

Memory Components

ROM: Basic microcode for starting and maintaining device; POST, bootstrap, ROMMON, and RXBOOT.

(D)RAM: Stores running config, routing tables, ARP cache, and packet buffers. IOS loaded into RAM at boot to run.

NVRAM: Nonvolatile RAM: Random-access memory that keeps its contents intact while power is turned off. Contains startup-config.

Flash: Stores IOS.

Boot Sequence

Bootstrap program runs POST (Device finds hardware and performs hardware-checking routines).

Bootstrap checks configuration register, which specifies where to load the IOS.

Load/decompress IOS into RAM.

Load startup-config.

Configuration Register

Sh version

Lowest 4 bits make up boot field.

0x2102: Default. Loads IOS from flash memory and uses default startup-config.

0x2142: Password Recovery. Boots and ignores startup config. (Reboot -> break -> 0x2142 -> reboot -> enable -> copy start run -> change PW -> copy run start -> 0x2102 -> reboot).

0x###0: Boots into ROM Monitor mode (ROMMON).

0x###1: Boots into Mini-IOS (RXBOOT). Can connect to a TFTP server to download an IOS image to Flash memory.

0x###2-F: Use the image specified with the “boot system” command.

Cabling

Thinnet: Also called 10Base2. Bus network that uses a thin coax cable and runs Ethernet media access up to 185 meters.

Thicknet: Also called 10Base5. Bus network that uses a thick coaxial cable and runs Ethernet up to 500 meters.

10BASET: 10Mbps baseband. Uses two pairs of twisted-pair CAT 3, 4, or 5. One pair sends, the other receives. 100 meters.

100BASET: 100Mbps baseband Fast Ethernet, UTP wires.

100BASETX: 100Mbps baseband Fast Ethernet. Uses two pairs of UTP or STP wires. One pair sends, the other receives. 100 meters.

Synchronous Optical Networking (SONET): Standardized protocol that transfers multiple digital bit streams over optical fiber using lasers or LEDs. Immune to EMI, has longer range.

Fast Ethernet: Any Ethernet specification with a speed of 100Mbps. Fast Ethernet is 10 times faster than 10BaseT while retaining qualities such as MAC mechanisms, MTU, and frame format. These similarities make it possible for existing 10BaseT applications and management tools to be used on Fast Ethernet networks.

Crossover Cable: Swap pins 1 -> 3 and 2 -> 6.

Straight-Through Cable: Uses pins 1, 2, 3, and 6.

DoD vs. TCP/IP Stack

DoD	OSI
Process/ Application	Application
	Presentation
	Session
Host-to-Host	Transport
Internet	Network
Network Access	Data Link
	Physical

Internetwork: Any group of networks interconnected by routers and other mechanisms, typically operating as a single entity.

Physical Topology: How components are physically interconnected.

Logical Topology: How traffic actually flows through the network.

Broadcast (Multi-Access): Networks, such as Ethernet, which allow multiple devices to connect to, or access, the same network. Provides a broadcast ability in which a single packet is delivered to all nodes on the network.

Non-Broadcast Multi-Access (NBMA): Networks, such as Frame Relay, X.25, and ATM, which allow for multi-access but have no broadcast ability. NBMA networks require special OSPF configuration to function properly and neighbor relationships must be defined.

Address Resolution

ARP: IP -> MAC

RARP: MAC -> IP

IARP: Frame Relay DLCI -> IP

Gratuitous ARP: Used by hosts to ensure there are no conflicts with IP addresses assigned by DHCP.

Proxy ARP: Allows redundancy in case of a failure with the default gateway. An intermediate device, such as a router, answers ARP requests for addresses not on its own network with its own address. It then acts as a proxy and directs the traffic to the intended destination.

IPv4 Add: 32 bits.

IPv6 Add: 128 bits.

MAC Add: 48 bits, or 6 bytes.

IP Classes

Class A: 0 - 127 (Leading bit: 0).

Class B: 128 - 191 (Leading bits: 10).

Class C: 192 - 223 (Leading bits: 110).

Private IPs

Class A: 10.0.0.0 - 10.255.255.255

Class B: 172.16.0.0 - 172.31.255.255

Class C: 192.168.0.0 - 192.168.255.255

IPv6

Standard Stateless Autoconfiguration:

- IPv6 hosts can configure themselves automatically when connected to an IPv6 network by using Neighbor Discovery Protocol within ICMPv6 by means of router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet that contains network-layer configuration parameters.
- If IPv6 stateless address autoconfiguration is unsuitable for an application, a network may use stateful configuration with DHCPv6 or hosts may be configured statically.

IPv6 Routing Protocols: OSPFv3, EIGRP for IPv6, RIPng.

Anycast: A single IPv6 address assigned to multiple devices. Communication flow is one-to-nearest. Used as a way to provide high availability and load balancing (access to replicated data).

2000::/3 Global unicast: Publicly routable addresses.

FC00::/7 Unique local unicast: Allows communication throughout a site while being routable to local networks, but not out to the Internet.

FE80::/10 Link-local unicast: Intended only for communication within the network segment or a point-to-point connection that a host is connected to. Routers do not forward.

FF00::/8 Multicast: Packets addressed to these addresses are delivered to all interfaces tuned into the multicast address.

2002::/16 Used with 6to4 tunneling.

Summarization (Route Aggregation)

- Consolidation of publicized subnetwork addresses so that a single summary route is advertised to other areas by an area border router.
- Reduces the size of the routing table on routers to save memory.
- Once you find your block of networks, the network address is always the first address in the range, and the subnet mask tells you the block size in the interesting octet.

- If using a routing protocol that auto-summarizes (RIPv1 or EIGRP) it will send the subnet mask of the classful boundary, not the actual subnet mask. **no auto summary** will turn this feature off in RIP and EIGRP, and send the actual subnet mask (use with discontiguous networks). If using OSPF, not necessary because OSPF does not auto-summarize.

TCP

Full-duplex, sequenced, and reliable, but with high overhead.

Connection-Oriented: Three-way handshake: SYN, SYN ACK, ACK.

Virtual Circuits: Call setup -> Data transfer -> Call termination.

Windowing: Used to control the amount of outstanding, unacknowledged data segments.

Flow Control: Uses sliding window to control the speed data is transferred.

Positive Acknowledgement and Retransmission (PAR): Uses timers and acknowledgments to guarantee delivery.

CDP

Uses layer 2 multicast to gather hardware and protocol info.

Sh cdp: Shows timers and holdtimes.

Sh cdp interface: Show encapsulation type, and frequency packets are sent.

Sh cdp neighbor: Shows the directly connected neighbors, local connected interface, capabilities, platform, and neighbor's connected interface.

Sh cdp neighbor detail -OR- sh cdp entry *: Same as above, plus IP address and IOS version details.

(no) Cdp run: Turns on/off for entire device.

(no) Cdp enable: Turns on/off per interface.

DHCP

Provides IP address, subnet mask, domain name, default gateway, DNS servers, WINS servers, etc. to requesting hosts. Uses address pools and lease times.

Hosts use gratuitous ARP broadcasts on their local LAN to detect IP conflicts.

DORA: Discover -> Offer -> Request -> Acknowledge.

Ip dhcp pool [name] -> network [IP and netmask] -> default-router [IP] -> dns-server [IP]

ip dhcp excluded-address [start IP] [end IP]: Assigned from global configuration.

Ip helper-address: Used to forward DHCP requests to a DHCP server on another LAN. Converts a broadcasted DHCP request into a unicast, directed to the DHCP server.

Allocation Methods:

Dynamic: Uses lease times to assign addresses. Once leases expire, addresses are returned to the pool.

Automatic: Doesn't use leases, keeps database of previous grants and tries to give clients the same addresses used previously.

Static: Server keeps a database of MAC/IP address pairs.

IGMP: Controls multicasts.

ICMP: Internet Control Message Protocol

Types:

0	Echo Reply	Ping
8	Echo Request	
9	Router Advertisement	
10	Router Solicitation	
11	Time Exceeded	
30	Traceroute	

Port Numbers

0-1023: Well known.

>1023: Registered - For proprietary applications.

TCP and UDP Ports			
TCP	Ports	UDP	Ports
FTP	20, 21	DNS - Requests	53
Telnet	23	DHCP	67, 68
SMTP	25	TFTP	69
Zone Transfers Between Servers - DNS	53	NTP	123
HTTP	80	SNMP	161
POP	110		
Network News Transfer Protocol (NNTP)	119		
HTTPS	443		

Show Commands

Sh controllers: Information about the physical interface. Type of cable plugged into a serial port, clocking information, and if DTE or DCE.

Sh interface: Shows encapsulation and bandwidth.

Sh ip interface: Shows if ACLs are applied to interfaces.

Sh ip interface brief: Quick overview of interfaces, IPs, and statuses. Very useful.

Sh ip protocols: Displays the configured IP routing protocols, which interfaces on the device that are receiving updates or sending broadcasts, and update time intervals.

Sh protocols: Shows the routed protocols and network addresses configured on each interface.

Sh version: Shows the running IOS version, type of device, modules installed, name of IOS running, how last booted, configuration register setting, etc.

Sh users: On current device; lists active console and incoming VTY sessions.

Sh sessions: Shows current telnet/SSH sessions open on device out to other devices.

Terminal: 9600 Bps, 8 data bits, no parity, 1 stop bit, no flow control.

Ctrl + Shift + 6, then x: Suspends connection to remote device, but leaves it open.

Switching

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on a port in its management VLAN.

Transparent (Learning) Bridges: Pass frames along one hop at a time using bridging information stored in tables that associate MAC addresses with bridge ports (**forward/filter table**).

Considered transparent because the source node does not know it has been bridged because the destination frames are addressed directly to the end node. Help reduce traffic congestion.

Address Learning: Reads source MAC and enters MAC/port number into database called the forward/filter table. If the port is unknown, switch floods packets out all ports except source.

Filter/Forward Decisions (Frame Filtering): When a frame is received, the switch looks at the destination MAC and determines the exit interface from the filter table. The frame is only forwarded out the specified exit port where the destination hardware address is located. Provides more bandwidth.

Loop Avoidance: If multiple connections between switches are created for redundancy, loops can occur. STP is used to stop loops while permitting redundancy.

Switching Processes

Cut-Through: Min latency. Performs address lookup and forwarding as soon as destination MAC is received. Doesn't verify Frame Check Sequence (FCS).

Fragment-Free: First 64 bytes of frame are buffered, frame is forwarded. Cisco proprietary.

Store and Forward: Max latency. Entire frame buffered before forwarding. Frame check sequence run (CRC).

STP - 802.1d

MAC Table Instability: Multiple copies of a frame arriving on different ports of a switch. Appears that a single MAC is reachable on multiple ports; switch is constantly updating MAC table.

Broadcast Storms: Switches flood broadcasts; looped topologies create multiple copies of a single broadcast and perpetually cycle them through the loop.

Duplicate Frames: Due to multiple paths to a single MAC, a frame may be duplicated to be flooded out all paths to a single destination MAC.

Port States:

Blocking: Ports start blocked when STP is enabled. Don't send data, but process BPDUs. **Nondesignated:** Remaining ports with higher costs than designated ports.

Listening: Temporary state. Send and receive BPDUs. Ensure no loops occur before passing data. MAC table not populated yet. 15 secs.

Learning: Temporary state. Ethernet frames are not forwarded but MAC addresses are learned from them to populate the MAC table. 15 secs.

Forwarding: Normal operation.

Disabled: Administratively disabled; virtually nonoperational.

Forward Delay Timer: Listening state + Learning State; 30 secs by default.

Convergence: 50 seconds.

Bridge Protocol Data Unit (BPDU): A STP initializing packet that is sent at definable intervals [2 seconds] for the purpose of exchanging information among bridges in networks.

Bridge Priority: The STP priority of the bridge. 32768 by default. Set with **spanning-tree vlan # (root) (primary)** or manually, **spanning-tree vlan # priority [multiple of 4096]**.

Bridge ID: Bridge priority + MAC address. How STP keeps track of all the bridges in a network.

Root Bridge: Bridge with the lowest bridge ID. All ports are forwarding.

Designated Bridge: The bridge with the lowest Root Path Cost.

Port Cost: Used to determine the best path when multiple links are used between two switches. Cost is determined by the bandwidth of a link.

Root Port: A single port per switch, which has the lowest Root Path Cost upstream, towards the root bridge.

Designated Port: Port(s) that have the lowest Root Path Cost downstream to networks, facing away from the root bridge.

Path Cost: Determined by the sum of the port costs to root bridge.

Port Security: Only on access ports. Prevents unauthorized devices from connecting to switch ports, based on their MAC address. Violations: Shutdown, restrict (SNMP alert), or protect (traffic from permitted MACs allowed to pass, other traffic dropped).

BPDU Guard: Only on access ports. If a switch is connected to an access port, it will receive BPDUs from that switch. This is an indication of a rogue switch and the port will be shut down.

Spanning-tree Portfast: Enable on access ports connected to a single host. Causes loops if port connected to a switch. Port moves directly to forwarding on link up. Skips STP convergence.

Trunking

Minimum 100Mb/s link speed.

Trunk Port Modes:

Trunk: Forced to trunk, even if neighbor doesn't agree. Used between switches, to routers, and from some servers to the switches. Trunk links carry traffic for multiple VLANs.

Access: Forced nontrunking. Used to connect host devices to a switch and carry only the VLAN information that the port is a member of.

Dynamic Auto: Default. Port is passively willing to convert to trunk. Subject to neighbor agreement (neighbor set to **on** or **desirable**). If both ends auto, will not trunk.

Dynamic Desirable: Port actively attempts to become a trunk. Subject to neighbor agreement (neighbor set to **trunk, desirable**, or **auto**).

NoNegotiate: Only in access or trunk mode. Disables the sending of DTP frames on the port. Used when the DTP frames confuse the neighboring (non-Cisco) 802.1q switch.

802.1q Encapsulation: Vendor neutral. Doesn't re-encapsulate; inserts 4-byte tag into the original header. Supports native VLAN (1 by default) which goes untagged, allowing native VLAN traffic to be sent to switch that doesn't support or have trunking enabled.

ISL Encapsulation: Frame tagging. Cisco proprietary. Re-encapsulates frames with VLAN ID. Increases frame size; if frame is already at MTU, it will be dropped. Depreciated.

VLAN Trunking Protocol (VTP): Used to update switches in a switch fabric with information about VLANs configured on a VTP server. VTP devices can be servers, clients, or transparent.

Servers update clients. Transparent devices are only local devices and do not share their own information with VTP clients, but VTP data can be passed through them. VTP devices send VLAN information down trunked links only. Switches must be in the same VTP domain, and must use the same password to exchange VTP information.

VTP Pruning: Reduces unnecessary broadcast traffic. Only forwards broadcasts and unknown unicast frames on a VLAN over a trunk if the receiving end of the trunk has ports in that VLAN.

Inter VLAN Routing: Router: Remove interface IP -> create subif -> **encapsulation dot1q [VLAN #]** -> add IP for subif -> add networks to routing process. **Switch:** Set port as trunk.

Administrative Distances

A number between 0 and 255 that expresses the level of trustworthiness of a routing information source. The lower the number, the higher the integrity rating. "Eeyore."

0 : Connected

1 : Static

90 : EIGRP

100 : IGRP

110 : OSPF

120 : RIPv1, RIPv2

170 : External EIGRP

255 : Unknown or Unreachable

Routing Metrics

Bandwidth, delay, hop count, path cost, load, MTU, reliability, and communication cost.

Any value that is used by routing algorithms to determine whether one route is superior to another; the lower the better.

Only the best possible routes are stored in the routing table, while all other information may be stored in link-state or topological databases.

Routing Loop Avoidance

Route Poisoning: Sets a downed link to a distance of infinity.

Split Horizon: Information about routes is prevented from leaving the router interface through which that information was learned.

Hold-down Timers: Used to stop a route from coming up and being advertised before it is considered reliable.

Triggered Updates: Used to tell neighbor routers about a change in the network when they occur.

Routing Protocols

Distance Vector:

Best path based on distance.

Each time a packet goes through a router, it is counted as a hop. The route with the least number of hops to the destination is determined to be the best route.

Periodically advertises the entire routing table to directly connected neighbors regardless of whether a change has occurred. (RIP(v2), IGRP).

Link State (Shortest-Path-First):

Routers each create three separate tables:

- One keeps track of directly attached neighbors.
- One determines the topology of the entire internetwork.
- One is used as the routing table.

Link-State Advertisement (LSA): Updates sent by routers containing information about neighbors and path costs. Receiving routers use LSAs to maintain their topology tables.

Link-state routers know more about the internetwork than any distance-vector routing protocol.

Routing decisions based on bandwidth, delay etc.

Calculates the paths to each destination from the topological database and places the best of them into the routing table

Updates triggered by changes in network.

Classful Routing: Routing protocols that do not include subnet mask information in routing updates. (RIP and IGRP).

Classless Routing: Protocols that include subnet mask information in the routing updates. Allows Variable Length Subnet Masking (VLSM) and supernetting. (RIPv2*, EIGRP*, and OSPF).

Ip classless: Enabled by default, allows subnetting.

No auto-summary: Stops routing process from summarizing networks at classful boundaries. Necessary when using EIGRP or RIPv2 and using discontiguous networks (Not OSPF). Not enabled by default, but should be.

If a router receives a packet for a destination subnet that's not in the routing table, it will be dropped.

Autonomous System (AS): A collection of networks under a common administrative domain; all routers share the same routing table information. Subdivided by areas.

Convergence: The process required for all routers in an internetwork to update their routing tables and create a consistent view of the network using the best possible paths. No user data is passed during the convergence time.

RIP

Distance Vector; hop count is sole metric. Max hop count is 15, 16 means unreachable.

Default hold-down timer: 180 seconds.

passive-interface int#: Used to stop a router from advertising out a particular interface.

Version 2: Classless, supports VLSM and discontiguous networks, uses multicasts (224.0.0.9) instead of broadcasts, and allows for MD5 authentication.

router rip

network #.#.#.#

OSPF - Open Shortest Path First

Link-state, hierarchical, scalable (unlimited hop count), vendor-neutral, VLSM support, multipath routing, load balancing, and least-cost routing. Suggested successor to RIP.

Uses Dijkstra algorithm.

Hello Protocol: Uses multicast address 224.0.0.5, provides dynamic neighbor discovery, and maintains the neighborship table. Hello packets and LSAs build & maintain the topology table.

Process ID: Locally significant, used to identify a unique instance of an OSPF database.

Router ID (RID): IP address used to identify the router. 1) **ospf router-id #.#.#.#** command. 2) Highest loopback IP address. 3) Highest IP address of any physical interface. 4) If none, 0.0.0.0.

Designated Router (DR): On multi-access networks, OSPF conserves bandwidth by electing a DR that will send/receive routing information to/from other routers on the network. Routers exchange information with the DR instead of each other, reducing the number of advertisements. Not necessary on point-to-point networks. DR is determined by the router with the highest priority, if tied (since all default to 1), the router with highest RID is elected. Priority can be changed at the interface level with the command **ip ospf priority #**.

Backup Designated Router (BDR): Elected to backup DR in case of failure.

OSPF Area: A grouping of contiguous networks and routers. All routers in the same area share a common Area ID. Because a router can be a member of more than one area at a time, an Area ID is associated with each interface on a router. All of the routers within the same area share the same topology table. Area 0, the backbone, is required.

Adjacency: A relationship between two OSPF routers that permits the direct exchange of route updates. OSPF directly shares routes only with neighbors that have established adjacencies.

Neighbor: Two or more routers that have an interface on a common network, e.g. two routers connected on a point-to-point serial link. Dynamically discovered using the Hello protocol.

Neighborship Database: A list of all OSPF routers for which Hello packets have been seen; including RID and state.

Topological Database: Contains information from all LSA packets that have been received for an area. This info is inputted into algorithm to compute the shortest paths to networks.

Stub Area: Area with only one exit path out of the network. Denied external route advertisements; assigned default routes (0.0.0.0) to reach external routes. This reduces the size of the link state database.

Router ospf [process ID]

network #.#.#.# [wildcard mask] area #

EIGRP

Fast convergence, MD5 authentication, multiprotocol (IP, IPX, AppleTalk, IPv6), and VLSM support (**no auto-summary**).

Hybrid Routing Protocol: Characteristics of both link-state and distance vector protocols.

DUAL: Algorithm used to calculate route metrics and to dynamically find and stop loops in the network.

Metric #: Bandwidth and delay by default; can optionally include reliability, load, and MTU.

Feasible Distance (FD): Lowest known distance from the router to a remote network. The route with the lowest FD is placed in the routing table. FD = metric reported by neighbor + metric to neighbor.

Reported/Advertised Distance (RD or AD): The total metric along a path to a destination network as advertised by an upstream neighbor.

Topology Table: Contains all destinations advertised by neighbor routers. Associated with each entry is the destination address and a list of neighbors that have advertised the destination.

Successor Route: The best route, loaded into the route table.

Feasible Successor: The backup route, saved in the Topology table.

Sh ip eigrp neighbors: Amount of time since router has heard from an EIGRP neighbor.

Passive State: A route is considered to be in the passive state when a router is not performing a route convergence.

Active State: A route is considered to be in the active state when a router is undergoing a route convergence.

Reliable Transport Protocol (RTP): Proprietary protocol; uses a mixture of multicasts and unicasts, responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors.

Max Hop: 255. Hop count is not used as a metric; simply limits the number of routers an EIGRP packet can go through before it is discarded; limits the size of the AS.

Autonomous system number is irrelevant as long as all routers use the same number.

Router eigrp [Autonomous system #]

Network #.#.#.#

WIFI

FCC regulates frequencies and power settings. IEEE, ETSI, and WLAN associations are also important governing bodies.

Wi-Fi Alliance: A global, nonprofit industry trade association, devoted to promoting the growth and acceptance of wireless LANs.

Basic Service Area: Physical area of coverage.

SSID: Service Set Identifier, names WLAN.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): For every packet sent, there is a request to send, clear to send, and acknowledgment. Not efficient.

Direct Sequence Spread Spectrum (DSSS): Modulation technique. Lower performance than OFDM. 802.11B. G can revert to DSSS for backwards compatibility with B devices, but slower.

Orthogonal Frequency Division Multiplexing (OFDM): Modulation technique. A/G/N

Multiple-Input Multiple-Output (MIMO), Spatial Multiplexing: Uses multiple transmitters and receiver antennas to increase data throughput and range.

IBSS : Independent BSS, mobile clients connect directly without an intermediate access point (Ad-hoc).

BSS : Basic SS, mobile clients use a single access point.

ESS : Extended SS, two or more BSS are connected by a common distribution system.

2.4 GHz : 3 non-overlapping channels: 1, 6, 11. Susceptible to interference from cordless phones, Bluetooth, and microwaves.

5 GHz : 12 non-overlapping channels.

A: 54 Mbps, 5 GHz. Uses OFDM.

B: 11 Mbps, 2.4 GHz. Uses CSMA/CA and DSSS.

G: 54 Mbps, 2.4 GHz. Uses OFDM.

N: Up to 600 Mbps, 2.4/5 GHz. 40 MHz channels, block acknowledgment, and MIMO.

WIFI Security

WEP: Weak. Static pre-shared key. AP sends the client a challenge-text packet that the client encrypts with WEP key and returns. Traffic can be monitored and key can be decrypted.

Wi-Fi Protected Access (WPA): Changes keys dynamically (while being used). Uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. RC4 encryption algorithm. Protects authentication process and data traffic thereafter. Per-frame sequence counters.

WPA2: TKIP replaced with more secure AES encryption and CCMP integrity checking.

Personal: Uses pre-shared keys instead of 802.1x.

Enterprise: Uses 802.1x or EAP for authentication.

802.1X: Client device (supplicant) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized by authentication server. The supplicant provides credentials (username/password or digital certificate) to the authenticator, and the authenticator forwards the credentials to the authentication server (Radius/Tacacs) for verification. If the authentication server determines the credentials are valid, the supplicant is allowed to access to the protected network.

Security

(Distributed) Denial of Service (DoS): Floods target system with unwanted requests, causing the loss of service to users.

Rate Limiting: Prevent DoS by controlling the rate of bandwidth.

Transport input ssh telnet: SSH > Telnet (under line vty)

Enable secret

No cdp run

Service password-encryption

Cisco Self-Defending Network Strategy: Make network secure by identifying, preventing, and adapting to threats.

Acceptable-use policy and incident-handling policy.

Access Lists

Sh ip access-list

One access list may be configured, per direction, per layer 3 protocol, per interface. Implicit deny at end (**permit ip any any**).

Wildcard mask: 0s match; 1s ignore corresponding bit in address.

ip access-group [#] [in/out]: Apply to an interface (access-class used for VTY lines).

Standard: 1 - 99 and 1300 - 1999.

Place close to destination.

access-list # [deny/permit] [any/host/(IP & wildcard)]

Wildcard mask optional but recommended.

Extended: 100 - 199 and 2000 - 2699.

Place close to source.

If using IP address, wildcard mask used.

access-list # [deny/permit] [protocol] [SOURCE any/host/(IP & wildcard)] [DEST any/host/(IP & wildcard)] [filter, usually [eq] for port] [port # or protocol] (established)
Example: access-list 110 deny tcp host 6.6.6.6 10.10.10.0 0.0.0.255 eq 23

NAT

Static, Dynamic, Overload, Overlapping

Port Address Translation (PAT): Overload. Allows a single public IP address to represent multiple internal private hosts by altering the source TCP or UDP port number.

Sh ip nat translations

Sh ip nat statistics

Clear ip nat translation [*] OR [inside/outside] OR [TCP/UDP]: Clears NAT translations, allowing you to delete or modify your NAT pool.

Debug ip nat detailed: Provides information about certain errors or exceptional conditions, such as the failure to allocate a global address.

Inside Local : The private IP address of a host as it appears on the inside network, probably assigned by DHCP.

Inside Global : A legitimate, public IP assigned by an ISP, that represents one or more inside local IPs. IP(s) used for the address pool.

Outside Global : The IP assigned to a host on the outside network by the host owner. The address is allocated from a globally routable address or network space.

Outside Local : The IP of an outside host as it appears to the inside network. Usually same as outside global, NAT may convert outside IPs to an address space routable on the inside.

Troubleshoot:

1) There must be enough addresses in the NAT pool.

2) Ensure correct router interfaces are assigned **ip nat inside/outside**.

3) The ACL referenced by NAT is permitting the necessary local IP addresses.

Example:

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool MyPool 24.17.5.1 24.17.5.14 netmask 255.255.255.240
ip nat inside source list 1 pool MyPool overload
interface Ethernet 0
ip nat inside
interface serial 0
ip nat outside
```

WAN

DSL: Circuit Switched, uses telephone lines, local-loop line for telephone voice communication, always-on connection for internet. Network transmissions are sent above 4-kHz frequency.

Can be added incrementally to an area, has distance limitations, not universally available.

Cable: Uses same coaxial cables as television service. Higher speed than leased lines.

Serial: Transmission takes place one bit at a time, over a single channel. Set bandwidth (manually) so routing protocols can select the best route.

HSSI: up to 52 Mbps

Circuit Switching

Used with dial-up networks such as PPP and ISDN. Passes data, but needs to set up the connection first—just like making a phone call.

Dedicated physical circuit is established, maintained, and terminated through a carrier network for each communication session.

Allows multiple sites to connect to the switched network of a carrier and communicate with each other.

Leased Line (Point to Point)

Serial, requires minimal expertise to install and maintain, and typically offers a high quality of service.

Provides a single, preestablished, permanent, dedicated, always available communications path from the customer, through a carrier network (e.g. telco), to a remote network.

Carriers usually lease point-to-point lines, which is why point-to-point lines are often called leased lines.

The carrier dedicates fixed transport capacity and facility hardware to the line of a customer.

HDLC

Default encapsulation of serial links. Cisco HDLC is proprietary and bit-oriented. If connecting to another vendor's router, use PPP instead.

Specifies an encapsulation method for data on synchronous serial data links using frame characters and checksums.

Includes support for both point-to-point and multipoint configurations.

Cisco HDLC lacks windowing, flow control, and authentication.

PPP

Vendor neutral. Originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. Commonly used for dial-up Internet. Offers optional compression.

Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Can encapsulate multiple L3 protocols on single L2 link.

Link Control Protocol (LCP): Used for establishment, configuration, and testing of the data-link connection.

Network Control Protocol (NCP): Method of establishing and configuring different Network layer protocols. Designed to allow the simultaneous use of multiple Network layer protocols.

Password Authentication Protocol (PAP): Method of validating connection requests. Requesting (remote) device must send an auth request containing a password and ID to the local router when attempting to connect. Unlike CHAP, PAP sends the password unencrypted and does not attempt to verify whether the user is authorized to access the requested resource; it merely identifies the remote end.

Challenge Handshake Authentication Protocol (CHAP): Performed periodically, uses three-way handshake, remote node replies with an MD5 hash. Newer and more secure than PAP.

Frame Relay

Industry-standard, shared access, best effort, packet switched, Data Link layer encapsulation that services multiple virtual circuits and protocols between connected mechanisms.

NBMA by default. Clocking provided by CSU/DSU.

The connection to the network edge is often a leased line but dialup connections are available from some providers using ISDN or xDSL lines.

Uses both error and flow control.

Provides both PVC and SVC service using shared medium-bandwidth connectivity that carries both voice and data traffic.

Permanent Virtual Circuit (PVC): Always connected, acts like a leased line. More common.

Switched Virtual Circuit (SVC): Dynamically established virtual circuit created on demand and dissolved as soon as transmission is over and the circuit is no longer needed.

DLCI: Used to identify virtual circuits in a Frame Relay network.

Local Management Interface (LMI): Signaling between the router and the local frame relay switch. Provides keepalive, multicast, and a status mechanisms and global addressing. Types are Cisco (default), ANSI, and Q.933A. **frame-relay lmi-type**.

Encapsulation: Cisco (default), or IETF.

Committed Information Rate (CIR): A Frame Relay network's agreed-upon minimum rate of transferring information. Averaged over a minimum span of time and measured in bps.

Discard Eligible (DE): Traffic exceeding CIR is marked DE.

Explicit Congestion Notification: Congestion avoidance policy. Congestion control bits are incorporated into the address field. **Forward (FECN)** bit is set to 1 to alert the **receptor** that congestion was encountered along the path from source to destination. **Backwards (BECN)** bit is set to 1 to alert the **sender** that congestion was encountered in the network in the direction opposite of the frame transmission.

Configuring Frame Relay Switch Routes:

- 1.) **Encapsulation frame-relay**
- 2.) **Frame-relay intf-type dce**
- 3.) **Clock rate ###**
- 4.) **Frame-relay route [DLCI in] interface [serial#/#] [DLCI out]**

Point-to-point Subinterfaces: Solves split horizon issues, and maps a single subnet to a single DLCI.

- 1.) Remove IP address on physical interface if using subinterfaces. (**no ip add**)
- 2.) **Encapsulation frame-relay**
- 3.) Create subinterface and specify as point-to-point or multipoint. (**int s#/#.#[point-to-point / multipoint]**)
- 4.) Assign IP address to subinterface.
- 5.) Assign DLCI to subinterface (**frame-relay interface-dlci #**)
- 6.) In order to map Layer 3 IP addresses to Layer 2 DLCIs, Frame Relay uses Inverse ARP, or static mapping:

Frame relay map ip [next-hop-address] [local dlci] (broadcast): Manually maps a DLCI # to the destination IP address. Broadcast keyword allows routing updates over the PVC.