1.0





# **OSI MODEL - Open Systems Interconnection Reference Model**

* Layer 7 - Application
* Layer 6 - Presentation
* Layer 5 - Session
* Layer 4 - Transport
* Layer 3 - Network
  + The ‘routing’ layer
  + Internet Protocol (IP)
  + Fragments frames to traverse different networks
* Layer 2 - Data Link
  + The basic network ‘language’
    - The foundation of communication.
  + Data Link Control (DLC) protocols
    - MAC address on Ethernet
  + The ‘switching’ layer
* Layer 1 - Physical
  + Signaling, cabling, connectors
  + Not about protocols

**The Ethernet Frame**



# **MAC Address**

* Ethernet Media Access Control address
  + The physical address of a network adapter
  + Unique to a device
* 48 bits / 6 bytes long
  + Displayed in hexadecimal
  + First 3 bytes is the **Organizationally Unique Identifier**
    - (The manufacturer)
  + Last 3 bytes is the **Network Interface Controller-Specific**
    - (The serial number)

i.e. 8c:2d:aa:4b:98:a7

**DUPLEX**

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

|  |  |
| --- | --- |
| **CSMA/CD**   * Referenced on older Half-Duplex networks/systems   + Not commonly used anymore since we have Full-Duplex systems. * CS - Carrier Sense   + Is there a carrier>   + Is there a signal available that we can use to send some data? * MA - Multiple Access   + More than one device on the network * CD - Collision Detect   + Collision - Two stations talking at once   + Identify when data gets garbled * **CSMA/CD operation**   + Listen for an opening     - Dont transmit if the network is already busy   + Send a frame of data     - You send data whenever you can     - Theres no queue or prioritization   + If a collision occurs     - Transmit a jam signal to let everyone know a collision has occured     - Wait a random amount of time     - Retry the transmission |  |

|  |  |
| --- | --- |
| **CSMA/CA**   * CA - COLLISION AVOIDANCE   + Common on wireless networks * Collision detection isn’t possible   + A sending station can’t ‘hear’ other stations * Use RTS/CTS   + Im ready to send.   + Your clear to send. * Solves the ‘hidden node’ problem   + Station A can hear the access point   + Station B can hear the access point   + Station A can’t hear station B |  |

|  |  |
| --- | --- |
| **1.3 NETWORK SWITCHING**  The Switch   * Forward or drop frames   + Based on the destination MAC address * Gather a constantly updating list of MAC addresses   + Builds the list on the source MAC address of incoming traffic * Maintain a loop-free environment   + Using **Spanning Tree Protocol (STP)**   Learning the MACs   * Switches examine incoming traffic   + Makes a note of the source MAC address * Adds unknown MAC addresses to the MAC address table   + Sets the output interface to the received interface   Flooding for unknown MACs   * The switch doesn’t always have a MAC address in the table * When in doubt, send the frame to everyone   Address Resolution Protocol   * Determine a MAC address based on an IP address   + You need the hardware address to communicate |  |

|  |  |
| --- | --- |
| **Collision Domains**   * A historical footnote   + Its difficult to find a collision these days   + The word ‘collision’ is misleading * The network was one big segment   + Everyone heard everyone else’s signals   + One big conference call * Only one station can ’talk’ at a time   + Is the like clear? ok, i can talk     - Carrier Sense Multiple Access (CSMA) * When two people spoke at the same time, there was a collision   + Collision Detection CD   + Send the jam signal | **Broadcast Domains**   * Spread the Word!   + Everyone must know     - ARP requests     - Operating system notifications     - Some dynamic routing protocols * How far can a broadcast go?   + Passed by a switch/bridge   + Stops at the router * This can be important   + More devices, more broadcasts |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Unicast**   * One station sending information to another station * Send information between two systems * Web surfing, file transfers * Does not scale optimally for real-time streaming data | **Broadcast**   * Send information to everyone at once * One packet, received by everyone * Limited scope   + The broadcast domain * Routing updates, ARP requests * Not used in IPv6   + Focus on multicast | **Multicast**   * Delivery of information to interested systems   + One to many * Multimedia delivery, stock exchanges * Very specialized   + Difficult to scale across large networks |
|  |  |  |

|  |  |
| --- | --- |
| **PDU (Protocol Data Unit)**   * A unit of transmission   + A different group of data at different OSI layers * Ethernet operates on a frame of data   + It has no idea wha’t inside * IP operates on a packet of data   + Inside is TCP or UDP, but IP doesn’t know that * TCP or UDP PDU   + TCP segment   + UDP datagram |  |
| **Maximum Transmission Unit (MTU)**   * **Maximum IP packet to transmit**   + **But not fragment** * **Fragmentation slows things down**   + **Losing a fragment loses an entire packet**   + **Requires overhead along the path** * **Difficult to know the MTU all the way through the path**   + **Automated methods are often inaccurate**     - **Especially when ICMP is filter** |  |



**Network Segmentation**





|  |  |
| --- | --- |
| **Spanning Tree Protocol (802.1D)**   * Loop protection   + Connect two switches to each other     - Create a loop with two cables     - They’ll send traffic back and forth forever     - There’s no ‘counting’ mechanism at the MAC layer   + This is an easy way to bring down a network     - And somewhat difficult to troubleshoot     - Relatively easy to solve   + IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990) * STP Port States   + Blocking     - Not forwarding to prevent a loop   + Listening     - Not forwarding and cleaning the MAC table   + Learning     - Not forwarding and adding to the MAC table   + Forwarding     - Data passes through and is fully operational   + Disabled     - Administrator has turned off the port | RSTP (802.1w)   * Rapid Spanning Tree Protocol (802.1w)   + A much needed update to STP   + Latest standard * Faster convergence   + From 30-50 seconds to 6 seconds * Backwards compatible with 802.1D STP |

|  |  |
| --- | --- |
| **Switch Interface Properties**   * Speed and duplex   + Speed: 10 / 100 / 1,000   + Duplex: Half/Full   + Automatic and manual   + Needs to match on both sides * IP address management   + Layer 3 interfaces   + VLAN interfaces   + Management Interfaces   + IP address, subnet mask/CIDR block, default gateway, DNS (optional) * VLANs   + VLAN assignment     - Each device port should be assigned a VLAN   + Trunking     - Connecting switches together     - Multiple VLANs in a single link   + Tagged and untagged VLANs     - A non-tagged frame is on the default VLAN       * Also called the native VLAN     - Trunk ports will tag the outgoing frames       * And remove the tag on incoming frames * DMZ   + Demilitarized zone     - An additional layer of security between the Internet and you * Power over Ethernet (PoE)   + Power provided on an Ethernet cable     - One wire for both network and electricity     - Phones, cameras, wireless access points     - Useful in difficult to power areas   + Power provided at the switch     - Built-in power - Endspans     - In-line power injector - Midspans   + Power Modes     - Mode A - Power on the data pairs     - Mode B - Power on the spare pairs   + **PoE: IEEE 802.3af-2003**     - The original PoE specification     - Included in 802.3at     - Now part of the 802.3 standard     - 15.4 watts DC power     - Maximum current of 350 mA   + **PoE+: IEEE 802.3at-2009**     - The updated PoE specification     - Now also part of the 802.3 standard     - 25.5 watts DC power     - Maximum current of 600 mA * Port mirroring   + Examine a copy of the traffic     - Port mirror (SPAN), network tap   + No way to block (prevent) traffic | **Routing**   * Send IP packets across the network   + Forwarding decisions are based on destination IP address * Each router only knows the next step   + The packet asks for directions every hop along the way   + The list of directions is held in a routing table * **Static Routing**   + Administratively define the routes   + Advantages     - Easy to configure and manage on smaller networks     - No overhead from routing protocols (CPU, memory, bandwidth)     - Easy to configure on sub networks (only one way out)     - More secure - no routing protocols to analyze   + Disadvantages     - Difficult to administer on larger networks     - No automatic method to prevent routing loops     - If there’s a network change, you have to manually update the routes     - No automatic rerouting if an outage occurs. * **Dynamic Routing**   + Routers send routes to other routers     - Routing tables are updated in (almost) real-time   + Advantages     - No manual route calculations or management     - New routes are populated automatically     - Very scalable   + Disadvantages     - Some router overhead required       * CPU, Memory, Bandwidth     - Requires some initial configuration to work properly * **Default Route**   + A route when no other route matches     - The ‘gateway of last resort'   + A remote site may have only one route     - Go that way -> rest of the world   + Can dramatically simplify the routing process     - Works in conjunction with all other routing methods |

**AS (Autonomous System)**

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

|  |  |
| --- | --- |
| **IGP (Interior Gateway Protocol)**   * Used within a single autonomous system   + Not intended to route between AS     - Thats why there’s Exterior Gateway Protocols * IPv4 dynamic routing   + OSPFv2 (Open Shortest Path First)   + RIPv2 (Routing Information Protocol version 2)   + EIGRP (Enhanced Interior Gateway Routing Protocol) * IPv6 dynamic routing   + OSPFv3   + EIGRP for IPv6   + RIPng (RIP next generation) | **EGP (Exterior Gateway Protocol)**   * Used to route between autonomous systems   + Leverages the IGP at the AS to handle local routing * BGP (Border Gateway Protocol)   + Many organizations use BGP as their EGP |

**Dynamic Routing Protocols**

* Listen for subnet information from other routers
  + Sent from router to router
* Provide subnet information to other routers
  + Tell other routers what you know
* Determine the best path based on the gathered information
  + Every routing protocol has its own way of doing this
* When network changes occur, update the available routes
  + Different convergence process for every dynamic routing protocol
* Which routing protocol to use?
  + What exactly is a route?
    - Is it based on the state of the link?
    - Is it based on how far away it is?
  + How does the protocol determine the best path?
    - Some formula is applied to the criteria to create a metric
    - Rank the routes from best to worst
  + Recover after a change to the network
    - Convergence time can vary widely between routing protocols
  + Standard or proprietary protocol?
    - OSPF and RIP are standards, some functions of EIGRP are Cisco proprietary
* **Distance-vector routing protocols**
  + Information passed between routers contains routing tables
    - How many ‘hops’ away is another network?
    - The deciding ‘vector’ is the ‘distance'
  + Usually automatic with very little configuration
  + Good for smaller networks
    - Doesn’t scale well to very large networks
* **Link-state routing protocols**
  + Information passed between routers is related to the current connectivity
    - If its up, you can get there
    - If its down, you can’t.
  + Consider the speed of the link
    - Faster is always better, right?
  + Very scalable
    - Used most often in large networks
  + OSPF
    - Large scalable routing protocol
* **Hybrid routing protocols**
  + A little link-state, a little distance-vector
    - Not many examples of a hybrid routing protocol
  + **BGP (Border Gateway Protocol)**
    - Determines route based on paths, network policies, or configured rule-sets

|  |  |
| --- | --- |
| **IP Addressing**   * IP Address : 192.168.1.1   + Every device needs a unique IP address * Subnet Mask : 255.255.255.0   + Used by the local workstation to determine what subnet its on     - The subnet mask isn’t (usually) transmitted across the network     - You’ll ask for the subnet mask all the time * IP address is a combo of network ID and a host ID   + The subnet mask determines what part of the IP address is the network and which part is the host   **IPv4**   * OSI Layer 3 address * 32 bit |  |
| **IPv6**   * 128 bit address * Hexadecimal * IPv6 Address Compression |  |

**Dual Stack Routing**

* Dual stack IPv4 and IPv6 routing
  + Run both at the same time
  + Interfaces will be assigned multiple address types
* IPv4
  + Configured with IPv4 addresses
  + Maintains an IPv4 routing table
  + Uses IPv4 dynamic routing protocols
* IPv6
  + Configured with IPv6 addresses
  + Maintains a separate IPv6 routing table
  + Uses IPv6 dynamic routing protocols.
* Tunneling IPv6
  + 6-4 addressing
    - Send IPv6 over an existing IPv4 network
    - Creates an IPv6 address based on the IPv4 address
    - Requires relay routers
      * IP protocol 41 - a transition technology
    - No support for NAT
* Tunneling IPv6
  + Send IPv4 over an existing IPv6 network
* Teredo / Miredo
  + Tunnel IPv6 through NATed IPv4
    - End-to-end IPv6 through an IPv4 network
    - No special IPv6 router needed
    - Temporary use
      * We’ll have IPv6 native networks soon (?)
  + Miredo
    - Open-source Teredo for Linux, BSD Unix, and Mac OS X
    - Full functionality

**NDP (Neighbor Discovery Protocol)**

* No broadcasts
  + Operates using multicast with ICMPv6
* Neighbor MAC discovery
  + Replaces IPv4 ARP
* SLAAC (Stateless Address Autoconfiguration
  + Automatically configure IP address without DHCP server.
* DAD (Duplication Address Detection)
  + No duplicate IPs
* Discover Routers
  + Router Solicitation (RS) and Router Advertisement (RA)

|  |  |
| --- | --- |
| (Finding the Router) - ICMPv6 adds NDP   * Routers also send unsolicited RA messages from multicast dest ff02::1 * Transfers IPv6 information prefix value, and prefix length, etc |  |
| Theres No ARP in IPv6   * How is the MAC address discovered?   Neighbor Solicitation (NS)   * Sent as a multicast   Neighbor Advertisement (NA) |  |

**Prioritizing Network Traffic**

* Many different devices and different applications which have different network requirements and different priorities.
* Packet Shaping:
* Packet shaping / Traffic shaping
* Control with bandwidth usage or data rates
* Set important applications to have higher priorities than other apps.
* QoS (Quality of Service)
* Prioritize traffic performance
  + VoIP > web browsing
* Describes the process of controlling traffic flows.
* Many different methods across many different topologies.
* Managing QoS
* CoS (Class of Service)
  + OSI Layer 2
  + Ethernet frame header in an 802.1Q trunk
  + Usually applied in the intranet (not from an ISP)
* Differentiated Services (DiffServ)
  + OSI Layer 3
  + QoS bits are enabled in the IPv4 header
  + Bits are set external to the application
  + Routers apply the QoS
* DSCP (Differentiated Services Code Point)
  + DS (Differentiated Services) field in the IP header

|  |  |
| --- | --- |
| **NAT (Network Address Translation)**   * Estimated over 20 billion devices connected   + IPv4 supports around 4.29 billion addresses   + Address Space for IPv4 is exhausted | **PUBLIC AND PRIVATE ADDRESSES** |
| **NAT overload/PAT (Port Address Translation)** | **Port Forwarding**   * 24x7 access to a service hosted internally * External IP/port number maps to an internal IP/port   + Does not have to be the same port number * Also called Destination NAT or Static NAT   + Destination address is translated from a public IP to a private IP   + Does not expire or timeout |

**Access Control Lists**

* Packet Filtering
  + Used to allow or deny traffic
    - Also used for NAT, QoS, etc.
  + Defined on the ingress or egress of an interface
    - Incoming or outgoing
  + ACLs can evaluate on certain criteria
    - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICPM
  + Deny or permit
* Firewall Rules
  + Access Control Lists
    - Allow or disallow traffic based on tuples
    - Groupings or categories
      * Source IP, Destination IP, port number, time of day, application, etc
  + A logical path
    - Usually top-to-bottom
  + Can be very general or very specific.
    - Specific rules are usually at the top
  + Implicit deny
    - Most firewalls include a deny at the bottom
      * Even if you don’t put one.

**Circuit Switching**

* Circuit is established between endpoints before data passes
* Nobody can use the circuit when idle
  + Inefficient use
* **POTS (Plain old telephone service)**
* **PSTN (Public switched telephone network)**
* T1 / E1 / T3 / E3
  + Create a circuit between two sites
* ISDN (Integrated Services Digital Networking)
  + Use a phone number to call another ISDN modem

Packet Switching

* Data is grouped into packets
  + Voice, data, video, etc
  + Like a network
* Media usually shared
* SONET, ATM
* DSL
* Frame Relay
* MPLS
* Cable Modem
* Satellite
* Wireless

SDN (Software Defined Networking)

* Networking devices have two functional planes of operation.
  + Control plane, data plane
* Directly programmable
  + Config is different than forwarding
* Agile
* Centrally managed
* Programmatically configured
* Open standards / Vendor neutral
* Distributed Switching
  + Remove the physical segmentation
  + When a VM moves, the network doesn’t change

1.4

Binary Math

IPv4 Addresses

* Each device has an IP address
* Loopback address
  + An address to yourself
  + 127.0.0.1 - 127.255.255.254
* Reserved addresses
  + 240.0.0.1 - 255.255.255.254
* Virtual IP addresses (VIP)
  + Not associated with a. Physical network adapter
  + Virtual machine, internal router address.

Subnetting

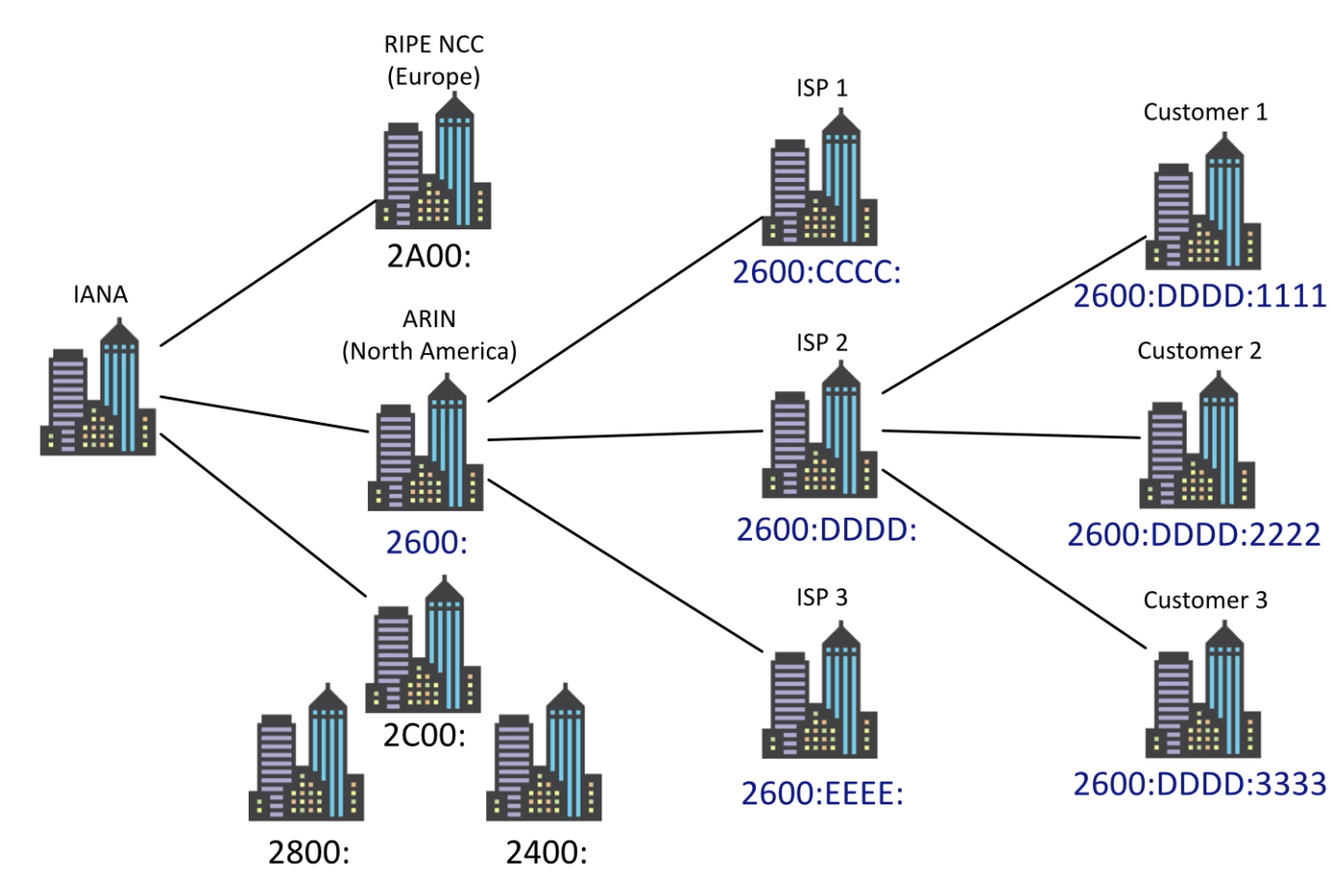
|  |  |
| --- | --- |
| Classful Subnetting |  |
| CIDR |  |

Construction of a subnet

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

|  |  |  |
| --- | --- | --- |
| 10.74.222.11 | Network | Host |
|  | 10. | 74.222.11 |
| Network Address | 10. | 0.0.0 |
| First host address | 10. | 0.0.1 |
| Broadcast address | 10. | 255.255.255 |
| Last host address | 10. | 255.255.254 |

IPv6 Subnet Masks



VLSM (Variable Length Subnet Masks)

* Class-based networks are inefficient
* Allows network admins to define their own subnet masks

Calculating Subnets and hosts

|  |  |
| --- | --- |
|  |  |

Assigning IPv4 Addresses

* DHCP (Dynamic Host Configuration Protocol)
  + Provides automatic address / IP configuration for most devices
  + Assigns an IP address from first available from a large pool of addresses
  + Static
    - Server, printer, etc...
    - Configure an IP reservation on the DHCP server
      * Associate a specific MAC address with an IP address
* APIPA (Automatic Private IP Addressing)
  + A link-local address
    - No forwarding by routers
  + 169.254.0.1 - 169.154.255.254
    - First and last 256 addresses are reserved
    - Functional block of 169.254.1.0 - 169.254.254.255
  + Automatically assigned
    - Uses ARP to confirm the address isn’t currently in use

|  |  |
| --- | --- |
| Assigning IPv6 Addresses   * Stateful DHCPv6   + Similar to DHCPv4     - Ump/546 (client) and ump/547 (server)   + fe80 link-local prefix     - Link-local used for packets sent only to directly connected devices (not routed) * Converting EUI-48 to EUI-64   + Split the MAC     - Two 3-byte (24-bit) halves   + Put FFFE in the middle     - The missing 16 bits   + Invert the seventh bit     - Changes the address from globally unique/universal     - Turns the burned-in address (BIA) into locally administered address     - This is the U/L bit (universal/local) |  |

1.5

Network Topologies

|  |  |
| --- | --- |
| * Star   + Used in most large and small networks   + All devices are connected to a central device   + Switched Ethernet networks |  |
| Ring |  |
| Bus |  |
| Mesh |  |

LAN (Local Area Network)

* Local is relative
* A building or group of buildings
* Ethernet and 802.11 Wireless networks
  + Any slower and it isn’t ‘local'

WLAN

* 802.11 technologies
* Mobility
  + Within a building
  + In a limited geographical area
* Expand coverage with additional access points
  + Downtown area
  + Large campus

MAN

* Metropolitan Area Network
  + A network in your city
  + Larger than a LAN, often smaller than a WAN
* Historically MAN-specific topologies
  + Everyone is moving to Metro Ethernet
* Common to see government ownership

WAN

* Wide Area Network
  + Spanning the globe
* Generally connects LANs Across a distance
  + Generally much slower than the LAN
* Many different WAN technologies
  + Point-to-point serial, MPLS, etc
  + Terrestrial and non-terrestrial

CAN

* Campus Area Network
* Limited geographical area
* LAN technologies
  + Fiber connected
  + High speed Ethernet

NAS vs. SAN

* Network Attached Storage
  + Connected to a shared storage device across the network
  + File-level access
* Storage Area Network
  + Looks and feels like a local storage device
  + Very efficient reading and writing
* Requires a lot of bandwidth

PAN

* Personal Area Network
  + Your own private network
  + Bluetooth, IR, NFC...
* Automobile
  + Audio output
  + Integrate with phone
* Mobile Phone
  + Wireless headset

IoT (Internet of Things)

* Wearable tech
* Home automation
* Z-Wave
  + Home automation networking
  + Wireless mesh networking
  + Uses the ISM band
    - Industrial, Scientific, and Medical
    - 900 Mhz frequencies in the US
    - No conflicts with 802.11
* ANT / ANT+
  + Wireless sensor network protocol
    - 2.4Ghz ISM band (industrial, scientific, and medical)
    - Ultra-low-power protocol
    - Fitness devices, heart rate monitors, etc
  + A separate wireless service
    - Not 802.11 or Bluetooth
  + Denial of service
    - Spectrum jamming
  + Optional encryption
    - And no method to maintain integrity
* Bluetooth
  + High speed communication over short distances
    - PAN
  + Connects our mobile devices
    - Smartphones
    - tethering
    - Headsets and headphones
    - Health monitors
* NFC
  + Near field Communication
  + Two-way wireless communication
    - Builds on RFID
  + Payment systems
    - Major credit cards
    - Online wallets
  + Bootstrap for other wireless
    - NFC helps with Bluetooth pairing
  + Access token, identity ‘card'
    - Short range with encryption support.
* IR
  + Infrared
  + Included on many smartphones, tablets and smartwatches
    - Not really used for file transfers and printing
  + Control your entertainment center.
* RFID
  + Radio-frequency identification
  + Everywhere
    - Access badges
    - Inventory/assembly line tracking
    - Pet/Animal identification
  + Radar technology
    - Radio energy transmitted to the tag
    - RF powers the tag, ID is transmitted back
    - Bidirectional communication
    - Some tag formats can be active/powered.
* IEEE 802.11
  + Wireless networking (802.11)
  + WiFi

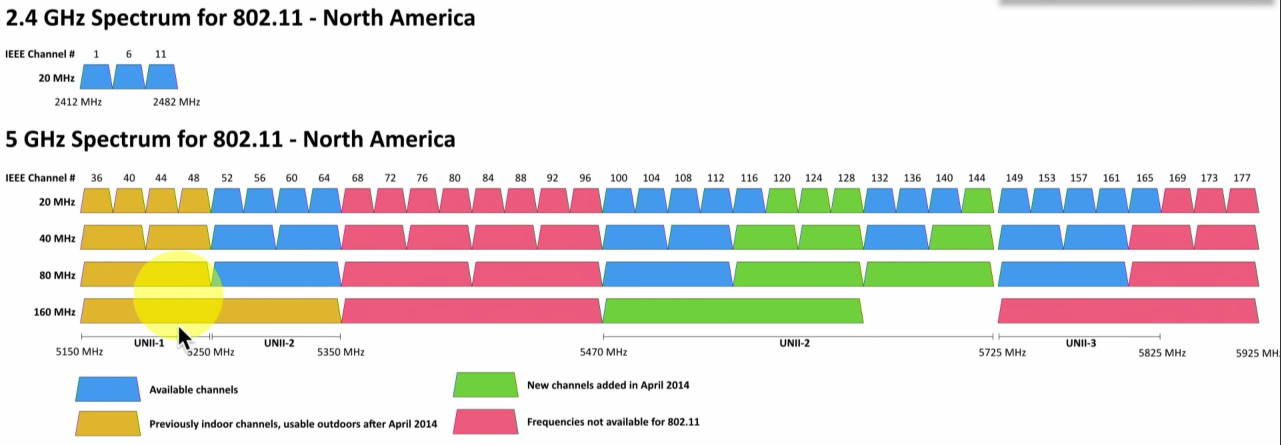
1.6

Wireless Network Technologies

* Frequency
  + 2.4GHz or 5GHz
    - (Sometimes both)
  + Channels
    - Groups of frequencies, numbered by the IEEE
    - Non-overlapping channels would be necessary
  + Bandwidth
    - Amount of frequency in use
    - 20MHz, 40MHz, 80MHz, 160Mhz
* MIMO
  + Multiple Input Multiple Output
* MU-MIMO
  + Multiple User - Multiple Input Multiple Output
* Omnidirectional Antennas
  + One of the most common
  + Signal is evenly distributed on all sides
  + Good choice for most environments.
* Directional Antennas
  + Increases the distance
  + Send and receive in a single direction
  + Antenna performance is measured in dB
    - Double power every 3dB of gain
  + Yagi antenna
    - Very directional and high gain
  + Parabolic Antenna
    - Focus the signal to a single point

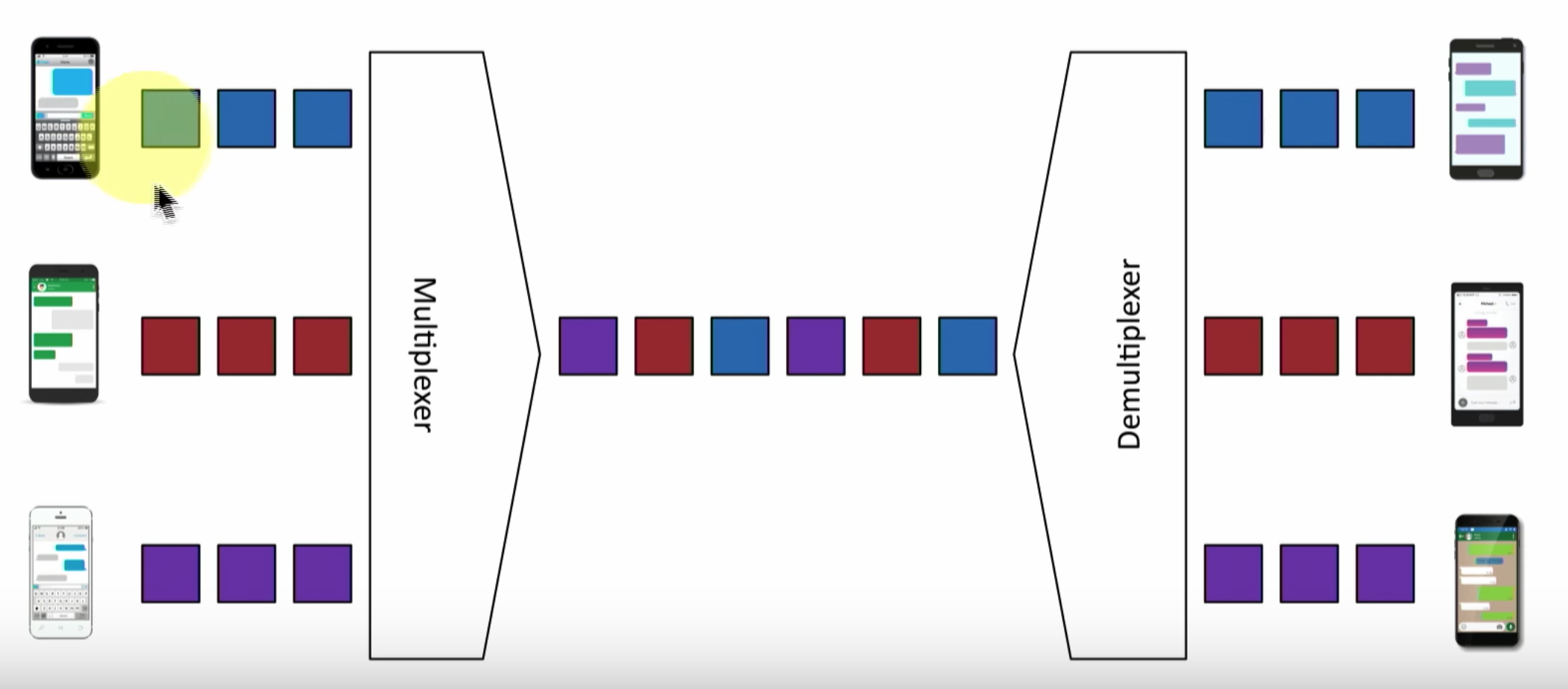
Wireless Standards

|  |  |
| --- | --- |
| * 802.11a   + 5Ghz   + 54Mb/s   + 20MHz Channel bandwidth   + Smaller range than 802.11b     - Higher frequency is absorbed by objects in the way     - Many rules-of-thumb calculate 1/3 the range of 802.11b or 802.11g |  |
| * 802.11b   + 2.4GHz range   + 11Mb/s   + 22MHz channel bandwidth   + Better range than 802.11a     - Less absorption problems   + More frequency conflict |  |
| * 802.11ac   + 5GHz band     - Less crowded, more frequencies (up to 160 MHz channel bandwidth)   + 40MHz for 802.11n stations   + 80MHz required for 802.11ac stations   + 160MHz optional (contiguous channels or non-contiguous bonded channels.)   + Increased channel bonding     - Larger bandwidth usage   + Denser signaling modulation     - Faster data transfers   + Eight MU-MIMO streams     - Twice as many streams as 802.11n     - Nearly 7 gigabit per second |  |
| * 802.11n   + Update to 802.11g 802.11b, and 802.11a   + 20 or 40MHz channel widths     - 2 contiguous 20MHz bonded channels     - In 2.4GHz, a 40 channel uses over 80% of the available bandwidth   + 5GHz and/or 2.4GHz     - 40MHz channel widths   + 600Mbit/s     - 40 MHz mode and 4 antennas   + 802.11n uses MIMO     - Multiple-input multiple-output     - Multiple transmit and receive antennas |  |
|  |  |



Cellular Networks

* Mobile devices
* Separate land into ‘cells'
* 2G networks
  + GSM - Global System for Mobile Communications
    - 90% of the market
      * Originally an EU standard
    - Original GSM standard uses TDMA to multiplex calls
  + CDMA - Code Division Multiple Access
    - Everyone communicates at the same time
    - Each call uses a different code
    - The codes are used to filter each call on the receiving side
* Poor data support
  + Originally used circuit-switching
  + Minor upgrades for some packet-switching
* TDMA
  + Time-Division Multiple Access
  + Multiple streams are combined into a single stream.



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

1.7

Cloud

1.8

DNS (Domain Name System)

|  |  |
| --- | --- |
| * Translates human-readable names into computer-readable IP address * Resource Records   + Address Records (A) (AAAA)     - A records are for IPv4 addresses     - AAAA records are for IPv6 addresses   + Canonical name records (CNAME)     - A name is an alias of another, canonical name       * One physical server, multiple services   + Service records (SRV)     - Find a specific service       * Where is the Windows Domain Controller       * Where is the instant messaging server       * Where is the VoIP controller   + Mail exchanger record (MX)     - Determines the host name for the mail server   + Name Server records (NS)     - List the name servers for a domain       * NS records point to the name of the server   + Pointer Record (PTR)     - The reverse of an A or AAAA record       * Added to a reverse map zone file   + Text Record (TXT)     - Human-readable text information     - SPF protocol (Sender Policy Framework)       * Prevent mail spoofing       * Mail servers check that incoming mail really did come from an authorized host     - DKIM (Domain Keys Identified Mail)       * Digitally sign your outgoing mail       * Validated by the mail server, not usually seen by the end user       * Put your public key in the DKIM TXT record |  |

## DHCP

|  |  |
| --- | --- |
| IPv4 address configuration used to be manual   * IP address, subnet mask, gateway, DNS servers, NTP servers, etc   October 1993 - The bootstrap protocol   * BOOTP   BOOTP didnt automatically define everything   * Some manual configurations were still required * BOOTP also didnt know when an IP address might be available again |  |
| Step1: Discover  Step2: Offer  Step3: Request  Step4: Acknowledge |  |
| Managing DHCP in the enterprise   * Limited Communication Range   + Uses the IPv4 broadcast domain   + Stops at a router * Multiple servers needed for redundancy   + Across different locations * Scalability is always an issue   + May not want (or need) to manage DHCP servers at every remote location. |  |
| DHCP Relay   * Configure router with a DHCP relay   + Changes broadcast to unicast |  |
| IP Address Management (IPAM)   * Manage IP addressing   + Plan, track, configure, DHCP * Report on IP address usage   + Time of day, user-to-IP mapping * Control DHCP reservations   + Identify problems and shortages * Manage IPv4 and IPv6   + One console |  |

## Configuring DHCP

* Scope Properties
  + Ip address range
    - And excluded addresses
  + Subnet mask
  + Lease durations
  + Other options
    - DNS server
    - Default gateway
    - WINS server
* DHCP pools
  + Group of IP addresses
    - Each subnet has its own scope
* DHCP address allocation
  + Dynamic Allocation
    - DHCP server has a big pool of addresses to give out
    - Addresses are reclaimed after a lease period
  + Automatic Allocation
    - Similar to dynamic allocation
    - DHCP server keeps a list of past assignments
    - You’ll always get the same IP address
  + Static Allocation
    - Administratively configured
    - Table of MAC addresses
      * Each MAC address has a matching IP address
    - Other Names:
      * Static DHCP Assignment
      * Static DHCP
      * Address Reservation
      * IP Reservation
* DHCP Leases
  + Leasing your address
    - Its only temporary
    - But it can seem permanent
  + Allocation
    - Assigned a lease time by the DHCP server
    - Administratively configured
  + Reallocation
    - Reboot your computer
    - Confirms the lease.
  + Workstation can also manually release the IP address
    - Moving to another subnet
* DHCP renewal
  + T1 timer
    - Check in with the lending DHCP server to renew the IP address
    - 50% of the lease time (by default)
  + T2 timer
    - If the original DHCP server is down, try rebinding with any DHCP server
    - 87.5% of the lease time (7/8ths)

## NTP (Network Time Protocol)

* Switches, routers, firewalls, servers, workstations
  + Every device has its own clock
* Synchronizing the clocks becomes critical
  + Log files, authentication information, outage details
* Automatic updates
* Flexible
* Very accurate
* NTP server
  + Respond to time requests from NTP clients
  + Does not modify their own time
* NTP client
  + Requests time updates from NTP server
* NTP client/server
  + Requests time updates from an NTP server
  + Responds to time requests from other NTP clients
* NTP stratum layers
  + Some clocks are better than others
  + Stratum 0
    - Atomic clock, GPS clock
    - Very accurate
  + Stratum 1
    - Synchronized to Stratum 0 servers
    - Primary time servers.
  + Stratum 2
    - Sync’d to stratum 1 servers