        - Fiber Channel – high-performance storage specific to itself
        - iSCI – uses TCP/IP, enabling communications across existing networks
            - performance costs, due partly to frame processing
            - use of jumbo frames to ease number of headers
        - InfiniBand – unique NICs and cabling, provide interconnection between storage array and servers
            - aggregated links, commonly four or eight connections
- NAS
    - dedicated file server with own file system, need to perform file-sharing systems work for all clients
    - simple and low cost

- Virtual Networking
    - network admins create virtual version of network devices
  - Virtual Switches
    - oldest way to give VMs valid IPs is to bridge NIC – Layer 2 of OSI Model
        - virtual NICs are same as physical NICs – IP address, subnet masks, etc
    - bridging NICs use a virtual switch – software that does the same as a physical L2 switch
        - VMs and host NIC are all connected to virtual switch
        - still need virtual routers and firewalls
  - Distributed Switches
    - virtual ones use a web interface for configuration
    - growth is exponential so careful configuration is necessary
    - centralized installation, configuration, and handling of every switch is distributed switching
        - VLAN assignment, trunking
  - Virtual Routers and Firewalls
    - allow dynamic reconfiguration on networks
- Software Defined Networking
    - traditional hardware routers/switches are a control and data plane pair
        - control makes decisions on how to move traffic and speak routing protocols such as OSPF and BGP
    - Software Defined Networking – cuts out control plane and uses network controller to dictate how physical/virtual network components move traffic through a network
        - data plane must be designed to take input from network controller
        - network controller is programmable
- To the Cloud
    - VMs are files, which can be placed and run in the cloud
- The Service-Layer Cake
  - servers and networks are used through layers of software
    - local/cloud software divide is minimized
    - IaaS, PaaS, SaaS
  - Cloud Delivery Models
    - Public
    - Private
    - Community

        - Hybrid

Chapter 16 – Mobile Networking

- Mobile Network Technologies
        - 802.11 Wifi and Z-Wave
    - Cellular WAN
        - generation based
        - GSM and EDGE, CDMA, HSPA+, LTE
    - GSM and Edge
        - Global System for Mobile Communications
            - first group – 2G
            - time division multiplexing (multiple access) TDMA
        - TDMA enabled multiple uses to share same channel
        - GSM introduces subscriber identity module (SIM)
        - latest version Enhanced Data routers for GSIM Evolution (EDGE)
    - CDMA
        - Code Division Multiple Access
        - Spread Spectrum Form of transmission
            - incompatible with TDMA
            - frequencies changed by user
            - lacked SIM
    - HSPA+
        - International Telecommunication Union (ITU) IMT-2000
            - support for MMS
        - Evolved High Speed Packet Access (HSPA+) was final 3G standard ~ 10 Mbps
    - LTE
        - Long Term Evolution
            - 4G ~ 300Mbps download, 75Mbps upload
            - SIM card
    - 802.11
        - hotspot configuration
        - general configuration options
            - open networks, saved wireless profiles, spoofed AP risk
    - Bluetooth
        - PAN
            - more secure over time
                - require manual setting to discovery/discoverable (timed)
                - PIN use
            - early versions did not use one or both
                - Bluejacking victimization
                - Bluesnarfing
            - Patching secure up to v4.0
            - Be aware of BlueBorne vulnerability
- Less Common Mobile Network Technologies
    - NFC
        - low speed, short range
        - small monetary transactions
            - NFC tag and reader

        - power derived from reader, not tag
    - RFID
        - many different standards between 120khz to 10Ghz
        - broader applications
            - common features
                - close proximity - >1m
                - security – weak or none
                - labels – common location
        - easier to read
    - Infrared
        - androids have IP blasters
            - single commands with no risk to phone
    - ANT
        - Adaptive Network Technology
            - low speed and power
            - passive device and active reader
        - does not require a lot of resources and used for niche devices
            - AES encrypted
    - Z-Wave and Zigbce
        - home automation tech
        - Z-Wave is closed source, Zigbie is Open Source
- Deployment Models
    - BYOD
    - COBO – corporate owned business only
    - COPE – corporate owned personal enabled
    - CYOD – choose your own device
- On-boarding and Off-boarding
    - on-boarding requires previously unfamiliar device to go through a series of checks and scans
    - off-boarding requires inspection that detects proprietary applications and any sensitive data and removes them
- Scenarios
    - Geofencing
    - Locating and Disabling Lost Mobile Devices
    - Hardening IoT Devices
- Locating and Disabling Lost Mobile Devices
    - report loss/breach
    - locate/recover device
    - remote wipe
    - define encryption to mark keys lost/stolen
    - disable all associated accounts
    - reissue new device and configure accordingly
- Hardening IoT Devices
    - patch maintenance
    - physical security
    - internal security

Chapter 17 – Building a Real-World Network

- Designing a Basic Network
    - Seven Key Factors to Consider

        - list of requirements
        - device types/requirements
        - environmental limitations
        - equipment limitations
        - compatibility requirements
        - wired/wireless considerations
        - security considerations
    - Also consider cost and budget
- Define Network Needs
    - workstations, servers, internal cabling, intermediate distribution frames, solid connectivity
    - operating systems, network protocols, communication and industrial controls
- Documentation
    - support configuration management
    - Network Diagrams
        - physical and logical components
    - Asset Management
        - versions, upgrade paths, software
    - Licensing Restrictions
    - Inventory Management
    - IP Address Utilization
    - Vendor Documentation
    - Standard Operating Procedures
- Network Design
    - Workstations
        - OS's
    - Servers
        - Network Authentication and Management
        - Accounting and File Management
        - Intranet and Document Sharing
        - Development Environments and Software Repositories
        - NAS devices using CIFS, NFS, FTP
    - Equipment Room
        - centralized core
        - detailed rack diagrams
        - power management, power conversion/redundancy
            - dual power supplies
            - redundant circuits
            - battery backups, UPS's
    - Peripherals
- Compatibility Issues
        - Cat types within cabling
        - isolate legacy systems
            - implemented with VLANs
- Internal Connections
    - Structured Cabling
        - IDFs and 10GBaseT between buildings
        - Cat6a within buildings
    - Wireless
        - 802.11ac units controlled by unified wireless controller
    - VLANS
        - by department and/or network services

    - Set up Network IP Address Scheme
        - document and male copies
- External Connections
    - ISP, primary and fallback secondary
    - metro ethernet line
    - Main Distribution Frame (MDF)
- Unified Communication
    - VoIP
        - originally required several RJ45s for separate VoIP gateways that interface with PBX
            - classic Computer Telephony Integration (CTI)_
        - VoIP uses Real-Time Transport Protocol (RTP) on TCP ports 5004 and 5005 and Session initiation Protocol (SIP) on TCP ports 5060/5061
            - separation was an issue, leading to creation of Unified Communications
    - Unified Communication Features
        - provides presence information, video conferencing/real-time video, fax, messaging, collaboration tools, workflow
        - Real-Time Services (RTS's)
    - UC Network Components
        - UC Devices – VoIP telephone
        - UC Servers – dedicated box
        - UC Gateways – edge devices
    - UC Protocols
        - SIP and RTP, H.323 (TCP 1720) or MGCP (TCP2427/2727)
    - SIP Trunking
        - connect PBX systems from multiple locations seamlessly over Internet via virtual connections called SIP Trunks
- VTC and Medianets
        - medianets help to eliminate or reduce connection issues of VoIP
            - network of far-flung routers and servers that provide QoS and bandwidth for VTC
    - ISDN vs IP/SIP
        - Integrated Services Digital Network
            - 128kbps bandwidth
            - H.320 + compression
    - QoS and Medianets
        - differentiated services – architecture that makes QoS work
            - DSCP
                - Differentiated Services Code Point – first 6 bits with 8 classes of service
            - ECN
                - Explicit Congestion Notification – 2 bits
                    - 00 – not QoS aware
                    - 01/10 – QoS aware, not congested
                    - 11 – QoS aware, congested
            - both go into IP header
                - assignable to ports as priority queues
- ICS
        - things to monitor/control
        - specialized, interconnected
    - DCS
        - ICS has three basic components
            - Input/Output Functions – sensors/actuators
            - Controller

        - Operator Interface
    - Distributed Control System
        - local controllers connected centralized ICS server
        - interaction with human machine interface (HMI)
- PLC
    - Programmable Logic Controller
- SCADA
    - Supervisory Control and Data Acquisition
        - large scale, distributed processes
        - remote connections, intermittent
    - Remote Terminal Unit
        - controllers replaced by TRUs
        - autonomous capability and long distance communications
        - risk of interception
- Network Segmentation
    - security, reduce congestion, limit network problems
    - Using OSI
        - L1 – Physical – air gap
        - L2 – Data Link – VLANs, separate Broadcast Nets
        - L3 – Network – different subnets, block IPs
        - L4+ - VPNs, separate SSIDs, domains, virtualization
- Segmentation and Industrial Control System
    - ICS's are closed networks
        - public wireless can be used to connect to RTUs
        - SCADA servers connect to internet to provide intranet
    - Defend with VPNs

Chapter 18 – Managing Risk

- Risk Management
        - probability determination
    - Security Policies
        - defines how an organization will protect IT infrastructure
        - internal/external
    - Acceptable Use Policy
        - Ownership
        - Network Access
        - Privacy/Consent to Monitoring
        - Illegal Use
    - Network Access Policies
            - who can access, how they can access it, and what can be accessed
        - Privileged User Agreement Policy
            - aware of access without escalating a permission request
            - role separation
        - Password Policy
            - strength, rotation frequency
        - Data Loss Prevention Policy
            - data access levels
            - backups, redundancy

        - Remote Access Policy
            - VPNs
            - open portals
    - Externally Imposed Policies
        - Government and Regulation
            - international export controls, licensing restrictions
            - HIPAA
        - Adherence to Policies
            - difficult, requiring review and update regularly
- Change Management
    - change infrastructure in organized, safe way
    - change management team
        - investigate, test, authorize
    - Strategic-Level Changes
        - management-level, major in scope
    - Infrastructure-Level Changes
        - Department-level
  - Initiating the Change
    - Change Requests
        - type of change
        - configuration procedures
        - rollback process
        - potential impact
        - notification
  - Dealing with the Change Management Team
    - approval process
        - review, funding, approval
  - Making the Change Happen
    - purchasing, training
    - maintenance window
        - authorized downtime
    - notification of change
  - Documenting the Change
    - change management documentation
        - network configurations, additions
        - physical location changes
  - Patching and Updates
    - similar to change management and regular maintenance
    - every piece of software and firmware
    - OS updates
        - network server-based patching
            - test then distribute
        - device drivers
        - features and changes/updates
    - major vs minor updates
        - vulnerability patching with immediate application
        - minor patches implemented in a cycle
    - Firmware updates
        - manual process, but infrequent
  - How to Patch

        - Research
        - Test
        - Configuration Backup
            - downgrade/rollback
    - Training
        - end use awareness and training, ensure understanding of
            - security policies
            - passwords
            - system and workplace security
            - social engineering
            - malware
    - Points of Failure
        - avoid single points
        - ID critical assets and critical nodes
    - Critical Assets
        - typically senior management process
    - Critical Nodes
        - IT equipment
            - file server, web server, peripherals, edge routers
    - High Availability
        - work without interruption/downtime via failover
            - detect when a muster has failed and subsystems take over
            - using virtual IP, clusters accepting traffic from a single common IP
        - Redundant Backup
            - virtual open Router redundancy Protocol (VRRP)
            - Cisco Proprietary Hot Standby Router Protocol (HSRP)
            - multiple routers ganged together into a single virtual router with single virtual IP address
                - used a default gateway
                - doesn't load balance
    - Redundancy
        - Alternate Business Practices
        - Fault Tolerance
            - clustering
            - load balancing
- Standard Business Documents
    - Service Level Agreement (SLA)
        - Definition of service provided
        - equipment
        - technical support
    - Memorandum of Understanding
        - parties commit to perform for each other and a time frame for MOU
        - define costs, contacts, logistics, etc. for occasional business partnership
    - Multi-source Agreement
        - defines interoperability of components between manufacturers
    - Statement of Work
        - legal contract between vendor and customer
        - services/products, time frames, milestones
    - Nondisclosure Agreements
- Security Preparedness
    - Vulnerability Scanning

        - Microsoft Baseline Security Analyzer
        - Nmap
            - Zenmap GUI
        - Nessus
        - OpenVAS
    - Vulnerability Management
    - Penetration Testing
        - Aircrack-ng
        - Metasploit
            - Armitage GUI
        - Kali Linux
- Contingency Planning
    - Incident Response
        - first responders
            - address, ignore, escalate, resolve
            - evaluate scope and course
            - restore and prevent
    - Disaster Recovery
        - recovery of primary infrastructure
            - snapshots, backups, archives
        - Traditional Backup Techniques
            - full backup
            - incremental backup
            - differential backup
    - Backup Plan Assessment
        - determine data loss and restoration potential
        - Recovery Point Potential Objective
        - Recovery Time Objective
        - Mean Time Between Failures (MTBF)
        - Mean Time To Failure (MTTF)
        - Mean Time To Recovery (MTTR)
    - Business Continuity
        - Business Continuity Planning
            - Backup Sites
                - Cold, Warm, Hot
        - Succession Planning
- Forensics
    - Certifications
        - Certified Forensic Computer Examiner – IACIS
        - Certified Computer Examiner – ISFCE
        - Certified Forensic Analyst – GIAC
    - First Responder
        - support first responder
        - capture hard drive and RAM
        - secure area
            - document scene – copious notes
                - collect evidence – Chain of Custody
                    - Interface with Authorities
                - legal hold and electronic discovery
- Safety
    - Electrical Safety

        - danger of electricity
        - grounding
        - static
            - ESD
    - Physical/Installation Safety
        - proper attire
        - cable clutter avoidance
        - lifting/moving equipment
    - Rack Installation and Maintenance
        - Power
            - proper power source
                - 20amp dedicated circuit minimum
                - each rack should have UPS
                    - single power converter per rack
        - Mounting
            - secure with screws, secure racks themselves
            - enclosed, open frame, and goal post
            - tool safety
        - Environment
            - environmental controls
            - optimized airflow
                - HVAC
            - fire suppression
            - MSDS
        - Emergency Procedures
            - building layout, fire escape plan, safety and emergency exits, fail open/fail closed, emergency alert system

---

Chapter 19 – Protecting Your Network

- Network Threats
    - Spoofing
        - spoof data for impersonation
            - Src MAC/IP addresses
            - emails, web addresses, usernames
        - DNS cache poisoning
            - counter with DNSSEC
    - Packet/Protocol Abuse
        - NTP for example
            - use of peers for accurate time keeping
            - query servers with htpdc monlist
                - query can be used for DoS
            - malformed packets via Scapy with incorrect info can break servers
    - Zero-Days
    - ARP Cache Poisoning
        - falsification of device info to disrupt network traffic
        - allows for MitM attacks
    - Dynamic ARP Inspection and DHCP Snooping
        - DAI tracks good ARP info, blocking bad/unknown ARP commands

        - DHCP snoops will block unknown MAC devices
        - enhanced port protection
    - Denial of Service
        - render incoming request processing as unavailable
            - amplification through monlist commands
            - botnet use
        - reflective DDoS attacks
            - traffic spiking
    - Deauthentication Attack
        - targets 802.11 WiFi, kicking clients off network WAP
            - rogue WAP grabs connection
    - Man in the Middle Attack
        - covert traffic interception
        - rogue WAPs or ARP cache poisoning
    - Session Hijacking
        - grabs authentication information
    - Brute Forcing
- Physical/Local Access
    - Compromised System
        - counter with fault tolerance and redundant systems
    - Insider Threats
        - Trusted/Untrusted Users
            - unsecured access to private resources
            - compromise of trusted user accounts
            - forgotten temporary upgrades of untrusted user privileges
            - default device credentials
                - remove guest accounts and change default logins
        - Malicious Users
            - packet sniffing
            - network/port mapping
            - banner grabbing
            - MAC OUI number collection and research
- VLAN Hopping
    - Administrative Access Control
        - Access Control Lists
            - careful control of admin accounts
- Malware
    - cryptomalware/ransomware
    - viruses
    - worms
    - macros
        - application macro exploits
    - logic bombs
    - trojans
    - rootkits
    - adware/spyware
- Social Engineering
    - Phishing
    - Physical Intrusion
- Common Vulnerabilities
    - Unnecessary Running Servies

        - disable them to limit TCP/UDP open ports
            - be wary of blocked ports
    - Unpatched/Legacy Systems
        - update systems as needed with proper process
        - isolate legacy systems
        - system life cycle policies address asset disposal
    - Unencrypted Channels
        - Telnet vs SSH
        - using HTTP vs HTTPS
        - Insecure remote desktops like VNC
        - using insecure protocols in the clear
    - Cleartext Credentials
        - FTP, Telnet, POP3 credentials are sent in cleartext
        - poor configurations of applications
            - password authentication protocol (cleartext)
    - RF Emanation
        - RF spill as they penetrate physical mediums
        - NSA TEMPEST to counter
            - rarely need
- Hardening Your Networks
    - Physical Security
        - prevention and control to IT resources to appropriate personnel
        - track actions of authorized personnel
        - locks, key control, guards, mantraps, badges
        - tamper detection, biometrics, multifactor
    - Monitoring
        - video surveillance, CCTV, IP cameras, motion activated
    - Network Security
        - Access Control
        - Controlling User Accounts
            - principle of least privilege
            - improper/unauthorized access
        - File Permissions/Groups
            - effective permissions but be wary of conflicting permissions
            - avoid default accounts
            - inheritance between folders and subfolders
        - Edge
            - devices that have been optimized to perform a given task
                - installed closer to a client than the core and keeps local copies of necessary databases
    - Posture Assessment
        - Network Access Control (NAC)
            - verify node meets certain criteria before joining network
            - Cisco Network Admission Control
        - Posture Assessment
            - query network devices to ensure meet minimum security standards
            - AV, QoS, OS version/type, real/virtual machine, keylogger presence
    - Persistent and Non-Persistent Agents
        - Agents answer posture assessment queries by scanning the computer to create an inventory of config info, resources, assets
            - persistent agents, once installed, stay installed and run upon each boot

                - non-persistent agents are downloaded via portal/network and released from memory once client leaves
            - Cisco Access Control Server decides to accept/deny a node
                - ACS directs edge device to allow a connection or deny
            - As there are devices outside of workstations, 802.1z supplicants in the form of either an agent or client
                - agent-less client assessment
    - Guest Networks and Quarantine Networks
        - denied or devices that fail assessment are sent to quarantine or guest networks
- Device Hardening
    - changing default credentials, avoiding common password, keep network devices up to date, disable unnecessary services, using secure protocols, disabling unused ports
- Host Security
- Malware Prevent and Recovery
    - Malware Prevention
        - frequency of symptoms
        - detection of symptoms
    - Symptoms
        - sluggishness, crashes, increased network outflow, “top talkers”
    - Dealing with Malware
        - AV, training and awareness, patch management, remediation
        - AV, host, network, or cloud based
            - signature based
- Firewalls
    - software (host based) or hard (network based)
    - Advanced Firewall Techniques and Features
        - stateful inspection
            - packet part of an existing connection
        - stateless inspection
            - all packets are inspected regardless
        - Application/Context aware firewalls are at L7 of OSI Model and filter traffic based on traffic source
            - address port hopping applications
    - Next-Generation Firewalls (NGFW)
        - operates at multiple layers of OSI
            - L3 – IP filter
            - L5 – port filter
            - L7 – application filter
    - Unified Threat Management
        - firewall and IPS and load balancing
- Implementing and Configuring Firewalls
    - place between internet and internal network
        - performance critical from connection speed
- Restricting Access via ACLs
        - allow/deny traffic
        - implicit deny
        - assign ACL to interface
            - apply to each direction
        - web content/IP filtering
    - DMZ and Firewall Placement

        - network segment carved out by firewall routers to provide a special place on the network for any servers that need to be publicly accessible from the Internet
        - network segmentation
            - create perimeter network with different levels of trust
    - Honeypots and Honeynets
- Troubleshooting Firewalls
    - misconfigured firewalls, variance in definitions, incorrect ACL settings, misconfigured applications

---

Chapter 20 – Network Monitoring

- SNMP
    - de facto management protocol for TCP/IP
    - SNMP Manager – requests/processes info from devices
        - managed devices – run agents
            - Management Information Bases – categorizes data that can be queried
    - SNMP Manager runs specialized software called Network Management Stations
        - extensible protocol
    - Once established, SNMP network runs regular queries to managed devices and gather in usable format
        - eight core functions
        - Protocol Data Unit
            - GET – query an agent
            - Response – agent reply
            - Set – NMS tells agent to make changes
            - Trap – agent solicits info from NMS
        - can also automate tasks
            - snmpwalk utility
            - eventmanagement capability
    - SNMPv1-v3
        - UDP ports 161/162
        - NMS listens on port 162, agent lists on port 161
        - unsecure unless with TLS
            - ports 10162/10161
- Monitoring Tools
    - packet sniffers
    - protocol analyzers
    - interface monitors
        - measure various metrics
            - bandwidth/throughput
            - utilization
            - packet drops
            - error rate
            - discards
            - interface resets
        - Cisco Network Assistant
    - performance monitors
        - tied to a particular OS or app
        - Windows Performance Monitor (PerfMon)

        - syslog (mac, linux)
    - logs
    - baselines
    - Log Management
        - ensure log security, and maintain logs
            - control access, ensure safe/secure storage
                - cyclical storage
    - Network Operations Center
        - SNMP with Graphing program or alerts via Nagios Network Analyzer
            - look for top talkers and bottlenecks
- SIEM
    - monitor and manage networks
        - SEM – security event monitoring
        - SIM – security information management
    - file integrity monitoring (FIM) checks
        - attributes and file size
        - config values
        - content
        - credentials
        - hash values
        - privileges and security settings
    - detect changes to indicate possible compromise

Chapter 21 – Network Troubleshooting

- Troubleshooting Tools
    - Hardware Tools
        - Cable Testers, TDRs, OTDRs
            - cabling issues typically crop up during installation or change
                - lacking continuity, shorts, wire map problem, crosstalk, noise pickups, impedence, mismatch, echo
            - testers detect continuity
            - TDRs/OTDRs locate cable breaks (copper and fiber respectively)
        - Certifiers
            - handle rated capacity
            - detect crosstalk, attenuation, interference, impedance, mismatch
            - needs loopback adapter
        - Light Meter
            - measure light loss
        - Voltage Quality Recorder/Temperature Monitor
            - heat/power issues affect connectivity
            - HVAC issues
        - Cable Strippers/Snips
            - make UTP cables
            - need crimper as well
            - punchdown tool
        - Multimeter
            - test AC/DC voltage, resistance, continuity
        - Tone Probes and Tone Generators

                - help locate particular cables
                - used together
            - Punchdown Tools
                - UTP wires into 66 and 110 blocks
    - Software Tools
                - built in and third party
            - tracerouter/tracert
                - detect router path between two points
                - windows sends ICMP, Linux sends UDP or ICMP
            - ipconfig/ifconfig/ip
            - arp
                - view/change arp table
            - ping, pathping, arping
                - try arping if ping is blocked
                - pathping combins ping and traceroute
            - nslookup/dig
            - mtr
            - route
                - display and edit local system routing table
                - shows routing table with route print or netstat -r
            - netstat and ss
                - current state of all the running IP processes on a system
            - Packet Sniffer/Protocol Analyzer
                - wireshark, tcpdump
            - Port Scanners
                - Nmap, Angry IP Scanner
            - Throughput Testers
                - measure data flow on network
                - online speed-test sites
            - Looking Glass Sites
                - allow for testing of connectivity outside of local environment
- The Troubleshooting Process
            - don’t make problem worse
            - backup at risk data beforehand
    - ID problem
            - gather info, replicate problem, question, ID symptoms, determine changes, separate problems
    - Establish Theory of Probably Cause
            - even the obvious, multiple approaches, topDown/BottomUp, OSI model
    - Test Theory
            - confirm or reformulate
    - Plan Action to Resolve Problem, ID Side Effects
    - Implement/Escalate
    - Verify System Function, Implement Prevention
    - Document
- Resolving Common Network Service Issues
    - Hands On Problems
            - physical and configuration problems
                - power failure/anomalis
                - hardware failure

        - link light statuses
        - transceiver failure
        - EMI/RFI
    - Interface Errors
        - incorrect termination
        - crossover cables, wrong cable type
        - incorrect IP config
            - incorrect default gateway
            - incorrect netmask setting
        - simultaneous wired/wireless connection handling and priority
- LAN Problems
    - duplicate IP addresses, expired IP addresses
    - duplicate MAC addresses
    - exhausted DHCP scope
  - Client Misconfiguration
    - incorrect netmask or gateway issue
  - Server Misconfigurations
    - misconfigured DHCP (host), or DNS (server)
        - unresponsive serve or names not resolving
        - ping by address but not name?
            - DNS issues
  - Adding VLANs
    - interface misconfiguration
    - VLAN mismatch
    - cable placement errors
  - Link Aggregation Errors
    - NIC Teaming
    - LACP and PAgP
        - two or more connections can work together simultaneously
        - devices need two or more interconnected network interfaces configured for LACP
            - active/passive ports (never two passive)
            - teaming misconfiguration
        - multicast must be enabled on all devices
- WAN Problems
    - local machine, LAN switches, WAN routers, distant network switches, distant machines
    - router configuration issues, issues with ISPs, frame sizes, misconfigured multi-layer network appliances, certificate issues, company security policies
  - Router Problems
    - Router Configuration Issues
        - Incorrect ACLs
        - Missing IP routes
    - ISPs/MTDs
        - MTU mismatch, corrected by PMTD but PMTD uses ICMP (blocked by routers)
    - Appliance Problems
        - technician error
        - NAT Interface Misconfiguration
    - Certificate Problems
        - untrusted

        - Company Security Policy
            - blocking policy, fair access policy, utilization limits, throttling policy
    - Beyond Local
        - Escalate
            - Broadcast Storms
            - Switching Loops
            - Proxy ARP
                - VPN concentrator misconfigured proxies can cause DoS
- End to End Connectivity
    - ensure users are connected with essential resources within a smaller network
    - ensure proper ports are open on an application server
    - right people have right permissions to access resources and white list and black list ACLs are setup correctly

---

END
