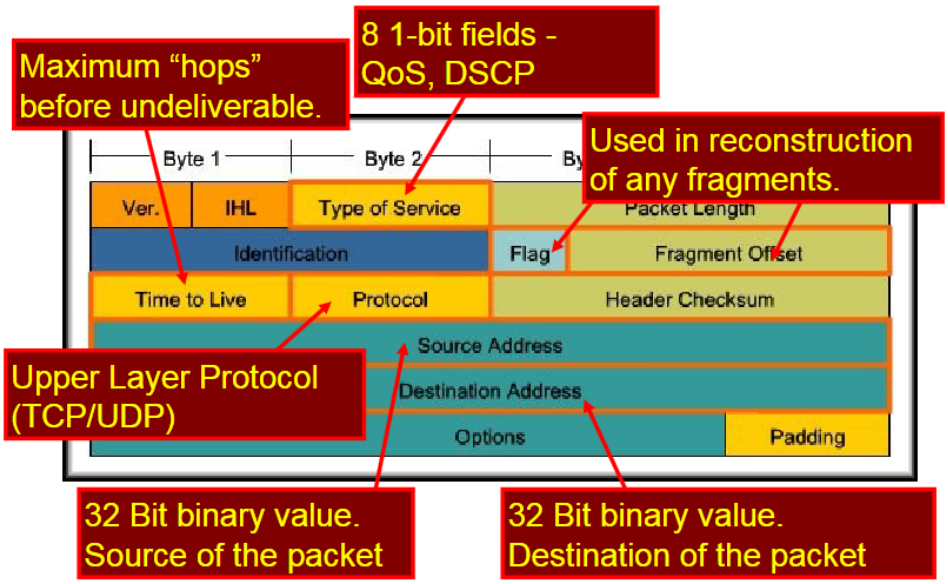
The Network Layer

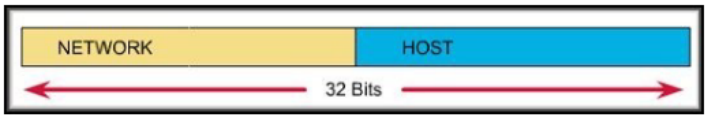
- Network Layer
  - Addresses packets with an IP address
  - Encapsulates the packet
  - Routes the packet to the destination
  - Decapsulates the packet
- IPV4 Characteristics
  - Connectionless
    - The sender doesn't know
      - If the receiver is present
      - If the packet arrived
      - If 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



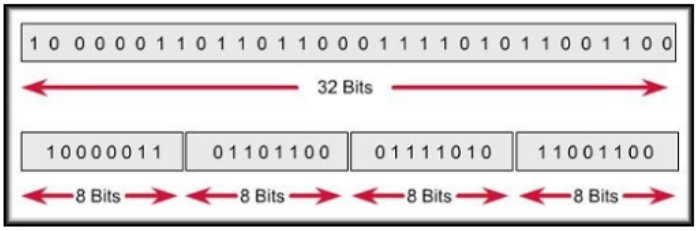
- Why separate hosts into networks?
  - Performance

Security

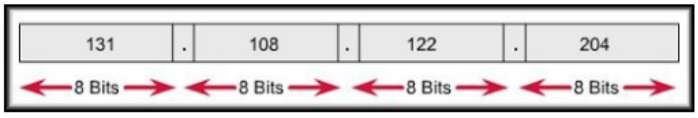
  - Address management
- Hierarchical addressing
  - IP addresses are divided into a 2-level hierarchy – Network and Host
- Dividing networks from networks



IP Version 4 addresses are **32** bits in length.



Divided into four separate groups of 8 bits each – 4 Octets.



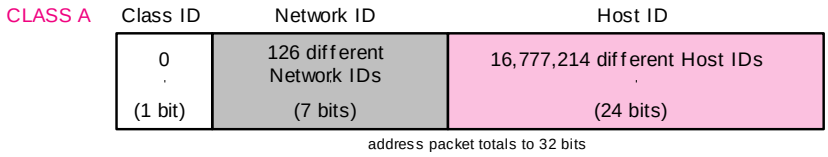
  - Convert from binary to decimal – **Dotted Decimal Notation**.
  - An IP Version 4 address has two parts:
    - Network number
    - Host number

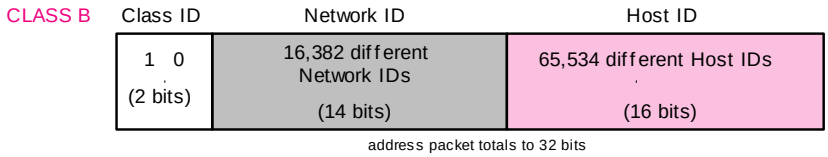
        - The network portion of the address is the same for all hosts on the network.
        - Each device is identified by a unique host portion.
    - This hierarchy means that routers only need to know the network portion – not the address of each individual host.
    - There is a direct relationship, bit 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.

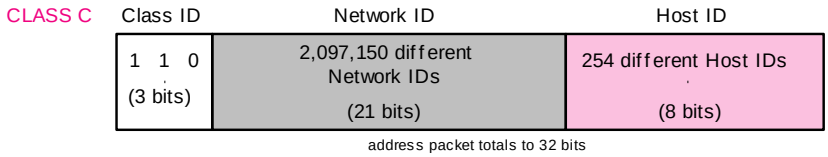
    - Remote networks are networks not directly connected to the router (manual configuration or learned dynamically).
- Address Resolution
    - The process of mapping a hardware address to a higher-layer protocol address
    - Address Resolution Protocol
        - Maps IPv4 address to a specific MAC address
        - 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?





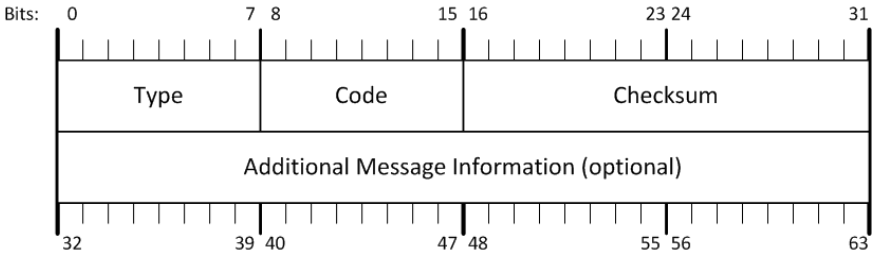


    -
- Subnetwork mask

    - 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

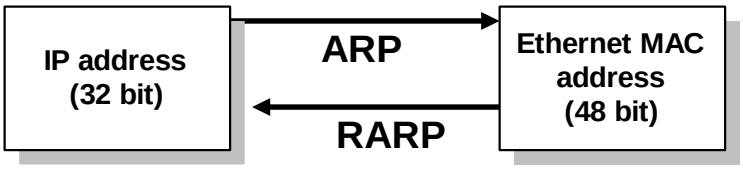
- Internet Control Message Protocol (ICMP)
  - Defined in RFC 792 (Sept. 1981)
    - What was RFC 791?
    - Has been largely unchanged since that time
  - Offers "messages" to provide feedback about network operations and delivery of datagrams
    - Does not make IP reliable
    - Uses IP for delivery 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

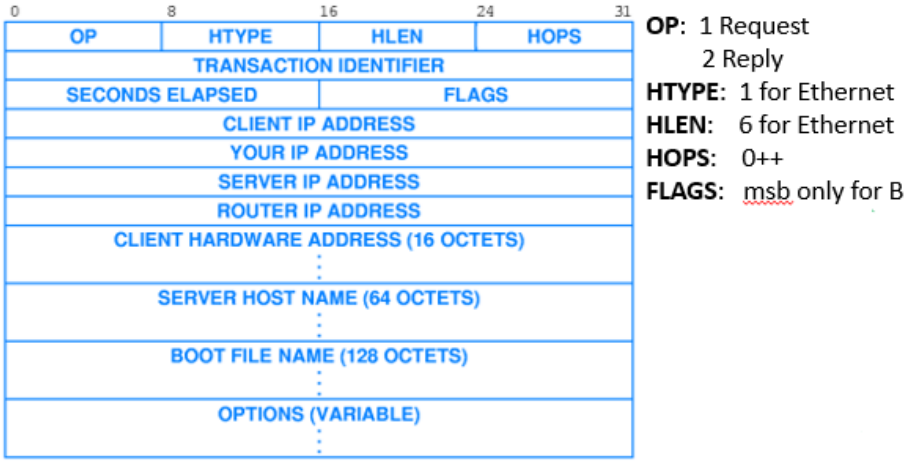
- ICMP Message Types
  - 0 – Echo Reply
  - 3 – Destination Unreachable
  - 4 – Source Quench
  - 5 – Redirect
  - 8 – Echo Request
  - 9 – Router Advertisement
  - 10 – Router Solicitation
  - 11 – Time Exceeded
  - 12 – Parameter Problem
  - 30 – Traceroute
  - Message types 1, 2, and 7 are undefined
  - 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
    - 

    OP: 1 Request
    2 Reply
    HTYPE: 1 for Ethernet
    HLEN: 6 for Ethernet
    HOPS: 0++
    FLAGS: msb only for B
- DHCP Message Type

TYPE FIELD	DHCP MESSAGE Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE
8	DHCPINFORM

- 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.

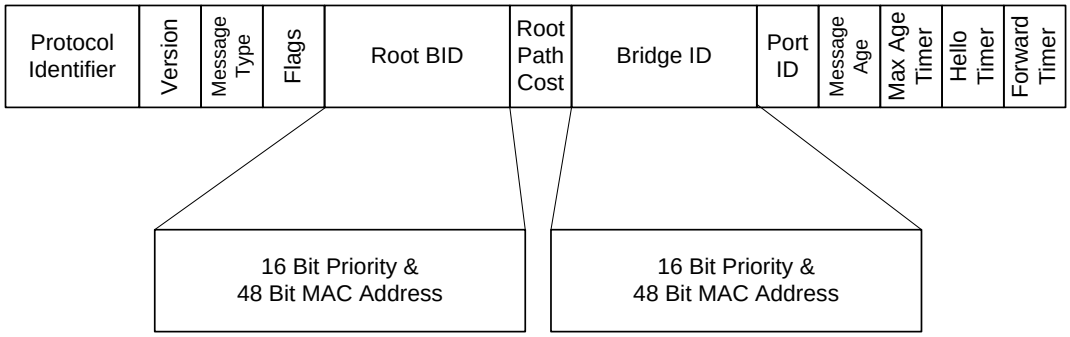
        - If the addresses you want to assign are not contiguous, you must create a scope encompassing all the addresses you want to assign and then exclude specific addresses or address ranges from the scope.
        - You can create only one scope per subnet on a single DHCP server.
- DHCP Available Address 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

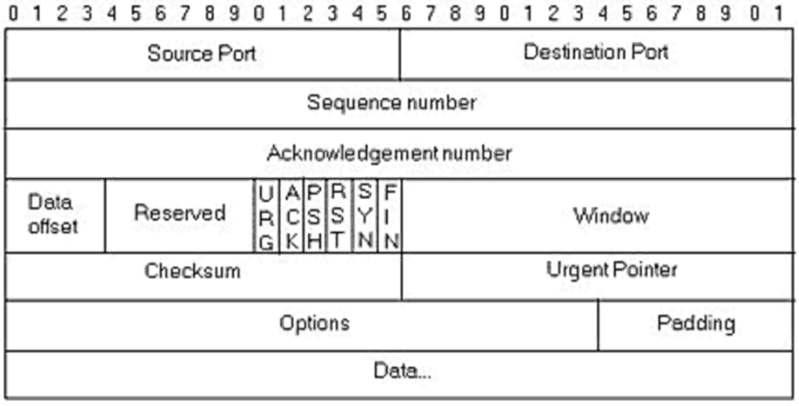
STP State	RSTP State	Port included in RSTP Topology	Port Learns MAC Addresses
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

  - 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

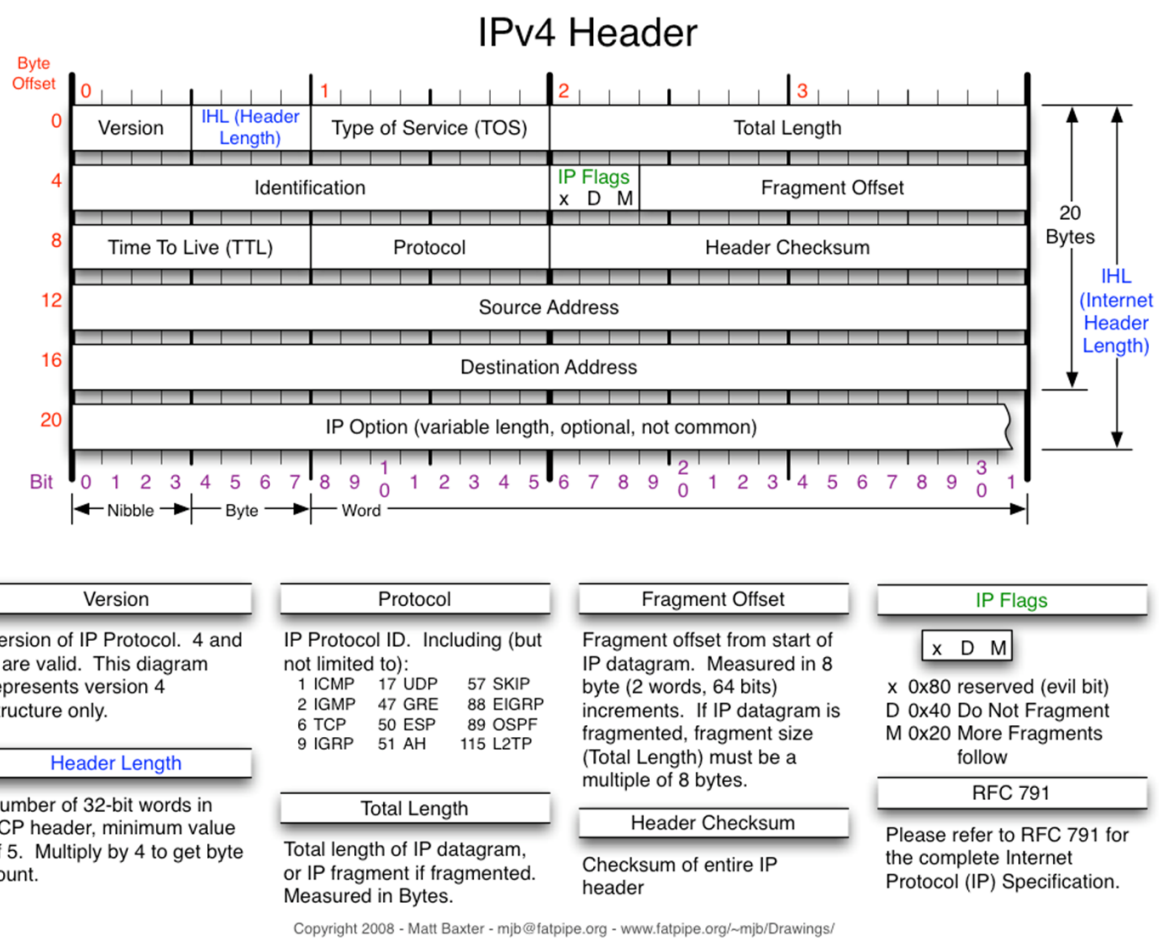
        - "Handshake" process
    - Backwards compatible with 802.1D (STP)
    - Improved treatment of host devices
- STP Problems?
    - So, we now have Multiple Spanning Tree
        - MST (802.1s 802.1Q-2003 802.1Q-2005)
        - Uses the RSTP convergence algorithm
        - Maintains a minimum number of 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
  - 

TCP Header

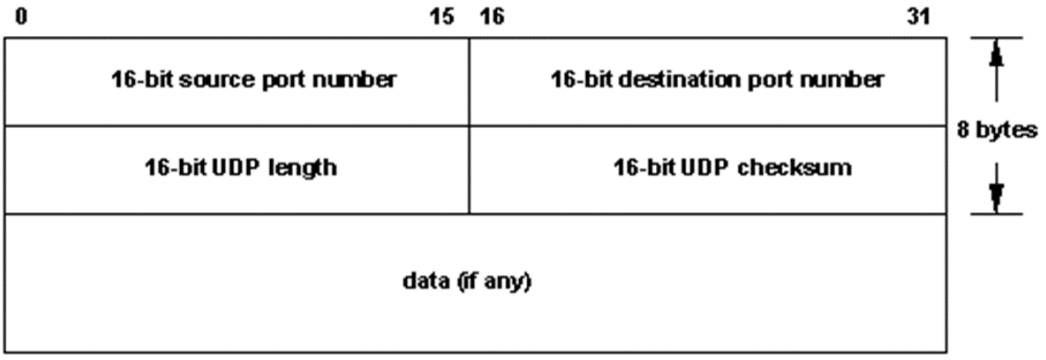


-
- Well Known Port Numbers (IANA)

Port	*Protocol*	*UDP*	*TCP*	*Description*
7	Echo	√		Echoes back a received datagram
9	Discard	√		Discards any datagram that is received
11	Users	√	√	Active users
13	Daytime	√	√	Returns the date and the time
17	Quote	√	√	Returns a quote of the day
19	Chargen	√	√	Returns a string of characters
20, 21	FTP		√	File Transfer Protocol
23	TELNET		√	Terminal Network
25	SMTP		√	Simple Mail Transfer Protocol
53	DNS	√	√	Domain Name Service
67	DHCP	√	√	Dynamic Host Configuration Protocol
69	TFTP	√		Trivial File Transfer Protocol
80	HTTP		√	Hypertext Transfer Protocol
111	RPC	√	√	Remote Procedure Call
123	NTP	√	√	Network Time Protocol
161, 162	SNMP		√	Simple Network Management Protocol

  -
- 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

Routing Operations & Processes

- The first router: Interface Message Processor
- Router Functionality
    - Network device that operates primarily at OSI layers 1 through 3
        - Able to function at all 7 layers if necessary
    - Identifies paths through the network(s) based on Layer 3 addresses
- Router Function: Physical Connectivity
    - Interfaces - Physical I/O ports
        - Define the physical communication medium, framing (or cell format), and appropriate connection
        - May support sub-interfaces
    - Configuration
        - Port number
        - Transmission technology
        - Bandwidth
        - Protocols supported
- Router Function: Logical Connectivity
    - Utilizes the Configuration provided by the Physical Connectivity
    - Learn Network Topology via Logical Connectivity
    - Routing Table

        - Correlation of port number (interface) with L3 address that is reachable via that interface
        - Typically, in RAM
    - Default Route
        - Associates a physical/logical interface with all unknown Layer 3 destinations
        - Used to minimize routing tables
- Routing Table Principles
    - Every router makes its decision alone, based on the information it has in its own routing table.
    - The fact that one router has certain information in its routing table does not mean that other routers have the same information.
    - Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.
        - Packets may traverse the network using one path and return through another path
        - Packets will be dropped if the path is unknown
- The Routing Process
    - Gateway is accessed by clients via transmitted frames
        - Client = Src MAC addr, Gateway = Dest MAC addr
    - Gateway receives L2 frames, check if Dest MAC addr = MAC of its interface
    - Gateway Interrogates packet header for Destination IP
        - Src IP = originating client; dest IP = Destination IP address
    - Gateway makes routing decisions based upon destination IP and routing table (statically configured, routing protocols and etc).
    - If entry is found, forward to the next hop, reconstruct L2 frame, else packet is dropped.
        - New Src MAC = MAC of this router's outgoing interface
        - New Dest MAC = MAC of the next hop
- Route Calculation & Maintenance
    - Identify potential routes to destination networks/hosts
    - Determine the best(?) path to each destination
        - Distance Vector – Primarily utilizes measure of distance (Hop Count)
            - RIP: best route is the path contains least amount of the routers (or hop count)
        - Link State – Utilizes a variety of link status information. Path is determined by factors include: Cost, Reliability, Capacity, Load, Delay, and etc.
            - OSPF: Open Shortest Path First (often minimum cost)
- Route Types
    - Connected
        - A path to a network that has a direct connection to the gateway
    - Static
        - A manually specified path to a destination network
    - Default
        - A path to a "helper" when the exact path to the network is not known
    - Dynamic

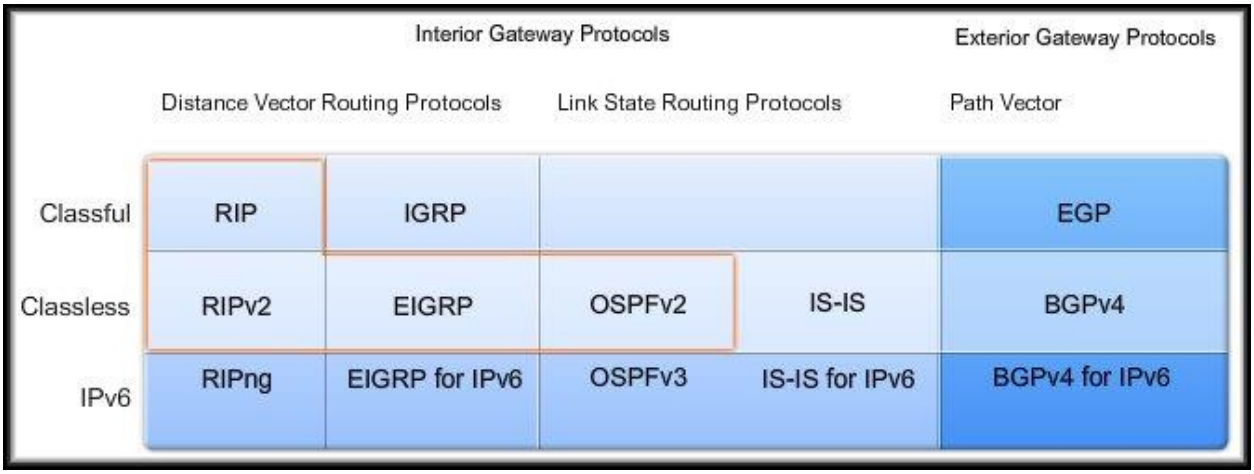
        - A path that is gained via a routing protocol that provides the path to a remote destination network
- Inter-Router Communication
    - Since not all destination networks are known by all devices in a network, there must be a mechanism to share this information
    - An agreed upon communications mechanism is required for each device attempting to learn &/or share information
    - When & How this communication is accomplished are the major differentiators between routing protocols
        - We use metrics as the primary term for distinguishing the best path from the current location to the desired destination
- Routing vs Routing Protocols
    - Routing is the process of forwarding the packets to the correct destination network
    - Longest Match Algorithm
        - The process of selecting the most specific entry in the routing table that matches the destination address
    - Routing Protocols
        - Establish efficient "paths" to a specific destination (network or host)
        - Defines preferential "path" utilization via metrics
        - Converge – The process by which all routers in a network agree upon that network's topology
        - Do NOT forward data packets
- A Packet Arrives…
    - Longest Prefix Match is applied because route entries will be much less if you specify rules for bigger networks and make exceptions to smaller networks.
    - Destination address of 10.23.128.1
        - 10.23.128.0/19 .10000000.00000000
        - 10.23.128.1/32 .10000000.00000001
        - 10.23.128.2/32 .10000000.00000010
    - Destination address of 10.23.128.3
        - 10.23.128.0/19 .10000000.00000000
        - 10.23.128.1/32 .10000000.00000001
        - 10.23.128.2/32 .10000000.00000010

Static Routing

- Devices on Directly Connected Networks
    - When a router only has its interfaces configured, and the routing table contains the directly connected networks but no other routes, only devices on those directly connected networks are reachable.
- Purpose and Command Syntax (ip route)
    - Static routes are commonly used when routing from a stub network.
    - Stub Network: A network accessed by a single route.

- Summary Static Routes
    - Route Summarization/Aggregation:
        - A summary route is a single route that can be used to represent multiple routes.
            - Generally a set of contiguous networks.
            - Have the same exit interface or next-hop IP address.
            - Creates smaller routing tables
            - More efficient routing table lookup process.
- Default Static Routes
    - A default route is a static route that is used when there are no routes that have a specific match to the destination network.
    - Default routes are used:
        - When a router has only one other router to which it is connected. This condition is known as a stub router.
    - ip route 0.0.0.0 0.0.0.0
        - [ip address | interface]
- Ethernet Interfaces Participate in ARP
    - A router's Ethernet interface participates in a LAN network just like any other device on that network.
    - This means that these interfaces:
        - Have Layer 2 MAC address.
        - Are recorded in a device's ARP Cache.
        - Issue ARP Requests when needed.
        - Issue ARP Replies when required.
- Examining Serial Interfaces (In the Lab)
    - The physical link between R1 and R2 is up.
        - Both ends have been configured correctly with:
            - An IP Address and Subnet Mask
            - The no shutdown command has been issued.
    - The line protocol is still down.
        - The serial interface is not receiving a clock signal.
        - Issue the clock rate command, on the router with the DCE cable.
    - The show controllers command is useful in determining the DTE/DCE status of a serial link without having to physically check the cables.
        - If the cable connected to the router is listed as DCE, then the clock rate command must be issued for the interface.
    - If a DTE interface is configured with the clock rate command, the IOS disregards it.

Dynamic Routing

- 

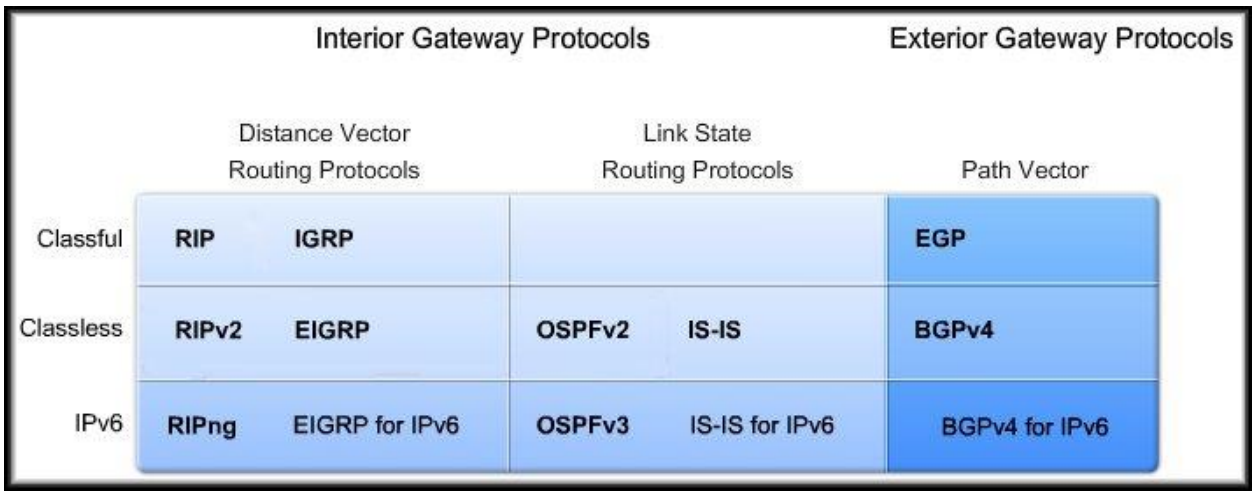
- Role of Dynamic Routing Protocol
  - Exchange of routing information between routers.
  - Dynamically learn information about remote networks and add routes to routing tables.
  - Determines the best path to each network.
  - Automatically finds alternate paths if needed.
  - Advantages over Static Routes:
    - Less administrative overhead.
    - Scales better.
    - Less prone to configuration errors.
- Network Discovery and Routing Table
  - Components of Dynamic Routing Protocols:
    - Data Structures:
      - Tables or databases for their operations, kept in RAM.
    - Algorithm:
      - An algorithm is a finite list of steps used in accomplishing a task.
      - Used for processing routing information and for best-path determination.
    - Routing Protocol Messages:
      - Discover neighboring routers.
      - Exchange, learn and maintain accurate network routing information.
- Distance Vector and Link State
  - Distance Vector:
    - Routes are advertised as vectors of distance and direction.
      - Distance:
        - Is defined in terms of a metric.
          - Hop Count: The number of routers between the source and destination networks.
      - Direction:
        - Is simply the next-hop router or exit interface.
    - Routing updates usually consist of periodic updates of the entire routing table.
      - (e.g.. Routing Information Protocol - RIP – every 30 seconds)
  - Distance Vector:

        - The network is simple and flat and does not require a hierarchical design.
        - The administrators do not have enough knowledge to configure and troubleshoot link-state protocols.
        - Worst-case convergence times in a network are not a concern.
    - Link State:
        - A Link State routing protocol can create a complete map of the network topology.
        - A link-state router:
            - Receives an update.
            - Builds a topology database.
            - Uses a Shortest Path First (SPF) algorithm to create its view of the network.
            - Builds the routing table.
        - Routing updates (not the entire table) are only sent to neighbouring routers when the topology changes.
            - (e.g.. Open Shortest Path First - OSPF)
    - Link State:
        - The network design is hierarchical, usually occurring in large networks.
        - The administrators have a good knowledge of the implemented link-state routing protocol.
        - Fast convergence of the network is crucial.
- Dynamic Routing Protocols and Convergence
    - Convergence:
        - The network has converged when all routers have complete and accurate information about the network.
        - The speed of convergence is an important characteristic of a network.
        - Convergence:
            - Generally:
                - Slower Convergence: RIP
                - Faster Convergence: EIGRP and OSPF
- Purpose of a Metric
    - There are times when a router will have multiple paths to the same destination.
    - Metrics are a way to measure and/or compare routes to determine which route is the best path.
    - The route chosen will depend on two things:
        - The routing protocol in use.
        - The metric used by the routing protocol.
- Metrics and Routing Protocols
    - Routing Information Protocol (RIP):
        - Uses hop count as its metric. Lower is better.
    - Open Shortest Path First (OSPF):
        - Uses bandwidth as its metric. Faster is better.
    - The routing table displays the metric for each dynamic and static route.
        - Dynamic routes with the lowest metric are installed by routing protocols.

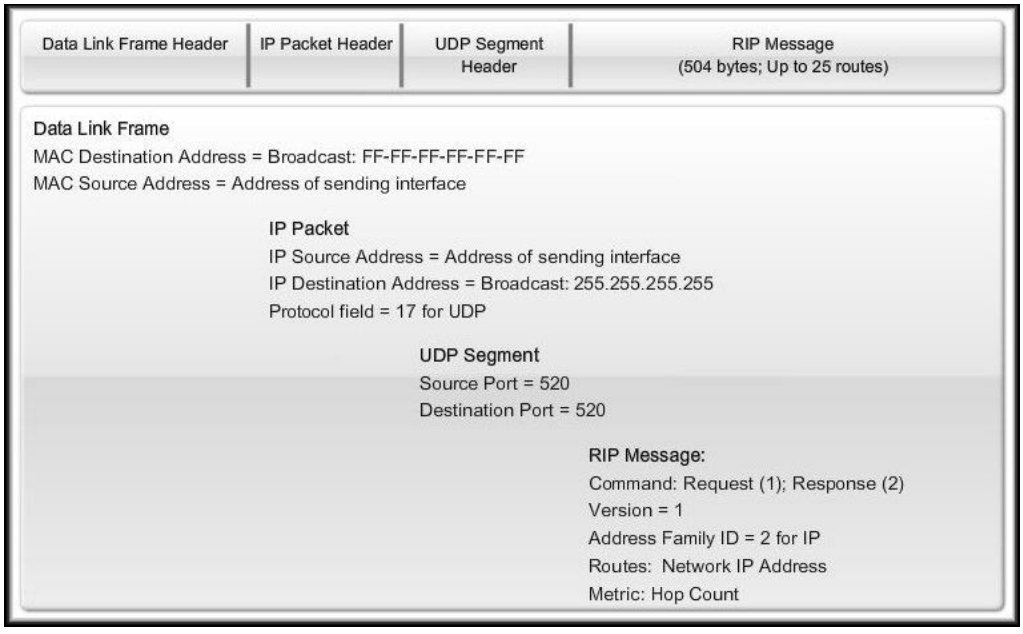
        - Static routes always have a metric of 0.
- Purpose of Administrative Distance (AD)
    - Administrative Distance is used to determine which route is to be installed in the routing table.
    - The route that has the lower AD will be preferred over the route with the higher AD and will be added to the routing table.
    - The term trustworthy is commonly used when defining administrative distance.
        - The lower the administrative distance value, the more "trustworthy" the route.

Distance Vector and Routing Information Protocol

- Meaning of Distance Vector
    - The routing protocol does not know the entire topology of a network.
    - It only knows the routing information received from its neighbors.
    - A Distance Vector routing protocol does not have the knowledge of the entire path to a destination network.
- Distance-Vector Routing
    - In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors. The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet. We can say that in distance-vector routing, a router continuously tells all of its neighbors what it knows about the whole internet (although the knowledge can be incomplete).
- Cold Start
    - When a router powers up:
        - Knows nothing about the network topology.
        - Knows only the information saved in NVRAM.
        - Sends updates about its known networks out all ports.
- Convergence
    - The amount of time it takes for a network to converge is directly proportional to the size of that network.
    - Routing protocols are compared based on how fast they can propagate this information - their speed to convergence.
    - A network is not completely operable until it has converged.
        - Network administrators prefer routing protocols with shorter convergence times.



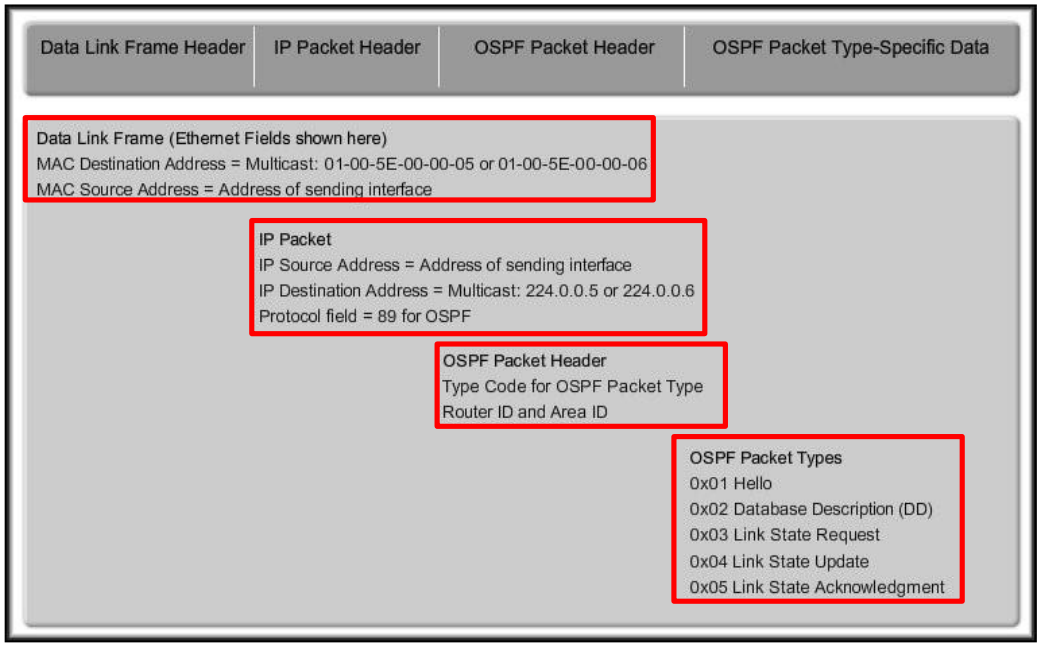
- Background and Perspective
  - RIP evolved from the Xerox Network System (NS) in the late 1970's.
  - In 1988, it was standardized under RFC 1058.
    - Still in use today, not a protocol "Rest In Peace"
    - Help understand fundamental concepts and comparisons of protocols such as classful (RIPv1) and classless (RIPv2).
    - An IPv6 form of RIP called RIPng (next generation) is now available..
- RIPv1 Characteristics and Message Format
  - RIP Characteristics:
  - Distance vector routing protocol.
  - Uses hop count as its only metric for path selection.
  - Advertised routes with hop counts greater than 15 are considered unreachable.
  - Routing Table Updates:
    - RIPv1: Broadcast every 30 seconds.
    - RIPv2: Multicast every 30 seconds.



- RIPv1 Limitations
  - RIPv1 (a classful routing protocol) is used as an example, so we can see how RIPv2 (a classless routing protocol) does not have these same limitations.
  - Classful routing protocols have three major limitations:
    - Does not support discontiguous networks.
    - Does not support VLSM.
    - Does not support CIDR.
  - RIPv1 is a CLASSFUL routing protocol and does not include the subnet mask
- RIPv1 Limitations - Discontiguous Networks
  - Solution:
    - Use RIPv2 to include the subnet mask.
    - Turn off auto summarization.
  - How do we do that?
    -
```
R2>en
R2#conf t
R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#no auto-summary

R2(config-router)#
```
- Verifying and Troubleshooting RIPv2
  - Begin with the basics:
    - Make sure all of the links (interfaces) are up and operational.
    - Check the cabling.
    - Check to make sure you have the correct IP address and subnet mask on each interface.
    - Remove any unnecessary configuration commands that are no longer necessary or have been replaced by other commands.
- Common RIPv2 Issues:
  - Network Statements:
  - Incorrectly configured or missing network statements configured with the network command.
  - The network command does two things:
    - It enables the routing protocol to send and receive updates on any local interfaces that belong to that network.
    - It includes the configured network in its routing updates to its neighboring routers.
  - A missing or incorrect network statement will result in missed routing updates and routing updates not being sent or received on an interface.
- Link-State Routing Protocols
  - Distance Vector routing protocols are like road signs.
    - Routers must make preferred path decisions based on a distance or metric to a network.
  - Link-State routing protocols are more like a road map.

        - They create a topological map of the network and each router uses this map to determine the shortest path to each network.
- Link-State Routing Process
    - How does a link-state routing protocol work?
    - 5 Step Process:
        - Each router learns about its own directly connected networks.
        - Each router is responsible for contacting its neighbors on directly connected networks.
        - Each router builds a link-state packet (LSP) containing the state of each directly connected link.
        - Each router floods the LSP to all neighbors, who then store all LSPs received in a database.
        - Each router uses the LSPs to construct a database that is a complete map of the topology and computes the best path to each destination network.
    - Step 1: Directly Connected Networks
        - Step 1: Each router learns about its own directly connected networks.
            - When a router interface is configured with an IP address and subnet mask and activated, the interface becomes part of that network.
            - Regardless of the routing protocols used, these directly connected networks are now part of the routing table.
    - Step 2: Hello Packets
        - Step 2: Each router is responsible for contacting its neighbors on directly connected networks.
            - The router will not be aware of any neighbor routers on the link until it receives a Hello packet from that neighbor.
            - At that time, it establishes an adjacency with the neighboring router.
        - A neighbor is any other router that is enabled with the same link-state routing protocol.
        - These small Hello packets continue to be exchanged between two adjacent neighbors.
        - These packets serve as a keepalive function to monitor the state of the neighbor.
- Step 3: Build the Link-State Packet (LSP)
    - Step 3: Each router builds a link-state packet (LSP) containing the state of each directly connected link.
        - The LSP contains the link-state information about the sending router's links.
        - The router only sends LSPs out interfaces where it has established adjacencies with other routers.
- Step 4: Flooding Link-State Packets
    - Step 4: Each router floods the LSP to all neighbors, who then store all LSPs received in a database.
        - Whenever a router receives an LSP from a neighboring router, it immediately sends that LSP out all other interfaces, except the interface that received the LSP.
    - Link-state routing protocols calculate the SPF (Shortest Path First) algorithm after the flooding is complete.

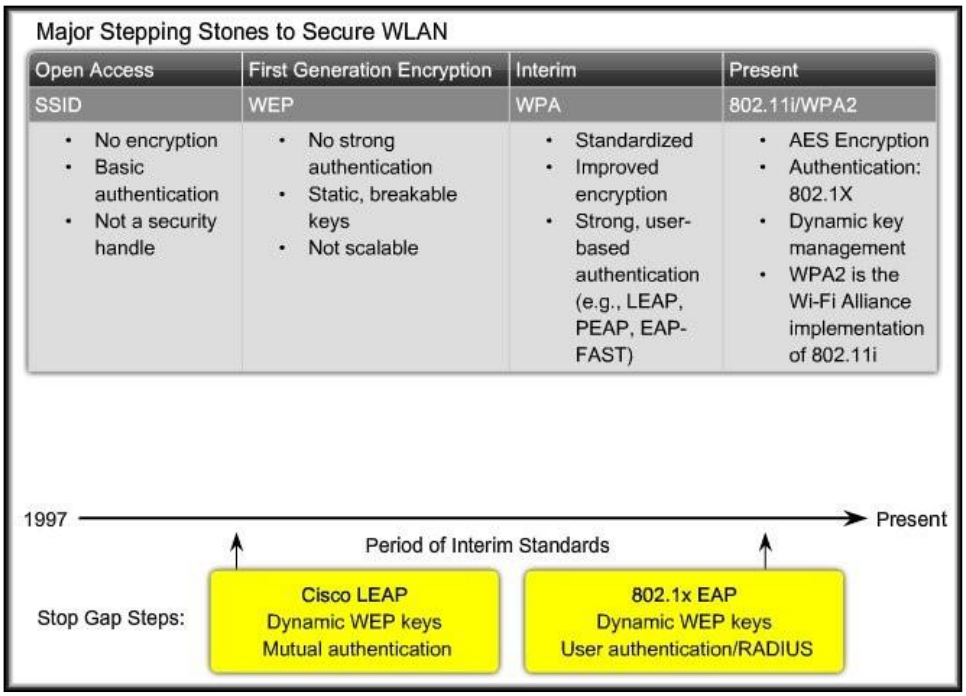
- As a result, link-state routing protocols reach convergence much faster than distance vector routing protocols.
- An LSP needs to be sent only:
  - During initial startup of the router or routing protocol.
  - Whenever there is a change in the topology (link going down or coming up) or a neighbor adjacency being established or broken.

- Step 5: Constructing a Link-State Database
  - Step 5: Each router uses the LSPs to construct a database that is a complete map of the topology and computes the best path to each destination network.
  - With a complete link-state database, R1 can now use the database and the shortest path first (SPF) algorithm to calculate the preferred path or shortest path to each network.
- Requirements: Link-State
  - More Memory because of the use of:
    - Link-state databases.
    - Creation of the SPF tree.
  - More CPU time because link-state protocols:
    - build a complete map of the topology.
  - The flooding of link-state packets can adversely affect the available bandwidth on a network.
    - This should only occur during initial startup of routers, but it can also be an issue on unstable networks.
- OSPF Message Encapsulation (Ethernet)
  - 

Wireless LAN

- Wireless LAN Security
  - Three Major Categories of Security Threats:

        - War Drivers:
            - War driving means driving around a neighborhood with a wireless laptop and looking for an unsecured 802.11b/g system.
        - Hackers/Crackers:
            - Malicious intruders who enter systems as criminals and steal data or deliberately harm systems.
        - Employees:
            - Set up and use Rogue Access Points without authorization. Either interfere with or compromise servers and files.
- Threats to Wireless Security
    - War Drivers:
        - "War driving" originally referred to using a scanning device to find cellular phone numbers to exploit.
        - War driving now also means driving around a neighborhood with a laptop and an 802.11b/g client card looking for an unsecured 802.11b/g system to exploit.
        - Software is readily available.
    - Man-in-the-Middle Attacks:
        - Attackers select a host as a target and position themselves logically between the target and the router of the target.
        - In a wired LAN, the attacker needs to be able to physically access the LAN to insert a device logically into the topology.
        - With a WLAN, the radio waves emitted by access points can provide the connection.
        - Because access points act like Ethernet hubs, each NIC in a BSS hears all the traffic.
        - Attackers can modify the NIC of their laptop with special software so that it accepts all traffic.
    - Denial of Service (DoS):
        - 802.11b/g WLANs use the unlicensed 2.4 GHz band.
        - This is the same band used by most baby monitors, cordless phones, and microwave ovens.
        - With these devices crowding the RF band, attackers can create noise on all the channels in the band with commonly available devices.
        - An attacker can turn a NIC into an access point.
        - The attacker, using a PC as an AP, can flood the BSS with clear-to-send (CTS) messages, which defeat the CSMA/CA function used by the stations.
        - The actual AP, floods the BSS with simultaneous traffic, causing a constant stream of collisions.
        - Another DoS attack that can be launched in a BSS is when an attacker sends a series of disassociate commands that cause all stations to disconnect.
        - When the stations are disconnected, they immediately try to reassociate, which creates a burst of traffic.
        - The attacker sends another disassociate and the cycle repeats itself.
- Wireless Security Protocols

- 

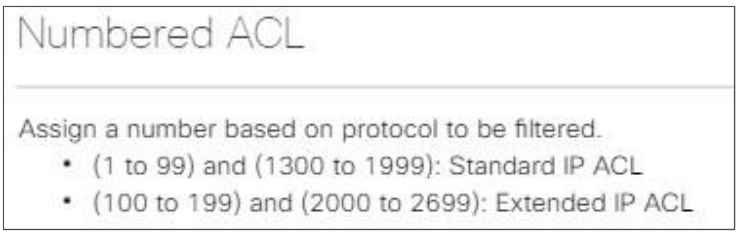
- Authenticating to the Wireless LAN
  - In an open network, such as a home network, association may be all that is required to grant a client access to devices and services on the WLAN.
  - In networks that have stricter security requirements, an additional authentication or login is required to grant clients such access.
  - This login process is managed by the Extensible Authentication Protocol (EAP).
- Wireless Encryption
  - Two Encryption Mechanisms:
  - 

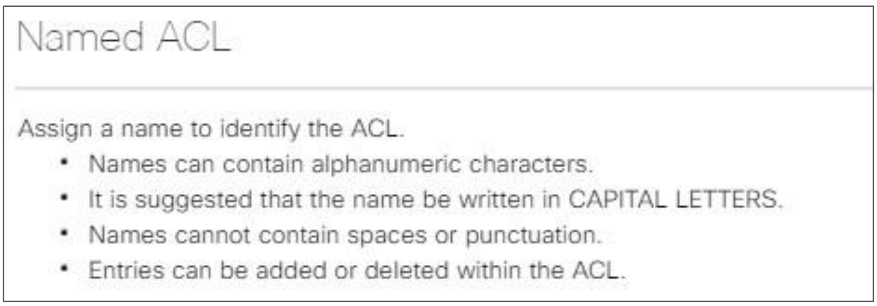
  - TKIP is the encryption method certified as Wi-Fi Protected Access (WPA).
    - Provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method.
    - Encrypts the Layer 2 payload.
    - Message integrity check (MIC) in the encrypted packet that helps ensure against a message tampering.
  - The AES encryption of WPA2 is the preferred method.
    - WLAN encryption standards used in IEEE 802.11i.
    - Same functions as TKIP.
    - Uses additional data from the MAC header that allows destination hosts to recognize if the non-encrypted bits have been tampered with.
    - Also adds a sequence number to the encrypted data header.

    - When you configure Linksys/TPLink access points or wireless routers you may not see WPA or WPA2.
        - Instead you may see references to something called pre-shared key (PSK).
    - Types of PSKs:
        - PSK or PSK2 with TKIP is the same as WPA.
        - PSK or PSK2 with AES is the same as WPA2.
        - PSK2, without an encryption method specified, is the same as WPA2.
- Controlling Access to the Wireless LAN
    - When controlling access, the concept of depth means having multiple solutions available.
        - Three step approach:
            - SSID cloaking:
                - Disable SSID broadcasts from access points.
            - MAC address filtering:
                - Tables are manually constructed on the access point to allow or disallow clients based on their physical hardware address.
            - WLAN Security:
                - Implement WPA or WPA2.
    - An additional consideration is to configure access points that are near outside walls of buildings to transmit on a lower power setting than other access points closer to the middle of the building.
    - This is to merely reduce the RF signature on the outside of the building.
        - Anyone running an application such as Netstumbler, Wireshark, or even Windows XP can map WLANs.
- Access Point Placement
    - A WLAN that just did not seem to perform like it should.
        - You keep losing association with an access point
        - Your data rates are much slower than they should be.
    - Some additional specific details:
        - Not mounted closer than 7.9 inches (20 cm) from the body of all persons.
        - Do not mount the access point within 3 feet (91.4 cm) of metal obstructions.
        - Install the access point away from microwave ovens.
        - Always mount the access point vertically..
        - Do not mount the access point outside of buildings.
        - Do not mount the access point on building perimeter walls, unless outside coverage is desired.
        - When mounting an access point in the corner of a right-angle hallway intersection, mount it at a 45-degree angle.
- Authentication and Encryption
    - The WLAN authentication and encryption problems you are most likely to encounter, and that you will be able to solve, are caused by incorrect client settings.
    - Remember, all devices connecting to an access point must use the same security type as the one configured on the access point.

ACL

- Access control list (ACL) consists of a table that tells an Operating System (OS) which access rights each user has to a particular system object, such as a file directory or individual file.
- ACLs are lists of conditions used to test network traffic that tries to travel across a router interface. These lists tell the router what types of packets to accept or deny. Acceptance and denial can be based on specified conditions. ACLs enable management of traffic and secure access to and from a network.
- How ACL executed
    - Made decisions by matching a condition statement in an access list and then performing the accept or reject action defined in the statement.
    - ACL statements operate in sequential, logical order
- ACL range for each protocol
Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099
    - Each ACL must have a unique identification number assigned to it. This number identifies the type of access list created and must fall within the specific range of numbers that is valid for that type of list.
- ACL Operation Overview
    - One ACL per protocol - To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
    - One ACL per direction - ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
    - One ACL per interface - ACLs control traffic for an interface, for example, GigabitEthernet 0/0.
- Types of IPv4 ACLs
    - Standard ACLs filter packets based on the source address only.
    - ```
      access-list 10 permit 192.168.30.0 0.0.0.255
      ```
    - Extended ACLs filter packets based on:
        - Protocol type / Protocol number (e.g., IP, ICMP, UDP, TCP, …)
        - ```
          access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
          ```
        - Source and destination IP addresses
        - Source and Destination TCP and UDP ports
    - Standard and extended ACLs can be created using either a number or a name to identify the ACL and its list of statements.





- ACL Operation Overview
  - Extended ACLs should be located as close as possible to the source of the traffic to be filtered.
    - Denies undesirable traffic close to the source network without crossing the network infrastructure.
  - Standard ACLs should be located as close to the destination as possible.
    - If a standard ACL was placed at the source of the traffic, it would filter traffic based on the given source address no matter where the traffic is destined.
- Types of IPv4 ACLs
  - An extended ACL will be configured to block all FTP and Telnet traffic from 192.168.11.0/24 going to 192.168.30.0/24.
  - The extended ACL should be applied closest to the source and therefore could be applied incoming on the R1 G0/1 interface.
    - Applying it outgoing on the R1 S0/0/1 interface would prevent reaching 192.168.31.0/24 but would also needlessly process packets from 192.168.10.0/24.
- Standard IPv4 ACL Implementation
  - The full syntax of the standard ACL command is as follows:
    - access-list ACL-# {deny | permit | remark} source [source-wildcard][log]
  - An IPv4 ACL is linked to an interface using the following interface configuration mode command:
    - ip access-group {ACL-# | access-list-name} {in | out}
  - Note:
    - To remove an ACL from an interface, first enter the no ip access-group command on the interface, and then enter the global no access-list command to remove the entire ACL.
  - To create a standard named ACL.
    - Use the ip access-list standard name global config command.
      - Names are alphanumeric, case sensitive, and must be unique.
      - The command enters standard named ACL configuration mode.

        - Use permit, deny, or remark statements.
        - Apply the ACL to an interface using the ip access-group name command.
- Structure of an Extended IPv4 ACLs
    - An application can be specified by configuring either:
        - The port number
        -
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```
        - The name of a well-known port.
        -
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```
    - Note:
        - Use the question mark (?) to see available well-known port names.
        - E.g., access-list 101 permit tcp any any eq ?
- Configure Extended IPv4 ACLs
    - Full syntax of the extended ACL:
        - access-list ACL-# {deny | permit | remark} protocol {source source-wildcard][operator [port-number | port-name]] {destination destination-wildcard][operator [port-number | port-name]]
    - Enhancement over standard ACL:
        - Support Layer 4 (port #)
        - Support Protocols
        - Support both source and destination
    - An extended ACL can be edited in one of two ways:
        - Method 1 Text editor
            - The ACL is copied and pasted into where the changes are made.
            - The current access list is removed using the no access-list command.
            - The modified ACL is then pasted back into the configuration.
        - Method 2 Sequence numbers
            - Sequence numbers can be used to delete or insert an ACL statement.
            - The ip access-list extended name command is used to enter named-ACL configuration mode.
            - If the ACL is numbered instead of named, the ACL number is used in the name parameter.
            - ACEs can be inserted or removed.