Hierarchical design model is composed of core, distribution, and access layers. Addressed simple issues, but lack:
- Place for wireless, workgroup and enterprise services
- Place for remote access
- Internet access and security model

Enterprise composite model is broken into 3 sections:

- enterprise campus (local LAN) contain campus backbone, building distribution, building access, management, edge distribution, and server farm.
- enterprise edge (connecting to larger world) include WAN, remote access, Internet connection, and E-commerce.

![Diagram showing network components]

- service provider edge (different networks join) include ISP, PSTN, Frame relay, ATM and PPP

Network design must follow one of the following models:
- Cisco Lifestyle services uses PPDIOO model.
- IT infrastructure library (ITIL) emphasize business requirements and processes.
- FCAPS have 5 management categories (fault, configuration, accounting, performance, and security)
- Telecommunications management network (TMN) is based on FCAPS model).

QoS function can be also achieved using Intelligent Information Network (IIN), which describes evolutionary vision of a network that integrates network and application functionality cooperatively and enables the network to be smart about how it handles traffic to minimize the footprint of applications.

IIN is build on top of Enterprise Composite Model and describes structures overlaid on top of the model in 3 phases;
- Phase 1, “integrated transport” described a converged network built along lines of composite model and based on open standards.
- Phase 2, “integrated services” attempt to virtualize resources.
Phase 3, “integrated applications” use application-oriented networking to make network application-aware and to enable the network to actively participate in service delivery.

SONA applies the IIN ideal to enterprise network. SONA breaks down IIN function into 3 layers:
- Network Infrastructure: hierarchical converged network and attached end systems
- Interactive services: resources allocated to applications
- Applications: include business policy and logic

EIGRP hello and acknowledgment packets are not acknowledged. If a reliable packet is not acknowledged, EIGRP periodically retransmits the packet to the nonresponding neighbor as a unicast. EIGRP has a window size of one, so no other traffic is sent to this neighbor until it responds. After 16 unacknowledged retransmissions, the neighbor is removed from the neighbor table.

To establish 2 way adjacency:
- RA send Hello
- RB send back a Hello with an update that contains routing information
- RA acknowledges update
- RA sends its update
- RB acknowledges

Hello/hold timers are:
- 5/15 sec for multipoint circuit of bandwidth > T1 and PtP media
- 60/180 sec for multipoint circuit of bandwidth < T1

3 main causes of SIA:
- Link congestion
- Router busy
- Unidirectional link

EIGRP always use the first valid key to check for authentication.

EIGRP over EoMPLS, CE built EIGRP adjacencies with each other. PE router doesn’t learn any MAC address or participate in SPT.
EIGRP over MPLS (L3 VPN) build adjacency between each connected PE and CE router.
EIGRP over Frame Relay may require static mapping, which can allow non-VC-connected routers to form neighborship. By default, router assume all WAN link has 1544 Kbps of bandwidth.
Suggestion: configure CIR on each PtP subinterface.
In case when hub is oversubscribed, set bandwidth on each subinterface arbitrarily low and specify EIGRP bandwidth percent value over 100 to allow EIGRP to use excess bandwidth.

4 factors affect EIGRPs’ scalability:
- Number of routes to exchange
- Number of routes that must know of a topology change
- Number of alternate routes to a network
- Number of hops from one end of the network to another (topology depth)
  To improve scalability, use:
  - EIGRP stub
  - Active process enhancement enables routers to use SIA-Queries and SIA-replies to prevent the loss of a neighbor unnecessarily. A router sends its neighbor a SIA-Query after no reply to a normal query. If the neighbor responds with a SIA-Reply, the router does not terminate the neighbor relationship after 3 minutes, because it knows the neighbor is available.
  - Graceful shutdown is a feature by which routers send special message to its neighbors when shutting down. This message causes neighbors to trigger a route calculation rather than wait for the hold timer to expire.

Dividing OSPF into areas:
- Minimize the number of routing table entries
- Restricts LSA flooding
- Minimize impact of topology change
- Enforce concept of hierarchical network design

LSDB overload protection monitors number of LSAs received and processed. If specified threshold exceed for one minute, router enters ‘ignore’ state by dropping all adjacencies and clearing OSPF LSDB. Operation is resumed after condition remain normal for certain period.
  Configured using ‘(config-router)#max-lsa NO [THRED_PERC] [warningonly] [ignore-time MIN][ignore-count NUM][reset-time MIN]’

Type 3 and 4 LSA are both presented as ‘O IA’ routing table entries. Type 8 - 12 LSAs are not present in routing table.

You can also enable OSPF using ‘(config-if)#ip ospf P_ID area A_ID’ which takes precedence over ‘network’ command.

Summary can be created by:
- ‘area A_ID range x.x.x.x y.y.y.y’ for T3 LSA, one subnet must be present to advertise summary.
- ‘summary-address x.x.x.x y.y.y.y’ for T5 LSA, router automatically create a static route pointing to Null0.
Hello/hold timer:
- 10/40 for LAN and PtP interface
- 30/120 for NBMA interfaces

OSPF has 5 network types:
- NBMA, default for multipoint serial interface, use DR, manual neighbor configuration
- P2MP, no DRs, automatically discover neighbors
- P2MPNB, no DR, manually discover neighbors
- Broadcast, default for LAN, use DR, automatic neighbor discovery. Proprietary when used on WAN
- P2P, automatic discover neighbor, no DR.

Note for NBMA:
- Neighbor may need to be statically configured
- Full mesh can be established using physical interface
- Partial mesh should be configured using PtP subinterface, especially when no single device has full connectivity to other devices. Subset of topology with full connectivity can use a multipoint subinterface
- Hub-and-spoke should either configure DR if hub can connect every spoke directly
- DR and BDR should have full virtual circuit connectivity to all other devices
- All frame relay or ATM maps should include ‘broadcast’ attribute

OSPF on L2 MPLS form adjacency between CE routers, elect DR/BDR, network type is broadcast.
OSPF on L3 MPLS VPN form adjacency between PE and CE. Network type is determined by PE and CE.

OSPF authentication must be enabled on both OSPF process and interface configurable. All OSPF neighbors reachable through an interface configured for authentication must use the same password.

To control routing update, use:
- Route map: match conditions on different lines are interpreted as logical AND, whereas match conditions on same line are interpreted as logical OR. ‘ip route-source’ refers the router to an access list that permits or denies advertising router IP address
- Prefix list
- Distribute list
- Passive interface: OSPF and EIGRP don’t send Hello message out a passive interface. RIP doesn’t send update out a passive interface but listens for inbound updates.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Redistribution Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP</td>
<td>Default metric is Infinity. Metric must be set, except when redistributing static or connected routes, which have a metric of 1.</td>
</tr>
</tbody>
</table>
### OSPF
Default metric is 20. Can specify the metric type; the default is E2. Must use `subnets` keyword or only classful networks are redistributed.

### EIGRP
Default metric is Infinity. Metric must be set, except when redistributing static or connected routes, which get their metric from the interface. Metric value is “bandwidth, delay, reliability, load, MTU.” Redistributed routes have a higher administrative distance than internal ones.

### Static/Connected
To include local networks not running the routing protocol, you must redistribute connected interfaces. You can also redistribute static routes into a dynamic protocol.

### BGP
Metric (MED) is set to IGP metric value.

'(config-router)#distance' changes AD of routes. An entry of 0.0.0.0 255.255.255.255 changes AD of all routes. EIGRP configures AD using ‘(config-router)#distance eigrp INT EXT’ and BGP uses ‘(config-router)#distance bgp INT EXT’. OSPF can change its external AD using ‘(config-router)#distance ospf external’ command.

**Suggestions:**

**Multipoint one-way redistribution:**
- Use a routing protocol with different ADs for external and internal routes
- Ensure AD of redistributed external routes is higher than AD of protocol they were originated

**Multipoint two-way redistribution:**
- Use a routing protocol with different ADs for external and internal routes
- Ensure AD of redistributed external routes is higher than AD of protocol they were originated
- Ensure only internal routes are redistributed by tagging routes then apply filter
- Adjust the metric of redistributed routes
- Consider using a default route to avoid multipoint two-way redistribution

**Redistribution notes:**
- Router redistribute only routes learned by source protocol.
- When redistribute at multiple points, check path taken. Suboptimal routing can be fixed by changing AD
- When redistributing routes into BGP, use ‘include-connected’ to advertise connected routes
- BGP doesn’t redistribute routes learned by iBGP into an IGP by default. To change this, use ‘(config-router)#bgp redistribute-internal’
- When redistribute routes between 2 OSPF processes, routers advertised into new process as Type 2
- Include ’subnets’ keyword in ‘redistribute’ command. Otherwise, only default classful subnet masks are redistributed into OSPF
- When redistributing routes into RIP, specify a seed metric. Otherwise, all routes are unreachable.

**Traffic pattern can be altered using:**
- Offset-lists increase the metric (hop count) or RIP and add delay to EIGRP. Can be specified over an interface, which takes precedence over a normal offset list.
- IP SLA use path jitter of various types of tests and measure network performance and host reachability. Useful for path control because it enables you to switch to a backup path if network performance on the primary path degrades.
- PBR allow you to choose a path based on factors other than destination IP address. Fast-switching PBR can be enabled, default to use CEF-switched PBR whenever CEF is enabled.
- OER monitor WAN performance and report information to master controller router. If result fall within configured range, no change is mode to default routing. If performance begin to degrade a specific link or network, controller notify border routers to reroute traffic.
- VRF segment traffic as L3 VLAN, VLANs create virtual switches with segregated CAM table.

To use IP SLA, you must:
- Create a monitor session on the probe source device
- Define the probe by specifying traffic type, destination IP address, and any other desired variable such as DSCP values
- Schedule probe beginning and ending time
- Define a tracking object that is linked to monitor session
- Link tracking object to a static route
   Enable with `(config)#ip sla responder` command.

PBR uses:
- `set ip next-hop IP_ADD` checks to see if next-hop address is reachable. If so, forwards traffic to that address. If not reachable, uses next hop from routing table
- `set interface INT_NAME` can list multiple interface and use the first active interface. If explicit route (not including default route) exist in the routing table, first valid interface is used as outgoing interface. If no explicit route exist in the routing table, command is ignored
- `set ip default next-hop IP_ADD` specifies the next hop for a destination network (selected by `match`) if no explicit route for that network exist in the routing table. If destination network shows up in routing table, command is ignored.
- `set default interface INT_NAME` specifies outgoing interface for a destination network (selected by `match`) if no explicit route for that network exist in the routing table. If destination network shows up in routing table, command is ignored.

Apply to interface using `(config-if)#ip policy route-map NAME` or to the router traffic itself, with `(config)#ip local policy route-map NAME`
Routers can only run one instance of BGP at a time.

Default local preference (100) can be changed with `(config-router)#bgp default local-preference VAL`.

History routes (‘h’) are known to BGP but doesn’t currently have a valid route to it. RIB failure (‘r’) means route was advertised into BGP but not installed because another source with lower AD is also advertising it. Stale (‘S’) routes are used for nonstop forwarding to indicate that the route is stale and needs to be refreshed when the peer is reestablished.

BGP uses 3 tables:
- Neighbor database, show ip bgp summary
- BGP RIB, show ip bgp
- Routing table, show ip route

### Branch office design factors:

<table>
<thead>
<tr>
<th></th>
<th>Small branch</th>
<th>Medium branch</th>
<th>Large branch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity technology</td>
<td>PSTN connectivity</td>
<td>MPLS or Frame Relay</td>
<td>MPLS and any-to-any connectivity</td>
</tr>
<tr>
<td>Resiliency</td>
<td>Primary</td>
<td>Dual connection</td>
<td>Highly available</td>
</tr>
<tr>
<td>Routing</td>
<td>Static or dynamic routing</td>
<td>Dynamic routing; load balancing</td>
<td>Route redistribution and filtering</td>
</tr>
<tr>
<td>Services</td>
<td>NAT, WAN optimization, DHCP</td>
<td>NAT, WAN optimization, DHCP, HSRP</td>
<td>WAN optimization</td>
</tr>
<tr>
<td>Security and compliance</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
</tr>
<tr>
<td>Mobility</td>
<td>None</td>
<td>None</td>
<td>VPN</td>
</tr>
</tbody>
</table>

Full branch office implementation aims at:
- Deployment strategy
- Network diagrams
- Installation and site tests
- Site survey results
- Installation guidelines
- Device-specific configuration templates
- Test and acceptance plan
- Documentation of new network.

### ADSL options

<table>
<thead>
<tr>
<th></th>
<th>Voice and data</th>
<th>Downstream 8 Mbps</th>
<th>Upstream 1 Mbps</th>
<th>Distance 5.46 Km</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL Voice and data</td>
<td>Downstream 52 Mbps</td>
<td>Upstream 13 Mbps</td>
<td>Distance 1.37 Km</td>
<td></td>
</tr>
<tr>
<td>VDSL</td>
<td>Data</td>
<td>Downstream 768 Kbps</td>
<td>Upstream 762 Kbps</td>
<td>Distance 6.7 Km</td>
</tr>
<tr>
<td>SDSSL; proprietary</td>
<td>Data</td>
<td>Downstream 2.048 Mbps</td>
<td>Upstream 2.048 Mbps</td>
<td>Distance 3.7 Km</td>
</tr>
<tr>
<td>HDSL</td>
<td>Data</td>
<td>Downstream 2.3 Mbps</td>
<td>Upstream 2.3 Mbps</td>
<td>Distance 8.52 Km</td>
</tr>
<tr>
<td>G.SHDSL</td>
<td>Data</td>
<td>Downstream 2.3 Mbps</td>
<td>Upstream 2.3 Mbps</td>
<td>Distance 8.52 Km</td>
</tr>
</tbody>
</table>

DSL is a L1 protocol that need L2 protocol to carry traffic, which can be bridging (Ethernet), PPPoE, and PPPoA.
IPsec establish a VPN connection between 2 hosts, it sets up two security association (SA) between them; each SA is unidirectional. ISAKMP defines how SAs are created and deleted. An IPsec transform set defines how VPN data will be protected by specifying the IPsec protocols that will be used. You can specify up to four transforms, and the algorithm to use with each. You can also configure either tunnel or transport mode. (Tunnel is default.)

Traffic allowed are specified in crypto ACL. Crypto map join transform sets and crypto ACL to associate them with a remote peer; it’s applied to the outgoing interface.

To use IPsec tunnel as ‘always-on’ connection, you need to send routing updates. However, IPsec only carries unicast traffic. There are 4 ways to create a tunnel:
- DMVPN: create multipoint tunnel on-demand. Good for spoke-to-spoke
- GET VPN: create encrypted multipoint tunnels on demand. Good for secure spoke-to-spoke
- VTI: create always-on tunnel carry unicast and multicast traffic. Configure routing protocol, save 4 bytes compared to GRE
- GRE: support multiple L3 protocol, allow multicast routing protocol across the tunnel. Use 20 byte IP header and 4 byte GRE header. Use along with IPsec to secure authentication, confidentiality, and integrity. Typically configured over untrusted WAN to minimize number of tunneled maintained by each router.

To create GRE tunnel:
1. Create a loopback interface to use as tunnel endpoint.
2. Create GRE tunnel interface
3. Add tunnel subnet to routing process to exchange routing updates across the interface
4. Add GRE traffic to crypto ACL to encrypt the traffic using IPsec.

Mobile worker connectivity requires:
- Bandwidth requirement: sufficient bandwidth using cable, DSL, or wireless
- Connection security: use site-to-site VPN for permanent home users and remote access VPN for mobile users, using either IPsec or SSL. IPsec requires a client on the endpoint, but it can provide full access to all network applications. SSL is used from a web browser, therefore, not compatible with all applications.
- Corporate security: firewall, IPS, and URL filtering should be applied at central site
- User authentication based on NAC, AAA and other authentication mechanism
- QoS are use when voice and video traffic are needed.
- Management: governance can be establishing using policies.

<table>
<thead>
<tr>
<th>Access to applications and services</th>
<th>Traditional Mobile Worker</th>
<th>Business-Ready Mobile Worker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice and video support</td>
<td>Limited to none</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS</td>
<td>No (best effort)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Mobile worker solution include:
- Corporate devices, headend routers, VPN concentrators, security appliance, and management appliance.
- Remote site devices include broadband access, VPN router with QoS capability and computer.
- Optional additional services such as IP phone, voice mail and contact center.

Components of mobile worker solution:
- VPN solution, either IPsec or SSL
- Firewall solution, for stateful L3 - 7 protection
- IPS to defend
- Wireless security with encryption and 802.1x authentication
- QoS for voice and video
- Ports for printers and other devices at remote site
- PoE ports for IP phone.

Cisco Easy VPN dynamically:
- Negotiate and establish VPN tunnel parameters
- NAT, PAT, or ACL configuration
- User authentication
- Manage encryption and decryption keys
- Authenticate, encrypt, decrypt traffic

Cisco Easy VPN has 2 components:
- Server: can be Cisco router, ASA firewall, or Cisco VPN concentrator; contain security policies and push them to remote clients
- Remote Client: can be Cisco router, ASA firewall, hardware client, or software client; contact server and receive policies from it to establish the IPsec tunnel.

Need a public address and a private address.

To configure Cisco Easy VPN,
1. Allow IPsec traffic (IP 50 for ESP, IP 51 for AH, UDP 500 for ISAKMP, and UDP 4500 for NAT-T) through edge firewall or ACL
2. Create IP address pool for VPN clients. Address is assigned using ‘(config)#ip local pool NAME FIRST_ADD LAST_ADD [mask MASK]’ on local router, but usually done by VPN support team.
3. Verify IPsec VPN configuration using ‘show crypto map’, ‘show crypt isakmp sa’, ‘show crypto ipsec sa’, and ‘show crypto engine connections active’
4. Ensure corporate devices have routes to the VPN subnets. Achieved using
   . Make VPN subnet a part of an existing subnet and advertise. Enable proxy-ARP on interface connected to the subnet
   . Use a separate subnet for VPN client (static route or reverse route injection from IPsec) and inject/redistribute that subnet into routing protocol.
5. Tune NAT to bypass VPN traffic, NAT should not be applied to VPN, therefore, your NAT ACL must be configured to overlook (deny) VPN traffic.
Ff02::2 is the link-local multicast address.
Ff05::2 is the site-local multicast address.
Ff02::1:FF00/104 is the solicited-node multicast address.
::/96 is IPv4 compatible address.

When ping IPv6 address, you must specify a source.

EUI-64 can be configured by ‘(config-if)#ipv6 address xxxx.xxxx.xxxx.xxxx::/64’ without ‘eui-64’ keyword.

Stateless autoconfiguration allow a host to automatically acquire an IP address without needing DHCP; configured with ‘(config-if)#ipv6 address autoconfig’. It creates the link-local address (using FE80::/64 and interface MAC address), then use NDP to ensure that address is unique.

NDP is used to:
- DAD: send NS message with its own address to ensure link-local address is unique
- Neighbor discovery: host discovers link-local address using NS message, which is similar to ARP messages.
- Router discovery: send RA listing network prefix. When hosts come online, it send RS message to all routers multicast address.

IPv6 support renumbering of network address by configuring an age with an address. Routers send out an RA with both prefixes and their lifetimes.

IPv6 support 3 types of links:
- Point-to-point: serial link borrow Ethernet’s MAC address. You can manually configure link-local address. Don’t always need global unicast address. If use link-local only, host is not routable.
- Point-to-multipoint: must map destination address to DLCI. You need 2 mapping, one to unicast global address and one to link-local address. Both using ‘frame-relay map ipv6 DEST_ADD out dlci DLCI broadcast’
- Multiaccess links: uses IPv6 ARP, or NDP to discover neighbors. Verify with ‘show ipv6 neighbors’. To add a static entry, use ‘(config)#ipv6 neighbor IPV6_ADD INT_NAME L2_ADD’

Transition mechanism from IPv4 to IPv6:
- Dual stack
- Translation using NAT-PT
- Tunneling serve as virtual PtP link between IPv6 domains. There are 5 ways to tunnel IPv6 over IPv4:
  - Manual tunnel: source and destination are IPv6 address in the same subnet. You might want to use loopback address to increase stability. Use ‘(config-if)#tunnel mode ipv6ip’. Verify with ‘debug tunnel’ or ‘show interface tunnel NUM’
. GRE tunnel is the same as manual tunnel, but you can allow a routing protocol. Use IPv6 interface address as tunnel sources and destination, create tunnel with ‘tunnel mode gre ipv6’
. 6to4 tunnels is dynamically created for point-to-multipoint interfaces using 2002::/16 plus IPv4 address of dual-stack router on the other side as next 32 bits. When IPv6 traffic arrives the an edge dual-stack router with this address, router use it to determine packet destination. Use IPv4 address as source but no destination, enable with ‘(config-if)#tunnel mode ipv6ip 6to4’ command. Each peer need to reach its peer on the other side using static route or BGP.
. IPv4 compatible IPv6 tunnels: deprecated. Encodes IPv4 address of tunnel source in lowest 32 bits of IPv6 tunnel address then pads the rest with 0. Use ‘(config-if)#tunnel mode ipv6ip auto-tunnel’
. ISATAP

IPsec is a set of rules for securing data communication across a public, untrusted network such as the Internet. It provides:
- Data confidentiality by encrypting portions/all of a packet
- Data integrity by ensuring packet has not been altered in transit.
- Data source authentication to ensure data originated with a trusted source
- Anti-replay protection to ensure that packets are not copied and send.

AH header authenticate the packet using a hash, but doesn’t encrypt packet payload. ESP header and trailer encrypt packet payload and optionally authenticate using AH. When used this way, ESP headers are added before AH header.

IPsec operate in either:
- Transport mode uses original header encrypt payload using ESP header. Often used with GRE.
- Tunnel mode replaces original IP header with a tunnel header. ESP header is placed between original IP header and new IP header. Tunnel mode can cause problems when used with NAT because L4 ports are hidden. NAT traversal detects the existence of NAT device and add an UDP header (contain L4 port 4500) after tunnel IP header.

IPsec support the following authentication:
- Username and password
- One-time password
- Biometric features
- Preshared key values
- Digital certificate
IPsec uses these encryptions: symmetric (DES, 3DES, or AES) or asymmetric (RSA, diffie-hellman).

IPsec uses PKI to manage encryption and identity information such as public keys and certificates.

IPsec VPN between two peers are established using security association (SA), which are unidirectional. There are 5 basic steps:
- VPN traffic identified by crypto access list arrived at the router
- IKE phase one: negotiate algorithms and hash to use, authenticate peers, and set up ISAKMP SA, which can be main or aggressive mode. Main mode uses 3 exchanges, where as aggressive mode send all information in one exchange. Exchanges contain transform sets that list the proposed encryption algorithm, authentication algorithm, key length, and mode. Multiple transform sets can be specified, but both peers must have at least one matching transform set or tear down the session.
- IKE phase two: use secure channel created above to set up SAs for ESP and/or AH, negotiate settings to be used. Renegotiate every so period depending on data transmitted or length of time. An additional Diffie-Hellman key may be exchanged.
- All are set, and data are transferred along the VPN between two peers
- Tunnel termination because of either direction termination or time out.

6 step to configure a site-to-site IPsec VPN:
- Configure ISAKMP policy using `(config)#crypto isakmp policy` command.
- Configure IPsec transform set(s) that specify the IPsec protocols used. You can create up to 4 transform sets using `(config)#crypto ipsec transform-set` command.
- Configure crypto ACL is a normal (standard/extended) ACL with permitted traffic encrypted and denied traffic not send over the tunnel.
- Configure a crypto map that pulls together all previous configuration and associate them with a remote peer. Crypto map also uses sequence number, multiple entries forms a crypto map set. Created with `(config)#crypto map NAME SEQ_NO ipsec-isakmp` command.
- Apply crypto map to outgoing interface using `(config-if)#crypto map NAME`, you may need to configure a static route to point all VPN traffic toward this interface.
- Optionally configure and apply an ACL that permits only IPsec or IKE traffic by specifying them in the access-list.
Verify with `show crypto isakmp sa`, `show crypto ipsec sa` and `debug crypto isakmp`.

GRE is a tunneling protocol that can support multiple L3 unicast and multicast routing protocols. It adds a 20 byte IP header and 4 byte GRE header, hiding existing packet headers. The GRE header contains a flag field and a protocol type field to identify L3 protocol being transported. Tunnel checksum, tunnel key, and tunnel sequence number can be optionally provided. Encrypt/authenticate traffic using IPsec, not by itself.

GRE tunnel is configured using `(config-if)#tunnel mode gre ip` under a tunnel interface.
Switch

A set of distribution device along with access layer device comprise of a switch block.

Access:
- High availability via hardware and software
- Converged network support
- Security through switching tools

Distribution:
- High availability via redundancy
- Routing and security policies applied
- Segmentation and isolation of workgroups from core

Core, added when connecting three or more switch blocks:
- Reliability through redundancy
- Scalability through protocol
- No policies

Small campus design (less than 200 devices), distribution and core are combined into one layer.

Medium campus design (200 - 1000 devices), may require a core layer. Each floor is a switch block linked together to core.

Data center is connected to users via core layer. Distribution layer is changed to aggregation layer that provide load balancing, content switching, SSL off-load, and security.

Applications may have different flow pattern:
- Peer-to-peer application have differing network requirements, and any or may not traverse the core
- Client-server application require access to servers centralized in data centers. Require fast and reliable access. Access must be securely controlled
- Client-enterprise application are located on servers at WAN edge, reachable from outside the company. Access must be secure and highly available.
PPDIOO lifecycle approach can be used to apply network changes using:
- Prepare: gathering information and prepare strategy
- Plan: requirement gathering, network examination, gap analysis, project plan
- Design
- Implement: detailed implementation plan
- Operate: day-to-day network operation and monitoring
- Optimize: proactive network management and fault correction

ISL can identify CDP and BPDU frames. ISL header can't be removed on a non-trunking port. By default, system installs ISL system CAM entries and drops the packet. In special cases, these CAM entries are installed for every active VLAN in the switch. To prevent such collision, enter 'no-isl-entries enable' command to connect to other switches.

On links that should not be trunks, turn off trunking negotiation by setting switchport mode to host. This sets it as access port, enables PortFast, and disables EtherChannel negotiation.

VTPv2 only perform consistency check when configured through CLI or SNMP. There may be too many VLANs for VTP to function correctly.

Some guidelines for EtherChannels follows:
- Interfaces in the channel do not have to be physically next to each other or on the same module.
- All ports must be the same speed and duplex.
- All ports in the bundle should be enabled.
- None of the bundle ports can be a SPAN port.
- Assign an IP address to the logical Port Channel interface, not the physical ones, if using a Layer 3 EtherChannel.
- Put all bundle ports in the same VLAN, or make them all trunks. If they are trunks, they must all carry the same VLANs and use the same trunking mode.
- The configuration you apply to the Port Channel interface affects the entire EtherChannel. The configuration you apply to a physical interface affects only that interface.

L2 etherchannel has a logical interface whereas L3 etherchannel don’t.

Verification command: ‘show run interface NAME”, ‘show interface NAME etherchannel’, ‘show etherchannel NAME port-channel’, ‘show etherchannel summary’, and ‘show etherchannel load-balance’

You can suspect there is a loop when:
- You capture traffic on a link and see the same frame multiple times
- All users in a bridging domain have connectivity problems at the same time
- There is abnormally high port utilization

TCN BPDU is send by a downstream switch toward the root when:
- There is a link failure
- Port starts forwarding, and there is already a designated port
- Switch receives TCN from a neighbor

A TCN BPDU is acknowledged with configuration BPDU with TCN acknowledgment bit set. When root bridge receives a TCN, it starts sending configuration BDPU with TCN bit set for a period of time = max age + forward delay. Switches that receive this change their MAC table aging time to Forward Delay time, causing MAC addresses to age faster. This also cause an election of root bridge, root ports and designated ports.

If an RSTP switch detects a topology change, it sets a TC timer to twice the hello time and sets the TC bit on all BPDUs sent out its designated and root ports until the timer expires. It also clears the MAC addresses learned on these ports. Only changes to the status of non-Edge ports cause a TC notification.

If an RSTP switch receives a TC BPDU, it clears the MAC addresses on that port and sets the TC bit on all BPDUs sent out its designated and root ports until the TC timer expires.

BackboneFast is used to detect indirect failure. Switch tries to find an alternate path (after receiving inferior BPDU) by sending RLQ frames:
- If the inferior BPDU was received on a blocked port, the root port and any other blocked ports are considered alternates.
- If the inferior BPDU was received on the root port, all blocked ports are considered alternates.
- If the inferior BPDU was received on the root port and there are no blocked ports, the switch assumes it has lost connectivity with the root and advertises itself as root.

BPDU filtering: In global config, if a Portfast interface receives any BPDUs, it is taken out of Portfast status. At interface config mode, it prevents the port from sending or receiving BPDUs.

Here is an example of features you can implement in a network

A MLS does L2 forwarding when destination MAC address is mapped to one of its interface. Here are the steps for forwarding, a lot of them are unnecessary if such feature wasn’t configured:

Input:
1. Receive Frame
2. Verify Frame Integrity
3. Apply inbound VLAN ACL
4. Look up destination MAC

Output:
1. Apply outbound VLAN ACL
2. Apply outbound QoS ACL
3. Select output port
4. Place in port queue
5. Rewrite
6. Forward

MLS does L2 forwarding when destination MAC address is one of it’s own interface:

Input:
1. Receive Frame
2. Verify Frame Integrity
3. Apply inbound VLAN ACL
4. Look up destination MAC

Routing:
1. Apply input ACL
2. Switch if entry is in CEF cache
3. Apply output ACL

Output:
1. Apply outbound VLAN ACL
2. Apply outbound QoS ACL
3. Select output port
4. Place in interface queue
5. Rewrite source and destination MAC, IP checksum, and frame check sequence, and decrement TTL
6. Forward

SVIs are used to:
- Route or fallback bridge between VLANs
- Provide a default gateway for users in that VLAN
- Route traffic into or out of its associated VLAN
- Provide an IP address for connectivity to the switch itself
- Provide an interface for routing protocol

SVI is considered “up” as long as at least one port in its associated VLAN is active and forwarding. You may not want the status of a single port to influence SVI, use ‘(config-if)#switchport autostate exclude’ command.

Traffic not handled by CEF (or punted) include:
- Packets with IP header options
- Tunneled traffic
- 802.3 (IPX) or other unsupported encapsulation types
- Packets with expiring TTL
- Packets that needs fragmentation

There are 5 components to high availability:
- Redundancy attempt to eliminate single point of failure by providing duplicate devices
- Technology include IP SLA, NSF, SSO, stackwise, etc
- People: include training, proper documentation, communication, support, etc.
- Process: refer to network management process, such as auditing, design compliance, continuity place, impact on change, etc.
- Tools: used to monitor the network. Good documentation also helps

A highly available network is a resilient network, which employs various techniques to recover and continue operating in the event of failure. Resiliency can include:
- Network-level resiliency: redundancy + quick to recover from failure
<table>
<thead>
<tr>
<th>Network Component</th>
<th>Convergence Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Spanning Tree</td>
<td>Subsecond for minor failures, 1–2 seconds for major failures.</td>
</tr>
<tr>
<td>Etherchannel</td>
<td>Approximately 1 second to redirect traffic to a different link in the channel.</td>
</tr>
<tr>
<td>First Hop Redundancy Protocols such as HSRP, VRRP, or GLBP</td>
<td>Default of 10 seconds. Recommended tuning of hello time to 1 second and hold time to 3 second yields a 3 second convergence time.</td>
</tr>
<tr>
<td>Routing Protocols</td>
<td>Subsecond for OSPF and EIGRP with recommended tuning of timers.</td>
</tr>
<tr>
<td>Switch Service Modules</td>
<td>Typically 3–5 seconds. Exception is Cisco Application Control Engine (ACE) with 1 second failover in active/active configuration.</td>
</tr>
<tr>
<td>Computer/Server TCP Stacks</td>
<td>9-second session teardown for Windows, longer for other OSs.</td>
</tr>
</tbody>
</table>

- System-level resiliency: redundancy within the hardware, and include features that enable fast failover.
- Network management and monitoring: to detect failure and inform actions taken. Include syslog, SNMP, IP SLA, etc.

Syslog is the system logging output of Cisco system, it takes the general format of ‘%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC:MESSAGE’. FACILITY-SUBFACILITY tells the protocol that generate the message. SEVERITY is expressed in numeric form from 0 (emergency) to 7 (debugging). MNEMONIC is a code that identifies action reported. MESSAGE describes the event that triggered the syslog message.

IP SLA enables a Cisco router or switch to simulate specific type of traffic and send it to a receiver, called a responder. The responder can be a computer or a server, you can configure it using ‘(config)#ip sla responder’ command. If Cisco device is the responder, it can add timestamp to it.

Layers 2–4 convergence time is enhanced in Cisco 4500 and 6500 series switches with redundant route processors (RP) by using NSF with SSO. When using this, only one RP is active. The standby RP synchronizes its configuration and dynamic state information (such as CEF, MAC, and FIB tables) with the active RP. When the active RP fails, SSO enables the standby RP to take over immediately. NSF keeps the switch forwarding traffic during the switchover, using the existing route and CEF tables. The goal of NSF with SSO is to prevent routing adjacencies from resetting, which prevents a routing flap. The switchover to the new RP must be completed before routing timers expire, or the router’s neighbors will tear down their adjacency and routing will be disrupted.

When the new RP is up, the old routes are marked as stale, and the RP asks its routing peers to refresh them. When routing is converged, it updates the routing and CEF tables on the switch and the linecards.

NSF is supported with EIGRP, OSPF, ISIS, and BGP. An NSF-capable router supports NSF; an NSF-aware router does not support NSF but understands it and continues forwarding traffic during SSO.

Switch design can be L2 access switch with distribute VLAN, L2 access switches with local VLAN or L3 access switches.
<table>
<thead>
<tr>
<th>HRSP</th>
<th>VRRP</th>
<th>GLBP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco proprietary</td>
<td>IETF standard; supported on Cisco 4500 and 6500</td>
<td>Open standard; supported on Cisco 4500 and 6500</td>
</tr>
<tr>
<td>0000.0c07.ACxx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standby monitor Hello from Active, and take over if no Hello is heard within dead timer from UDP 1985, 224.0.0.2</td>
<td>Standby monitor Hello from Active, and take over if no Hello is heard within dead timer from UDP 112, 224.0.0.18</td>
<td>Group members (AVF) multicast Hello every 3 seconds to UDP 3222, 224.0.0.102</td>
</tr>
<tr>
<td>Track using IP SLA or just 'standby track'</td>
<td>Track using IP SLA</td>
<td>Track using IP SLA or just 'glbp track'</td>
</tr>
<tr>
<td>Maximum of 255 groups</td>
<td></td>
<td>Maximum of 1024 groups</td>
</tr>
<tr>
<td>When using MLS, configure same switch as primary HSRP router and SP root</td>
<td>When using MLS, configure same switch as master VRRP router and SP root</td>
<td>If use same VLANs on multiple access switch, use HSRP or VRRP. Local VLANs should use GLBP</td>
</tr>
<tr>
<td>Initial: HSRP is not running</td>
<td>Hello timer = 1 second by default, change with '(config-if)#vrrp GROUP timers advertise SEC'</td>
<td>Uses 3 methods of load balancing:</td>
</tr>
<tr>
<td>Learn: doesn't know virtual IP address, wait to hear from Active</td>
<td></td>
<td>- Weighted load balancing</td>
</tr>
<tr>
<td>Listen: router knows IP and MAC of virtual router, but it's not active or standby</td>
<td></td>
<td>- Host-dependent load balancing: given host always uses the same router</td>
</tr>
<tr>
<td>Speak: send periodic HSRP and participate in election of active router</td>
<td></td>
<td>- Round-robin load balancing: each router MAC is used to respond to ARp request in turn.</td>
</tr>
<tr>
<td>Standby: monitor active Active: forward packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Show standby Show standby interface Show standby brief</td>
<td>Show vrrp brief</td>
<td>Show glbp brief</td>
</tr>
</tbody>
</table>
Here are some types of attacks against a switched network (including against wireless router or hubs, access switches, or hubs):
- MAC address attack rely on flooding the CAM table and can be mitigated using port security and port-based authentication (802.1x).
- VLAN-based attacks include VLAN hopping, switch spoofing (mitigated by turn off DTP) or 802.1Q double tagging (VACL, private VLAN, or protected port).
- Spoofing attacks include DHCP spoofing (DHCP snooping and IP source guard using ‘ip verify source port-security’), MAC address spoofing, and ARP spoofing (DHCP snooping + dynamic ARP inspection).
- Attacks against the switch: disable CDP, remove unused devices, set up and monitor syslog, use SSH, etc.

Cisco support 3 types of ACL:
- traditional ACL
- QoS ACL
- VACL is like route maps because it uses ‘set’, which can be ‘forward’, ‘drop’, or ‘redirect’. Verify with ‘show vlan access-map VACL’ or ‘show vlan filter access-map VACL’

Private VLAN allow you to have a secondary VLAN in additional to your current one. Secondary VLANs can be community VLAN or isolated VLAN.

802.1x can be enabled with
(config)#aaa new-model
(config)#aaa authentication dot1x default group radius
(config)#dot1x system-auth-control
(config-if)#dot1x port-control [auto | force-authorized | force-unauthorized]
Show dot1x

VoIP system can include:
- IP Phones: provide voice and applications to user
- Cisco Unified Communications Manager (UCM) serve as IP PBX. Register phones and control calls
- Voice Gateway: translated between PSTN and IP calls and provide backup to Cisco UCM
- Gatekeepers: optional component that can do CAC, allocate bandwidth for calls, and resolve phone numbers into IP address
- Video conferencing unit: allow video and voice in the same phone call
- Multipoint control unit: allow multiple participants to join an audio or video conference call
- Application server: provide services such as Unity voice mail and presence

VoIP system consist of voice traffic and call control signaling. Voice traffic is carried using UDP-based RTP. Call control uses one of several different protocols to communicate between the phone and UCM and between UCM and voice gateway.
Before implementing VoIP, consider the requirements:
- Maximum delay of 150 - 200 ms (one-way)
- No more than 1 percent packet loss
- Maximum average jitter of 30 ms
- Bandwidth of 21 - 106 Kbps per call, + about 150 Kbps/phone for control traffic
  Bandwidth need for phone call = packet rate/second * (packet payload + all headers)

When using VoIP, its traffic should only flow through voice VLAN. Voice VLAN enables
phones to be dynamically placed in a separate IP subnet from hosts, to have QoS and
security policies applied and make troubleshooting easier.

PoE switches can provide power to IP phones, there are Cisco and IEEE’s standard
that provide PoE. Some Cisco switches can only supply up to 20 W, a switch assumes
15.4 W of power until the connected device tell it the amount needed.

QoS for VoIP is applied differently than traditional QoS, but the theory still applies.
Main QoS actions include:
- Classification
- Marking
- Policing
- Queuing
- Dropping
- Traffic shaping and conditioning
  Voice has IPP value of 5 and DSCP value of 46 or expedited forwarding

When configure VoIP on a switch, consider to support:
- PoE
- Voice VLAN
- QoS: you can consider enable AutoQoS using ‘(config-if)#auto qos voip {trust I cisco-
  phone}’ command.
- Fast convergence
- Test plan

Video over IP roughly fall into one of 3 categories:
- Many-to-many: include interactive video, peer-to-peer video, video conferencing, etc.
  Data flow from client-to-client, or MCU-to-client. Bandwidth may require up to 12 Mb/s
  per location
- Many-to-few represent IP surveillance cameras, typically require up to 4 Mb/s of
  bandwidth per camera
- Few-to-many describe typical streaming video. Most predictable of all and users
typically tolerate less-than-perfect quality. Traffic flow from storage-to-client to from
server-to-client.
QoS requirement for video should include compression for those that don’t have a lot of moves. It should have its own queue.

Cisco unified wireless network has 5 components that work together to create a complete network, they are:
- Client services: Cisco clients and Cisco compatible third-party vendor clients
- Mobility platform: APs and bridges use LWAPP
- Network unification: leverages existing wired network, include WLAN controller and switch and router modules
- Network management: visualize and secure WLAN. WCS for location trafficking, RF management, wireless IPS, and WLC management
- Mobility services: applications such as wireless IP phone, location appliance, and RF firewall

Wireless products can be separated into 3 groups:
- Client wireless, allow mobile users to access wired LAN resources.
- Wireless connections between building
- Wireless mesh can span large distance because on edge APs connect to the wired network. Intermediate APs connect wirelessly to multiple other APs and act as repeater. Each AP has multiple paths through the wireless network. AWP protocol runs between APs to determine the best path to the wired network.

Client association connectivity:
1. Client send probe request and listen for beacons and probe responses
2. AP send probe responses
3. Client initiate an association to AP. 802.1x authentication, and any other information is send to AP
4. AP access association. SSID and MAC address information is exchanged
5. AP adds client’s MAC address to its association table.

Layer 2 roaming is done between APs on the same subnet and managed by the switches using a multicast protocol: Inter-Access Point Protocol (IAPP). Layer 3 roaming is done between APs on different subnets and is managed by the wireless LAN controllers. The switch connected to the AP updates its MAC address table when a client roams.

Short roaming times are needed for VoIP to reduce delay. A client will attempt to roam (or associate with another AP) when
- It misses too many beacons from the AP.
- The data rate is reduced.
- The maximum data retry count is exceeded.
- It is configured to search for another AP at regular intervals.

There are 2 wireless designs:
- Autonomous access points can be centrally managed by CiscoWorks Wireless LAN solution engines (WLSE), use Cisco Secure Access Control Server (ACS) for RADIUS
and TACACS+ authentication, and wireless domain services (WDS) for RF management. Support L2 roaming
- Lightweight access points in combination with WLAN controllers; also called split MAC. LWAPP uses AES-encrypted control messages and encapsulates, but doesn’t encrypt data traffic. They can also communicate with each other using CAPWAP, which is IETF standard that is very like LWAPP.

Lightweight AP discover WLC by:
1. AP requests DHCP address, server respond with management IP address of one or more WLC
2. AP send LWAPP or CAPWAP discovery request message to each WLC
3. WLC respond with an LWAPP or CAPWAP discovery response that include the number of APs currently associated to it
4. AP sends a Join Request to WLC with fewest APs associated with it
5. WLC responds with a Join Response; AP and WLC authenticate each other and derive encryption keys. WLC then configures AP with settings and parameters.

Note: AP and WLC must have IP reachability. Configuration is done on the WLC, which support both L2 and L3 roaming. Link between LAP and switch is access, whereas link between switch and WLC is trunk; EtherChannel is recommended.

WLC can be a
- Appliance: 5500 series for large deployment, support up to 250 AP. 4400 series for medium deployment and support up to 100 APs. 2100s for small deployment and support up to 25 APs
- Wireless service Module (WiSM) can be installed on Cisco 6500 and 7600 for large deployment that need support for up to 300 APs.
- Integrated into 2750G, which can support up to 25 APs/switch, or 100/switch stack.
- Cisco ISR router have a WLC module that can support up to 25 APs.

4400 can support EtherChannel, but not its protocols, so you need to specify its mode as “On”. Configure the channel as a trunk, allow only the management and wireless VLANs, and trust CoS.

The WiSM requires a separate VLAN for its management. This VLAN should be assigned only to the module’s service port and should not be used outside of the switch. Assign the VLAN to the service port with the global command `wism service-vlan vlan`. Assign an IP address to the VLAN interface; this IP address is used to communicate with the WiSM. The WiSM contains eight logical ports that connect to the switch fabric in two Etherchannel bundles. It also contains two separate controllers. Bundle configuration is done at each controller, using the `wism module slot# controller controller#` set of global commands.

H-REAP addresses any problem with WLC and AP separated by WAN links. It can operate in one of 2 modes, configured on WLC:
- Connect: traffic from AP is send to local switch to be tunneled to WLC when WLC is reachable.
- Disconnect: when WLC is not reachable, AP authenticates clients itself.

**TSHOOT**

Network maintenance involves:
- Installing new equipment
- Adjusting settings to support new service
- Securing the network
- Restoring service
- Back up configs
- Planning new or upgraded service
- Building redundancy and disaster recovery
- Documentation
- Responding to user complaints

It's recommended that you use a model to troubleshoot/maintain your network.

Common tasks:
- Adds, moves, and changes
- Compiling documentation
- Preparing for disaster
- Capacity planning/utilization monitoring
- Troubleshooting
- Proactive scheduled maintenance
- Rollback plans for each change
- Lab testing in a controlled environment before each change is put into production to minimize risk

Documentation should include:
- Configuration templates/standards
- Configuration history
- Equipment history
- Circuit inventory
- IP address assignment
- Network drawings
- Communication plan
- Out-of-band communication details
- Expected traffic pattern

Network services should be synchronized with NTP,
### Character Usage

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Begins with</td>
<td>^Fast matches lines that begin with FastEthernet.</td>
</tr>
<tr>
<td>$</td>
<td>Ends with</td>
<td>FastEthernet0/0$ matches lines that end with FastEthernet0/0.</td>
</tr>
<tr>
<td>.</td>
<td>Any character</td>
<td>Ethernet./. matches Ethernet 0/0, FastEthernet0/1, and Ethernet ?.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td>FastEthernet 0/0</td>
</tr>
<tr>
<td>_</td>
<td>Matches beginning, end, _Ethernet_ matches any line that includes the word “Ethernet.” or braces</td>
<td></td>
</tr>
</tbody>
</table>

Pings can be set to different packet size through Datagram Size. Router can automate testing a range of sizes. To do so, use the extended commands and choose to sweep a range of sizes.

By using telnet, you can test various ports to see if that service is available.

If you suspect problem with device hardware, use ‘show environment all’ command. Memory shortage can also cause problems, examine with ‘show memory’ ‘show controller’ is another method of discovering hardware issues.

You can use SPAN or RSPAN to monitor network performance.
Router IP traffic export (RITE) is similar to SPAN but used by routers to capture traffic to a monitoring port.

    (config)# ip traffic-export profile rite
    (config-rite)# interface FastEthernet 0/1
    (config-rite)# bidirectional
    (config-rite)# mac-address 00a.8aab.90a0
    (config-rite)# incoming access-list my_acl
    (config-rite)# outgoing sample one-in-every 10
    (config)# interface FastEthernet0/0
    (config-if)# ip traffic-export apply rite
NetFlow collects summaries of traffic information and transmits the summary to a NetFlow collector. NetFlow is enabled on each monitored interface. NetFlow support version 5 and 9, system should have the same version. NetFlow exports information to a targeted address.
(config-if)#ip flow ingress
(config)#ip flow-export version {5 | 9}
(config)#ip flow-export destination ip-address IP_ADD
#show ip cache flow

Embedded event manager (EEM) enables custom reactions to events (include CNMP< syslog, IOS command, and email message) and act as a supplement to SNMP.
SNMP is another monitoring protocol that can be enabled with
(config)#snmp-server host [ip-address IP_ADD]
(config)#snmp-server enable traps [NAME_OF_SPECIFIC_TRAP]

Ethernet performance issues are usually associated with:
- Port problem
- Duplex mismatch
- TCAM issues
  In ‘show interface’ or ‘show interface counters errors’, notice these counters:
  - Align-Err, runts: alignment errors are usually associated with cabling, NIC, or duplex mismatch
  - FCS-Err: usually associated with a cabling issue
  - Xmit-Err: occur because transmission buffers are full. Commonly associated with switching a faster to a slower link
  - Undersize, Giants: problem with transmitting NIC
  - Single-Col, Multi-Col, Late-Col, Excess-Col: sign of duplex mismatch.

Cisco switches support auto-MDIX that can automatically adjust speed and duplex. Enabled with ‘(config-if)#mdix auto’

VLAN switching issues are based on 3 failures:
- Wiring issues: cabling issues, power outage, or bad switch ports
- Switch issues: software/hardware bugs, loops, and ARP issues
- Logic (configuration) issues

Switch problems are often based on identify the path traffic takes through the switch, use ‘show platform forward’ and ‘traceroute mac’.

Verify CEF with ‘show ip cef’ and ‘show adjacency’
Catalyst 3560, 3750, and 4500 switches can also use ‘show platform’
Catalyst 6500 switches display forwarding details using ‘show mls cef’
Troubleshooting routing issues can be summarized into:
- Is this the correct route received?
- Is this the correct route advertised?
- Is the chosen path different than what you expect?

OSPF neighborship requires 6 parameters to form:
- Bidirectional communication
- Equal timer values
- Matching ASN
- Router must agree on type of their common area
- Router must agree on the prefix of their common subnet
- Authentication, if used, must agree on type and password.

‘show ip route profile’ shows routing table changes over consecutive 5-second interval. Helpful to show that routes are flapping.

High CPU utilization is a concern when it becomes on-going. Signs include dropped packets, increased latency, slow response to telnet and console, and when router skips routing updates.

Show process cpu can identify processes that are consuming CPU cycles. The ARP Input process consumes more cycles if the router has to generate a large number of ARPs, for instance in response to malicious traffic. Net Background is used to manage buffer space. IP Background is used whenever an interface changes state, utilization here could indicate a flapping interface.

Show process cpu history displays the overall utilization as a bar graph. This is a nifty way to see if the current load is an aberration or the norm.

Another router issue is switching mode, process switching requires high utilization of CPU.

Memory over-utilization is another problem that causes memory shortage. It can be caused by loading a IOS that requires more RAM than is present on router. Memory leaks can be recognized over time using show memory allocating-process totals and show memory dead and by researching known bugs within CCO. If found, the only solution is to move to a known good version of IOS.

Memory leaks sometimes appear on interfaces as buffer leaks. Buffer leaks can be seen using show interface, where the “input queue” shows buffer utilization. Show buffer also shows a buffer leak, here by looking at the number of free buffers.

Finally, memory leaks are sometimes seen in BGP, which is a heavy consumer of memory in the best of times, so a memory leak here can quickly bloom into a larger issue. show process memory | include bgp shows the memory utilization of the four BGP processes. show diag can be used to evaluate memory used on the line cards.
Network device has 3 parts, all of which are affected by security concern:
- Management plane: troubleshoot authentication is tricky and your rollback plan should include ‘reload in x’ command.
- Control plane: depends on the protocols, or reachability of different neighbors.
- Data plane: include support for user application, can be tested using traceroute and telnet. ACL should be logged.