The Network Layer

* Network Layer
  + Addresses packets with an IP address
  + Encapsulates the packet
  + Routes the packet to the destination
  + Decapsulates the packet
* IPV4 Characteristics
  + Connectionless
    - The sender doesn’t know
      * If the receiver is present
      * If the packet arrived
      * If the receiver can read the packet
    - The receiver doesn’t know
      * When it is coming
  + “Best effort” Delivery (Unreliable)
    - Unreliable means simply that IP does not have the capability to manage and recover from undelivered or corrupt packets
    - Since protocols at other layers can manage reliability, IP is allowed to function very efficiently at the network layer
  + Media independent
    - Not concerned with the physical medium. Is concerned Maximum Transmission Unit (MTU)
    - Fragmentation: Intermediary devices (routers) will need to split up a packet when forwarding it from one media to a media with a smaller MTU
    - MTUs:
      * Copper Ethernet: MTU = 1,518 bytes
      * Copper Serial: Frame Relay MTU = 512 bytes
      * Optical Fiber: ATM MTU = 17,966 bytes
      * Wireless: 802.11 MTU = 2272 bytes
  + IPV4 Packet Header
    - Timeline

      Description automatically generated
* Why separate hosts into networks?
  + Performance

## Security

* + Address management
* Hierarchical addressing
  + IP addresses are divided into a 2-level hierarchy – Network and Host
* Dividing networks from networks
  + Graphical user interface

    Description automatically generated with medium confidence
  + An IP Version 4 address has two parts:
    - Network number
    - Host number
    - The network portion of the address is the same for all hosts on the network.
    - Each device is identified by a unique host portion.
  + This hierarchy means that routers only need to know the network portion – not the address of each individual host.
  + There is a direct relationship, bit for bit, between the IP Address and it's associated subnet mask.
  + Any subnet mask bit that is a 1 means that the associated address bit belongs to the network number.
  + Any subnet mask bit that is a 0 means that the associated address bit belongs to the host number
* IP addressing – The subnet mask
  + There are two methods of expressing a subnet mask.
    - The traditional method is to use the decimal value of the 1 bits that apply to the network.
      * 192.168.1.2 255.255.255.0
        + This method is used for Classful Routing
    - The new method is known as IP Prefix or CIDR.
      * Simply follow the IP address with a slash (/) and the number of bits that make up the network portion.
      * The remainder of the 32 bits are for the host number.
        + 192.168.1.2 / 24

This method indicates Classless Routing or Classless Interdomain Routing (CIDR).

* Address Types
  + Two address types:
    - MAC address:
      * Physical address of the host
      * Burned in to the NIC
      * Layer 2 address
    - Network Address:
      * Logical address of the host
      * Assigned by network administrator
      * Layer 3 address
* Gateway
  + Default Gateway is defined to all hosts on the network.
  + Gateway address is the address of the router interface.
    - Network portion must be on the same network as all of the hosts.
  + Additionally, no packet can be forwarded without a route.
  + A router makes a forwarding decision for each packet that arrives at the gateway interface.
  + The destination may be one or more hops away.
* Route: A path to a network
  + The routing table stores information about directly connected and remote networks.
  + Remote networks are networks not directly connected to the router (manual configuration or learned dynamically).
* Address Resolution
  + The process of mapping a hardware address to a higher-layer protocol address
  + Address Resolution Protocol
    - Maps IPv4 address to a specific MAC address
    - MAC Address Table vs. ARP Table
    - A simple request-response protocol
      * Who has IP address …?
      * Response from host with that L3 address
* Drivers for IPv6
  + Early 90’s protocols
  + Perceived weaknesses of IPv4
    - Insufficient address space
    - Classes
    - No inherent support for time-sensitive traffic
    - No true ubiquitous security
    - “Poor” route handling
  + “Current” Drivers
    - Policy - US Office of Management and Budget
    - 3GPP
    - IEEE
    - Hardware – Cell phones, laptops, …
    - IPv4 Exhaustion
* IPV6 Address format
  + Dotted Decimal – 127.54.83.21
  + Colon-Hexidecimal
    - ABCD:0000:0000:0020:1919:0A12:0000:7201
  + Rules for condensing IPv6 address
    - Can skip leading zeros in each “tuple”
      * ABCD:0:0:20:1919:A12:0:7201
    - Can compress ONE sequence of all zero “tuple”
      * ABCD::20:1919:A12:0:7201
* IPv6 Host Addressing
  + Addresses are assigned to interfaces
  + Manual Addressing
  + DHCPv6
  + Stateless Auto-Configuration (RFC 2462)
    - EUI-64

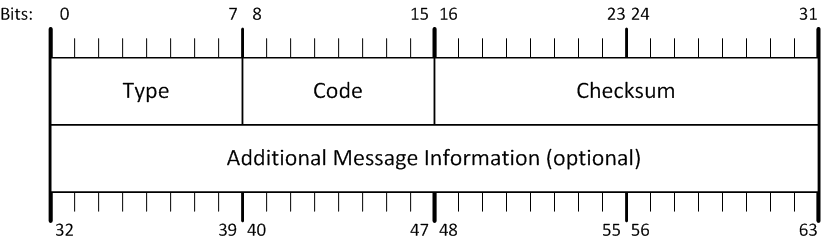
Subnetting

* IP addressing
  + We assign a single 32-bit binary value to each host residing in a network segment
    - Represented in “dotted decimal” form
    - Dotted decimal form is four 8-bit groupings [octets]
  + 10000000110100101000101100011111
  + 10000000 11010010 10001011 00011111
  + 128 210 139 31
  + 128.210.139.31
  + How do we know where the network ID stops and the host ID begins?
* 3 Approaches
  + Classes (2-layer hierarchy)
    - 3 classes (RFC 791 in 1981) A: 28, B: 216, C: 224
    - 4 classes (RFC 988 in 1986): Multicast
    - 5 classes (RFC 3330 in 2002): experiment
  + Fixed-Length Subnetwork Mask (3-layer hierarchy)
    - Created the idea of sub-networks (RFC 940 in 1985)
  + Non-Fixed-Length Subnetwork Masks (n-layer hierarchy)
    - VLSM (RFC 950 in 1985)
    - CIDR (RFC 1518 in 1993)
  + Class approach introduces the idea of 2-layer hierarchy.
  + Classful subnetting is 3-layer hierarchy
  + Classless subnetwork is n-layer hierarchy
* IP addressing – Class based
  + One portion of the address is for:
    - Subnetwork ID
    - Host ID
  + How is this represented?
    - ADC40721.wmf
* Subnetwork mask
  + Subnetwork – A network segment created from a larger network segment (major network)
  + Addition of 32-bit binary mask
    - Performs a logical AND function with IP Address to determine Network ID
    - Logical AND
      * 0 0 = 0
      * 0 1 = 0
      * 1 0 = 0
      * 1 1 = 1
* Subnetworking
  + Requires the borrowing of bits to create a more specific network ID (subnetwork ID)
    - Where do these bits come from?
      * Network ID - 10000000110100101000000000000000
      * Subnet Mask -11111111111111110000000000000000 = /16
      * New Mask - 11111111111111111111111100000000 = /24
        + This is the Extended Network Prefix (Mask)
    - If we use 8 bits, how many subnetworks can be created?
    - How do we uniquely identify each of them?
* Classful subnetting
  + Limitations of Classful Subnetworking
    - Only subnet the major network once
    - All subnets must be of equivalent size
    - There are two reserved subnets for each classful subnet process
      * The subnet ID with all 0s – Original Network ID
      * The subnet ID with all 1s – Broadcast
    - Reserved host IDs
      * All 0s = Subnetwork ID
      * All 1s = Broadcast
* Classless subnetting
  + Variable Length Subnet Mask (VLSM)
    - Eliminates some limitations of fixed length subnetting
    - Provides more granular control of network address space
  + Classless InterDomain Routing (CIDR)
    - No consideration for address classes
    - Provides the most granular control of network address space
    - Introduces the idea of supernetting
* The Subnetting Process
  + READ THE ENTIRE QUESTION!!!
  + Determine original network space
  + Determine need:
    - Desired number of subnets
    - Desired number of hosts
  + Mask Major Network ID with needed subnets
  + Perform logical AND operation
  + Convert to decimal values
* Options for Space Allocation
  + Minimize the host space/maximize subnet space

OR…

* + Minimize the subnet space/maximize the host space

Network support & Control Protocols

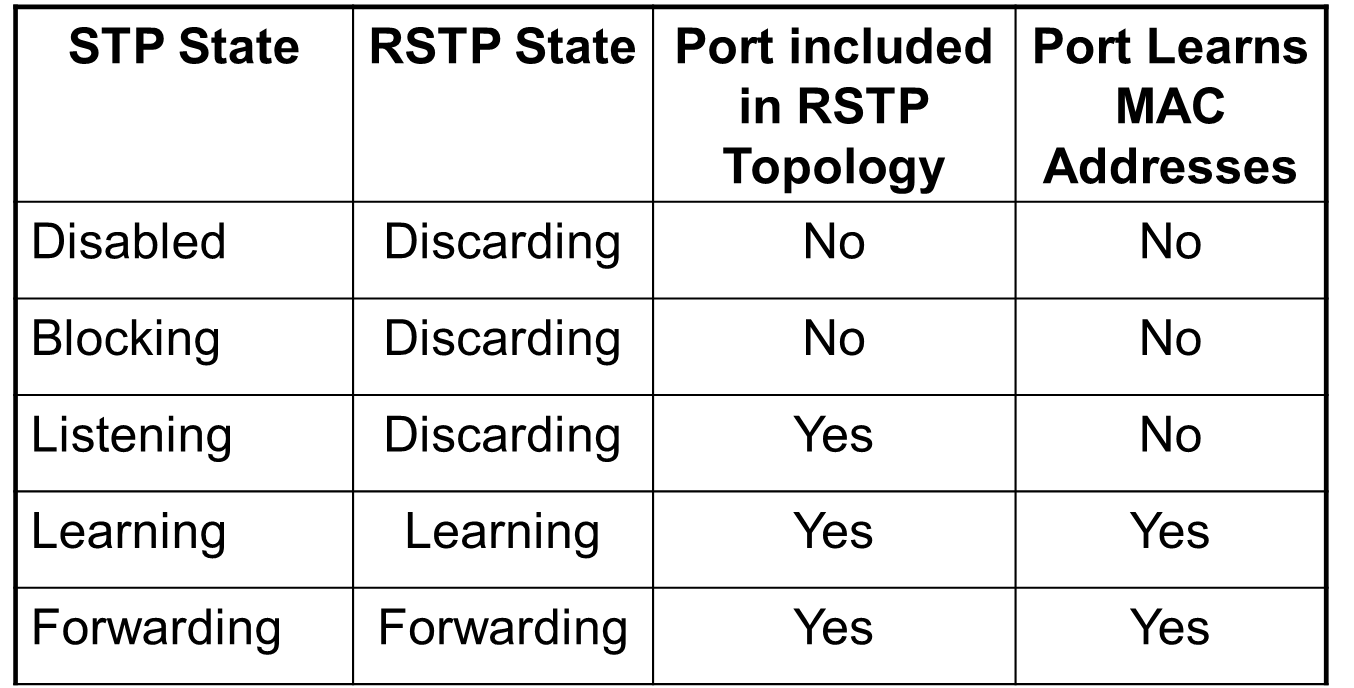
* Internet Control Message Protocol (ICMP)
  + Defined in RFC 792 (Sept. 1981)
    - What was RFC 791?
    - Has been largely unchanged since that time
  + Offers “messages” to provide feedback about network operations and delivery of datagrams
    - Does not make IP reliable
    - Uses IP for delivery of these messages
      * No guarantees that a datagram will be delivered or a control message will be received by intended destination
  + Is required in every IP deployment
    - Is sent in the IP packet payload
  + ICMP is more than ping and traceroute
* Basic ICMP Operations
  + As per RFC:
    - Messages SHOULD be created for control events
    - Messages SHOULD be honored by receiving devices
    - What does this mean?
  + Broadcast and multicast messages CAN NOT create ICMP messages
  + An error in sending an ICMP message CAN NOT generate another ICMP message informing of the error
  + Why is this important?
    - We limit the possibility of cascading and recursive failures in datagram processing.
* ICMP Message Format
  + 
  + Type – Defines the message format and actions
  + Code – Defines additional operational actions of a specific message type
  + Checksum – A one’s complement of one’s complement sum of the ICMP message in 16-bit sections
* ICMP Message Types
  + 0 – Echo Reply
  + 3 – Destination Unreachable
  + 4 – Source Quench
  + 5 – Redirect
  + 8 – Echo Request
  + 9 – Router Advertisement
  + 10 – Router Solicitation
  + 11 – Time Exceeded
  + 12 – Parameter Problem
  + 30 – Traceroute
  + Message types 1, 2, and 7 are undefined
  + Message types 19 – 29 are reserved for security and “robustness” experiments
  + Message types 42 – 255 are reserved for future use
  + All other types are defined by IANA
* ICMP Message Codes
  + Each Code is dependent upon the Type in which it is being defined
    - Type 4, Code 0 – Source Quench
    - Type 11, Code 0 – TTL Count Exceeded
  + Some Types have only one code
    - Code is set to zero (0)
    - Types 0, 4, 6, 8, 10, 13-18, and others
* ICMP Destination Unreachable
  + Type 3 Code X
    - Code value is going to describe the failure type
  + 0 – Network Unreachable
  + 1 – Host Unreachable
  + 2 – Protocol Unreachable
  + 3 – Port Unreachable
  + 4 – Fragmentation needed, but DF set
  + 5 – Source Route Failed
  + 6 – Destination Network Unknown
  + 7 – Destination Host Unknown
  + 11 – Host Unreachable for Specified ToS
  + 12 – Network Unreachable for Specified ToS
  + 13 – Communication Administratively Prohibited
* ICMP Operations – ping
  + Uses two ICMP message types
    - Initial message from source – Type 8, Code 0 (Echo Request)
    - Return message from active destination – Type 0, Code 0 (Echo Reply)
  + Operation within a network vs. between networks:
* ICMP Operations – traceroute
  + Used to determine the path a packet takes to a destination from a given source by returning the exact sequence of hops the test packet has traversed
  + Uses one message type
    - Type 30, Code 0
* ICMP Operations – Unreachable
  + There are many reasons for messages concerning unreachability
    - No route vs. rule to drop vs. error in delivery
    - Each of these is a distinct occurrence of undelivered packets
* Security Implications of ICMP
  + ICMP is not designed to be secure
    - Meaning – it is inherently insecure
  + There have been many different attacks developed using ICMP messages
    - Ping of Death (malformed message)
    - Smurf Attack (packet magnification)
    - ICMP Sweep (ping sweep)

DHCP

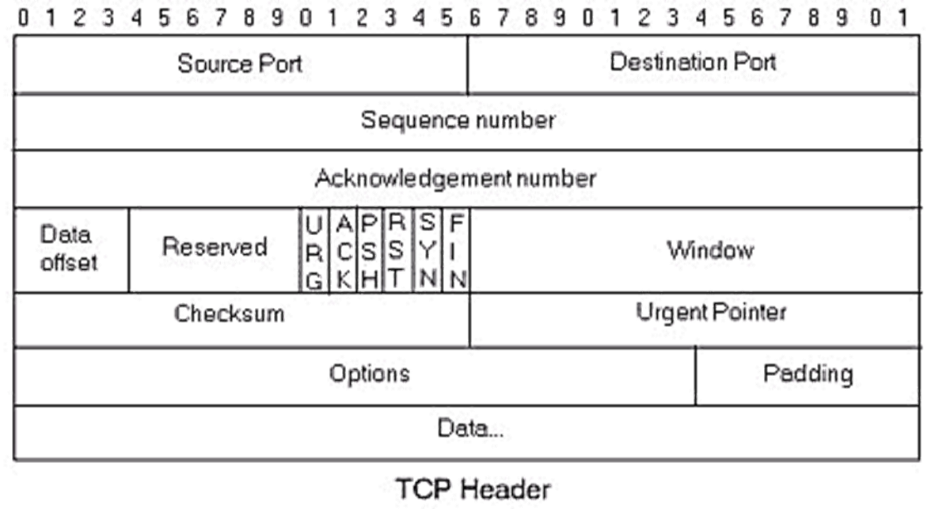
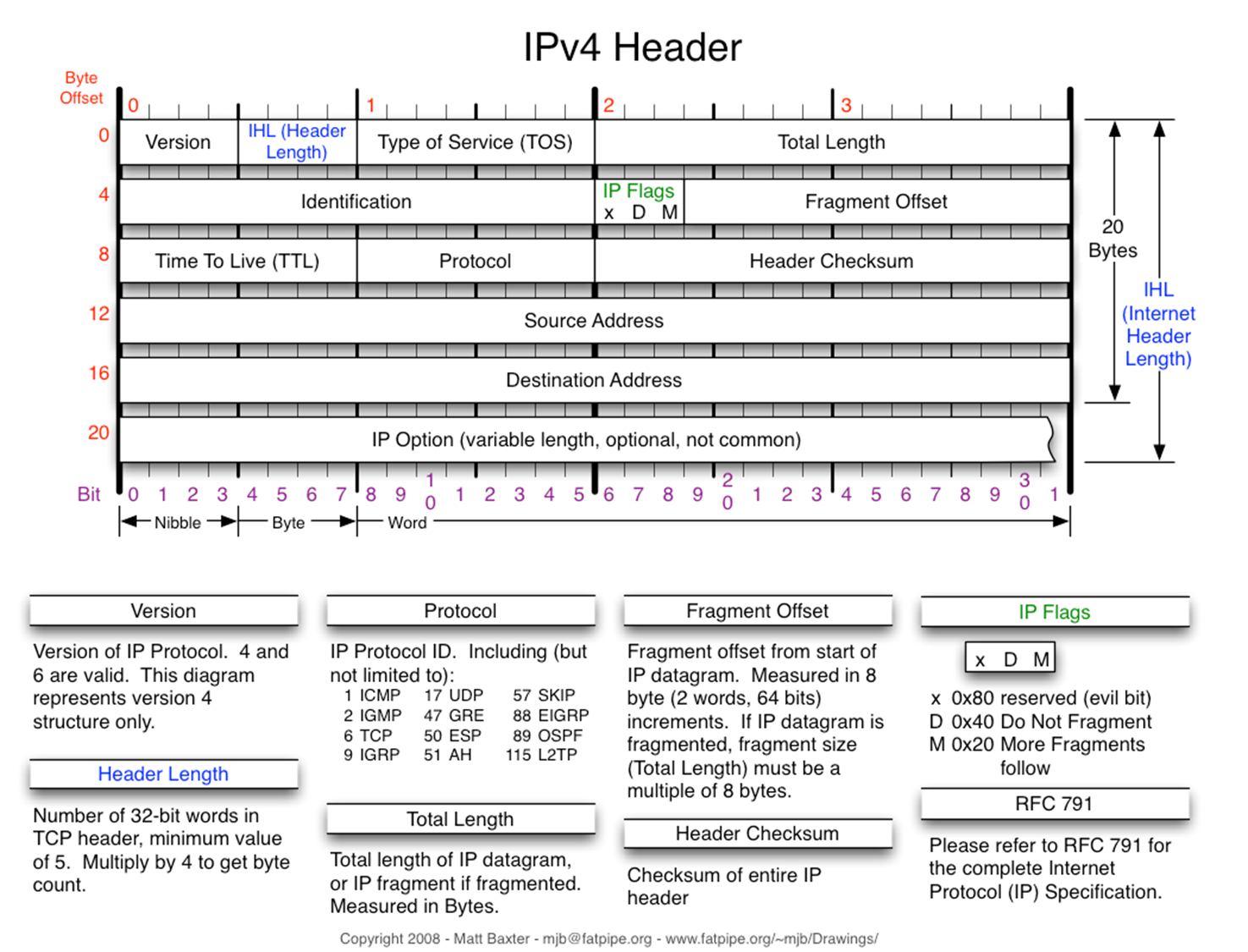
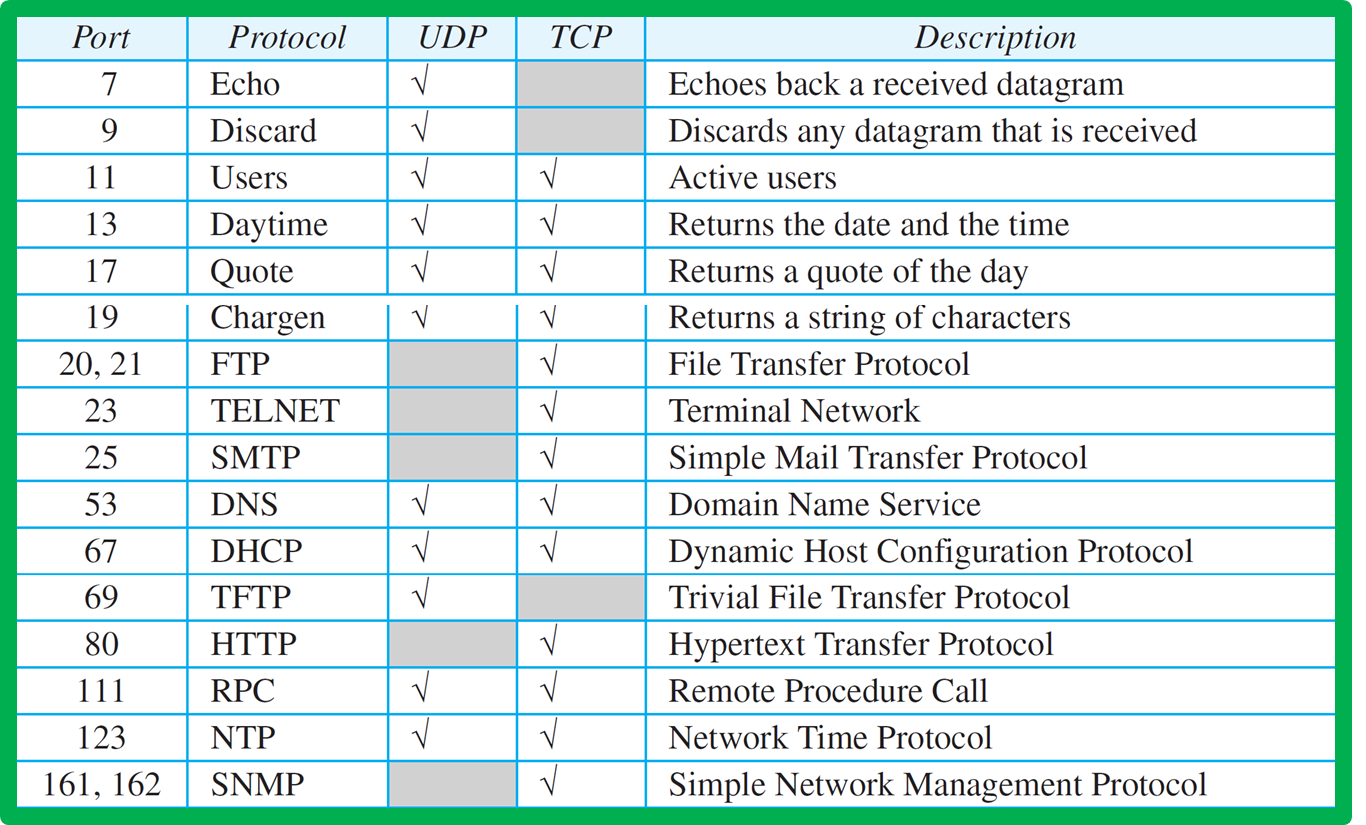
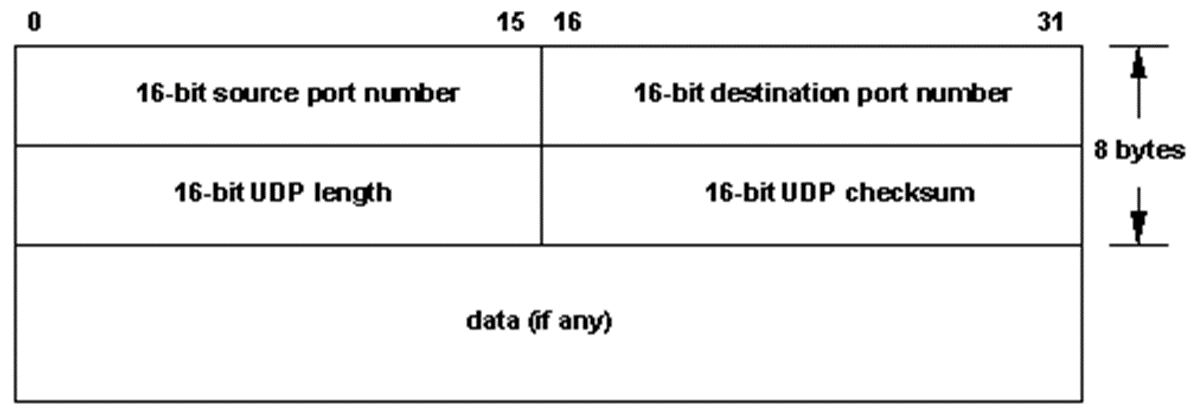
* Host Requirements
  + To communicate on an internetwork, a host needs local knowledge of:
    - Layer 2 address (MAC address)
    - Layer 3 address (IP Address)
  + MAC address is hard coded. It does not reflect the logical organizations of the host.
* Allocating Host Addresses
  + We can manually specify an IP address, but…
    - Network addresses can change over time
    - Hosts are changed over time
    - Not all hosts are continuously connected to the network
  + We can let a default address be applied
    - Is this a good idea?
  + Or we can dynamically assign addresses
    - Based on need, availability, network requirements, …
* Dynamic Addressing – RARP
  + RARP – Reverse ARP
    - RFC 903
    - Broadcast a request for the IP address associated with a given MAC address
    - RARP server responds with an IP address
    - Only assigns IP address (not the default router and subnet mask)
  + 
* Dynamic Addressing – BOOTP
  + BootP – Bootstrap Protocol
    - RFC 951
    - Host can configure its IP parameters at boot time. TWO phases:
      * Client IP address assignment and detection of the IP address for a serving machine.
      * Locate boot file name via tftp server
    - Not only assign IP address, but also default router, network mask, etc.
    - Sent as UDP messages (UDP Port 67 (server) and 68 (host))
    - Use limited broadcast address (255.255.255.255):
      * These addresses are never forwarded
    - Some drawbacks:
      * Work only on boot time
      * Does not rebind/renew. System has to reboot.
* Dynamic Addressing – DHCP
  + DHCP – Dynamic Host Configuration Protocol
    - RFC 1531 in 1993
    - RFC 1541 in 1993
    - RFC 2131 in 1997
  + A framework for passing configuration information to hosts on a TCP/IP network.”
    - Extends BootP functionality (Same ports, UDP 67, 68)
    - Client/Server Architecture
    - Adds the capability of additional configuration options
* DHCP Message Format
  + Table

    Description automatically generated
* DHCP Message Type
  + 
* Other DHCP Options
  + The OPTIONS field was specifically intended to allow vendors to enhance and extend functionality
* DHCP Leases
  + When a DHCP sends DHCPACK, lease time starts
    - Lease time is passed to client with two timer value, T1, and T2
    - When client receives the configuration, the client also starts timer T1, and T2
    - According to RFC 2132, T1 defaults to 0.5\* lease time, T2 = 0.875 \* lease time (or 7/8 of the lease time)
  + When T1 expires, the client will unicast a DHCPREQUEST to the server that offered the address
    - Server respond with DHCPACK and restart T1 and T2
    - Client received DHCPACK will reset T1 and T2
  + If no DHCPACK is received until T2 expires, client will broadcast a DHCPREQUEST message
  + Any DHCP server on the network can confirmed the lease extension with a DHCPACK message
  + If still no DHCPACK is received after its lease has expired, it has to stop using current TCP/IP configuration and restart the full DHCP process (from DHCPDISCOVER)
* Automatic Private IP Addressing (APIPA)
  + If the DHCP client is unable to locate a DHCP server and is not configured with an alternate configuration, the computer configures itself with a 169.254.0.0/255.255.0.0 address.
  + The auto-configured computer then tests to verify that the IP address it has chosen is not already in use by using a gratuitous ARP broadcast.
  + If the chosen IP address is in use, the computer randomly selects another address. The computer makes up to 10 attempts to find an available IP address.
* DHCP Scopes
  + Defines a set of IP addresses and associated configuration information that can be supplied to a DHCP client.
  + The IP addresses defined in a DHCP scope must be contiguous and are associated with a subnet mask.
    - If the addresses you want to assign are not contiguous, you must create a scope encompassing all the addresses you want to assign and then exclude specific addresses or address ranges from the scope.
    - You can create only one scope per subnet on a single DHCP server.
* DHCP Available Address Pool
  + Once a DHCP scope is defined and exclusion ranges are applied, the remaining addresses form what is called an available address pool within the scope.
  + Pooled addresses can then be dynamically assigned to DHCP clients on the network.
* DHCP Reservation
  + Network administrators can use DHCP reservations for DHCP-enabled hosts that need to have static IP addresses on your network.
  + Reservations must be created within a scope and must not be excluded from the scope.
  + An IP address is set aside, or reserved, for a specific network device that has the Media Access Control (MAC) address associated with that IP address.

Spanning Tree

* Spanning Tree Purpose
  + STP is IEEE 802.1D.
  + The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network.
  + Runs on bridges and switches.
  + Relieving Broadcast storms
* Spanning Tree
  + PVST+ - Cisco Proprietary adding VLAN features
  + RSTP – 802.1W improved – faster convergence – no VLANs
  + Rapid PVST+ - Cisco’s improvement with VLAN features
  + MSTP – Multiple Spanning Tree Protocol with all VLAN’s spanning networks
* Spanning Tree Process
  + Root Switch/Bridge Selection
    - What device is authoritative for this topology?
      * Election process – Communicating between all switches and can take around 45 seconds.
  + Looks at Priority between 0-65536, multiples of 4096, default is 32768
  + Plan based on MAC address, think of VLANs, turn off on ports never planned to use STP, and physical locations
  + Lowest Path Cost Selection
    - What is the best path to forward frames throughout the topology?
* Port Roles – Active States
  + Port Role Selection
    - What role should each port on the device perform?
  + Blocked Port
    - Startup – Forward no traffic
  + Designated Port
    - Forwards all packets
  + Root Port
    - Shortest path to root switch
    - Forwards all packets
  + In Blocking State, each switch will receive any STP BPDUs and frames associated with other network management messages. Will only respond to network mgmt frames.
  + In Listening state, each switch will continue to listen to the same frames that it did in Blocking state AND will also forward STP Root BPDUs. It will still not forward any data frames, and no MAC addresses are learned for the MAC/ARP tables
  + Timers – delay timer (20 sec), forwarding timer (15 sec : How long each interface will remain in Listening or Learning state)
* Timers
  + Normal MAC Address Table life
    - 5 minutes (per entry)
  + STP Hello Timer
    - 2 seconds [How often Root Port sends hello message]
  + Max Age Timer
    - 20 seconds [How long to keep ports Blocking before transition]
  + Forward Delay Timer
    - 15 seconds [How long to keep ports Listening/Learning before transition]
* STP Frame Format
  + 
  + When a switch has first booted, the RootBID and BID will be identical…because that’s the only info the switch currently knows. Additionally, the port that this frame will be sent out has the portID set
* STP Convergence
  + Topology may not be static
  + Notification when topology changes
  + Recalculation of STP only when a better path is received.
* Problems with STP
  + Very slow convergence
    - 30 seconds before ports become active
  + Lacks reliability
    - It’s a Data Link Layer protocol
  + Doesn’t consider actual physical topology
  + Where’s the security?
* Rapid STP (802.1w 🡪 802.1D - 2004)
  + Election process is the same as STP
  + Backwards compatible with STP
    - RSTP sets Version Field to 2
  + Defines new Port Roles
    - Edge Ports – edge of the broadcast domain uses PortFast with Cisco
    - Backup
    - Alternate
  + Greatly improves on convergence times (typically ~10sec)
    - Generation of BPDUs every <hello interval>
    - Accepts “inferior” Root BPDUs
    - Rapid transition based on physical interface feedback
  + The whole point of the listening/learning states is to determine if a loop is present.
  + By understanding the physical connections and monitoring their role, we can make some assumptions about how quickly the network can converge. Cisco PortFast is more or less included in the IEEE standard for RSTP.
  + Hello BPDUs are sent regardless of them being received. 802.1D mostly retransmits BPDUs from the root. Now treated as “keepalives”. More chatty now. Port info is now invalid after 3x <hello> vs Max Age of STP. Also, Blocking ports will also send BPDUs now.
  + “Inferior” BPDUs are now accepted because of the assumption that it will only be received if a failure has occurred. Even if a TCN BPDU hasn’t been received, it will apply the new root ID.
* RSTP vs STP
  + 
  + DP – forwarding
  + RP – Path cost determined-
  + AP – Alternate port best alternate path.
  + Backup Port – if DP fails it takes over
* Benefits of RSTP
  + Minimizes effects of switching loops
  + Faster Convergence
    - New Port Roles & States
    - “Handshake” process
  + Backwards compatible with 802.1D (STP)
  + Improved treatment of host devices
* STP Problems?
  + So, we now have Multiple Spanning Tree
    - MST (802.1s  802.1Q-2003  802.1Q-2005)
    - Uses the RSTP convergence algorithm
    - Maintains a minimum number of spanning tree instances for the VLANs present on the network
  + First, there are hosts connected to them. Second, they are VLANed networks…not all ports on a switch are members of the same VLAN. Should these ports be part of the same L2 network topology (from STPs perspective) if that is not the actual network architecture?
  + If there are 100 VLANs in the triangle network we looked at earlier, but they are not all used over all the links, does it make sense to have the same STP topology when there is a different logical topology?
  + Does it make sense to have 100 spanning tree topologies when many of the VLANs have identical logical topologies? So, MST uses the fewest number of spanning trees that addresses all of the logical topologies present.
* Per-VLAN Spanning Tree (PVST)
  + Operationally similar to 802.1D, PVST allows one spanning tree instance per VLAN
    - Can configure different roots per VLAN
    - A trunk port could be forwarding in one VLAN and blocking in another
    - Cisco proprietary
    - PVST only supports ISL links; PVST+ adds support for 802.1Q links
  + There is a 1-to-1 relationship between the number of VLANs and the number of spanning tree instances
* Rapid PVST and PVST+
  + Combines the RPST and PVST protocols
  + Cisco proprietary
  + One spanning tree instance per VLAN with enhancements to ensure rapid recovery after a failure
* Spanning Tree Best Practices
  + Run spanning tree
  + Understand the physical topology and know how spanning tree is operating
  + Manually configure the root bridge
    - Think about and purposefully choose the root bridge
    - Use a capable device
    - Physically connect the root bridge to the gateway for the network segment
* Identifying Switching Problems
  + show processes cpu history
    - % per sec (over last 60 seconds)
    - % per min (over last 60 minutes)
    - % per hour (over last 72 hours)
  + show int g0/33 | include minutes
    - Gives I/O bps and pps for last 5 minutes
    - Useful for attempting to identify the port generating traffic
  + show mac-address-table
  + show spanning-tree (summary)
    - Assumes you have spanning tree enabled

TCP/UDP

* Transportation Layer Protocols
  + Three Layer 4 protocols in current TCP/IP
  + TCP: Transmission Control Protocol
    - Connection oriented, reliable
  + UDP: User Datagram
    - Connection less, not reliable
  + SCTP: Stream Control Transmission Protocol
    - New protocol designed to offer reliable transmission over connectionless network
* TCP
  + Provides a reliable host-to-host connection
  + Includes controls for initiation, basic prioritization, flow control, congestion avoidance, and termination of connection
  + Many revisions to TCP exist, including:
    - Slow Start
    - Reno
    - Tahoe
    - Vegas
    - Compound TCP
    - BIC/CUBIC
* TCP Header Format
  + 
* 
* Well Known Port Numbers (IANA)
  + 
* TCP Header Fields
  + Sequence Number – The identifier of this segment being transmitted
  + Acknowledgement Number – The value of the next sequence number expected to be received
  + Data Offset – The number of 32-bit words in the TCP header
    - This indicates where the data begins
  + Control Fields (1 bit each)
    - URG - Urgent pointer valid flag, when set, priority data transfer feature will be invoked.
    - ACK - Acknowledgment number valid flag.
    - PSH - Push flag, when data, data will be immediately pushed to the application on the receiving device
    - RST - Reset connection flag.
    - SYN - Synchronize sequence numbers flag.
    - FIN - End of data flag.
  + Window - The number of data bytes beginning with the one indicated in the ACK # field that this device is able to accept
  + Checksum – A 16-bit one's complement of the one's complement sum of segment
* If ACK is not received by the time Recv timeout occurs, then message is considered LOST. The cause is assumed to be network congestion. Action – window size is decreased by half.
* TCP States
  + >netstat -a
* UDP
  + Provides minimal capabilities to deliver segments to a given destination
    - Not a reliable delivery mechanism
    - Lacks nearly all of the robust mechanisms used in TCP
* UDP Header Format
  + 
* UDP Header Fields
  + Length – The entire length of the segment
  + Checksum – A 16-bit one's complement of the one's complement sum of entire segment
  + Based on this, what can UDP not do?

NAT/PAT

* Network Address Translation
  + NAT – RFC 1631 (1994)
    - RFC 2663 (1999)
  + 2 major drivers
    - IP Address Depletion
    - Scaling of Routing Tables
  + NAT allows hosts in a private network to use a different IP address to access hosts &/or services on an external network
    - Potential use of private IP addressing
    - Reduces the need for globally unique IP addresses for an individual organization
* NAT Functionality
  + 1 or more public IP addresses assigned to a routing device and multiple internal clients utilizing private IP addressing
  + 2 major approaches (A.K.A. masquerading)
    - NAT
    - PAT/NAPT/NAT Overloading
  + This can be applied on the source address or the destination address
    - DNAT: Change Destination address
    - SNAT: Change Source address (port forwarding)
    - DNAT and SNAT can also mean dynamic NAT and static NAT
* NAT Terminology
  + Inside Local Address:
    - An RFC 1918 address assigned to a host on an inside network.
  + Inside Global Address:
    - A valid public address that the host on the inside network is assigned as it exits the router.
  + Outside Global Address:
    - A reachable IP address assigned to a host on the Internet.
  + Outside Local Address:
    - A local address assigned to a host on an outside network.
    - (Use beyond the scope of this course).
* NAT Operations
  + 1 internal host can utilize 1 external address
    - Modifies the source (potentially destination) IP address
    - Making this a 1:1 mapping
    - If you only have one external address configured on the NAT device…What happens?
  + Is this limiting?
* Port Address Translation (PAT) Operations
  + 1 internal host can utilize 1 external address
    - Still utilizes a defined external address
    - Enhances NAT with additional addressing (ports)
    - Making this approach 1: many
  + Same limitations?
* Port Forwarding
  + Typically done at the destination network’s gateway
  + Translates one destination port to another
    - Occasionally changes destination IP too
  + Processing overhead!
* Drawbacks of NAT
  + Added complexity in the network
  + Additional overhead to manage on the NAT device
  + Breaks the end-to-end functionality of IP
    - Discuss
  + Complicates Tunneling Protocols
    - Checksum violations
  + Requires a forwarder for any internal services
* Items to consider
  + NAT is NOT a security protocol
  + Don’t be fooled into thinking that it will protect your network
    - Use it in conjunction with a firewall for any security application
  + You can mitigate some of the drawbacks of NAT with:
    - STUN – Simple Traversal of UDP through NAT
    - ICE – Interactive Connectivity Establishment
    - TURN – Traversal Using Relay NAT